Journal of Information Systems and Informatics
Vol. 4, No. 1, March 2022 e-ISSN: 2656-4882 p-ISSN: 2656-5935
http://journal-isi.org/index.php/isi Published By DRPM-UBD

Tourism Application Information System Security Audit Using Cobit 5 Framework on Palembang City

Febriyanti Panjaitan[1], Susan Dian Purnamasari*[2], Windi Melisa[3]

[1]Informatics Study Program, Faculty of Computer Science, Bina Darma University
[2,3]Information Systems Study Program, Faculty of Computer Science, Bina Darma University
Jalan Ahmad Yani No.03 Plaju Palembang
Email: febriyanti_panjaitan@binadarma.ac.id [1], susandian@binadarma.ac.id[2]
windimelisa60@gmail.com [3]

Abstract

Information technology is important in organizations so that the goals and expectations of the objectives of implementing IT can be achieved. The tourism office of the city of Palembang is an institution that has used information technology to help the continuity of their work. The tourism office of the city of Palembang has not conducted an audit of improving the security of the existing information system. Therefore, to avoid events that do not require an information security system audit. Cobit 5 framework that can be used as a reference for information system governance to achieve the expected goals. This study only discusses the security management process which includes the DSS05 (Delivery, service, and security) domain by collecting data using a questionnaire. The value of the level of security improvement to be achieved in the security system should reach level 5 and can provide recommendations that will be followed up by the institution to make improvements in the future.

Keywords: Application, Cobit 5, DSS05

1. INTRODUCTION

Almost all agencies in government in the era of globalization have utilized technology to carry out the process of activities in government because information technology is important for achieving goals and strategies that are following the standards of the government organization. The role of this technology can be one of the media in the delivery of information to be faster, accurate and efficient. Currently, technology that is often used and easily accessible is in the form of applications that can provide information and services. The use of applications that are almost on all lines of life is the fruit of digitalization that makes people increasingly want a lot of convenience in various fields through the use of the internet in all sectors including the government sector which is related to the information, promotion and socialization process [1]. The more developed applications with internet-based systems, the higher the level of vulnerability to data security to be attacked by other unauthorized parties [2].

Palembang City Tourism Office is one of the bodies in the government that utilizes information technology by having an application that can be used by tourists to find out and get information about tourism in Palembang City. Since this application was launched, there has never been an audit of security maturity, even though this application is very useful for tourists who will visit Palembang city [3]. Today several methods and standards can be used to support the audit process effectively, efficiently and on target. Security audits are carried out to determine whether there is security of information systems and how the security process runs. In addition, audits are conducted as an effort to assess the risk and protection of the organization's assets. Thus, better security can be prepared against the asset to reduce the risks that may arise. To carry out the implementation of information technology-based security audits, a framework is needed that can help an organization to improve information technology governance by following IT governance standards in companies, one of which is the Cobit 5 framework so that it can be seen how the tourism application capabilities managed by the Palembang City Tourism Office.

Some studies that have implemented Cobit 5 as an information technology governance audit method in research [4] use Cobit 5 as a method in the information system security audit plan that exists in the environment in the city government in Yogyakarta in the form of information security, processing infrastructure and applications, while in research [5] Using Cobit 5 including APO13 and DSS05 domains has been done well with maturity information governance level in security audit is 1.84 is at level 2 (managed), with references from some previous research then framework that can be used to measure the maturity level of application security is the framework Control objective for Information and Related Technology (COBIT) version 5. COBIT was chosen because it provides good practice across domains and process frameworks in a logical governance structure to help optimize IT capabilities in investment and ensure that IT is successful in delivering business needs.

2. METHODS

2.2 Research Methods

The research method used by the author is the Descriptive Quantitative Method. According to Nazir in his book entitled Research Methods in 2011, one form of this method is a survey that is an investigation held to obtain facts of existing symptoms and seek factual information, both social, economic and political institutions of a group or region [7]

2.2 Cobit 5

a. Cobit 5

One of the frameworks for the governance and management of information technology that combines the latest thinking in corporate governance and management techniques provides principles, practices, analytical tools and models to help increase the trust and value of information systems.

b. Maturity Level

Cobit 5 has an IT process maturity model using assessment methods so that an organization gets numbers or indices from its OWN IT processes [4]. Here are the maturity levels of Cobit 5:

1) Level 0 –Incomplete process (incomplete process): At this level, the process is not implemented or fails to achieve its process objectives
2) Level 1-performance process: Initially this process has been implemented and managed including monitoring planning and adjustments
3) Level 3 – Established Process (process established): In this process, the process under construction is implemented using the process that has been defined to achieve the results of the process
4) Level 4-Predictable Process (predictable process): At this level, the process that has been built is then operated with limit limits to achieve the process.
5) Level 5- process optimizing (process optimized): At this level, predictable processes are continuously improved to meet business goals.

To see the level of the evaluation results using Cobit 5 of its maturity level, as for how to calculate using the equation:

$$\text{maturitas} = \frac{\Sigma\ (\text{Skala proses atribut per responden})}{\Sigma\ (\text{Jumlah responden})}$$

Source (ISACA. COBIT 5 Framework. 2012)

c. Measurement Scale

The measurement scale used in this study uses the scale provided by framework Cobit 5 [4] which can be seen in Table 1 below:

Table 1. Questionnaire Answer Scale

No.	Kelompok
0	The process is not done

1	The process is carried out and achieves the goal
2	The process is done, achieves the goal, and is well managed
3	The process has been established/ standardized
4	Processes are executed consistently within predetermined limits
5	Processes are executed consistently within predetermined limits

Table 2. Questionnaire Measurement Scale

Maturity Index	Maturity Level	Explanation
0.0 - 0.50	Level 0 (Incomplete Process)	The organization at this stage does not carry out it processes that should exist or have not succeeded in achieving the objectives of the IT process.
0.51 - 1.50	Level 1 (Performed Process)	The organization at this stage has successfully implemented the IT process and the objectives of the IT process have been achieved.
1.51 - 2.50	Level 2 (Managed Process)	Organizations at this stage in carrying out IT processes and achieving their goals are carried out in a well-managed manner, so there is more assessment because implementation and achievement are carried out with good management. Management in the form of a process of planning, evaluation and adjustment to be better.
2.51 - 3.50	Level 3 (Established Process)	Organizations at this stage have IT processes that have been standardized within the scope of the organization as a whole. This means that it already has process standards that apply throughout the scope of the organization.
3.51 - 4.50	Level 4 (Predictable Process)	Organizations at this stage have carried out IT processes within certain limits, such as time limits. This limitation results from measurements that have been made at the time of the implementation of the IT process before.
4.51 - 5.00	Level 5 (Optimizing Process)	At this stage, the organization has made innovations and made continuous improvements to improve its capabilities.

2.3 Respondent

The determination of respondents was made using RACI (Responsible, Accountable, Consulted and Informed) DSS 05 on Cobit 5 [4] or often called RACI Chart / RABI Chart Matrix. In an organization, RACI Chart is one of the tools that can be used for decision making and assisting management. This study will use 5 respondents and respondent information can be seen in Table 3.

Table 3. Respondent Information

No.	Type	Respondent
1	Sub section planning and reporting	1
2	Tourism marketing field	1
3	Tourism marketing strategy section	1
4	Tourism information section	1
5	Tourism promotion section	1

2.4 Cobit Mapping

To get an evaluation from Cobit, it is necessary to do mapping based on the needs of research, namely IT / IS governance which means focusing on Resource Optimisation thanks to the Primary (P) category, the primary category is the main activity provided by COBIT, while secondary is a supporting activity if needed [4]. The first mapping stages are:

1) Define Enterprise Goals.
2) Conduct mapping of Enterprise Goals to IT-Related Goals to align company goals with IT goals, Mapping Enterprise Goals to IT-Related Goals.
3) Mapping IT-Related Goals to Process, where the author has determined the domain to be used in evaluating IT / IS governance, the DSS 05 domain has activities that become tools in evaluating the form of questionnaires.

Table 4. Mapping IT-Related Goals to Process

			security of information, processing infrastructure and applications
	Cobit 5	Process	10 Internal
Deliver, service and support	DSS 05	Manage Security Service	

2.5 Instrumen Deliver, Service dan Support (DSS 05) Cobit 5

DSS 05 is a process that focuses on protecting information assets in organizations to maintain the level of information security risks that can be received by the organization following security policies. The goal of DSS 05 is to classify business process problems and look for root causes to prevent information vulnerabilities and incidents. DSS 05 contains management, namely:

a. DSS05.01 (Protect against malware)
It is a practice to protect against malware. Governance practices are implementing and maintaining prevention, and remedial measures in place throughout the organization to protect information and technology from malware such as viruses, spyware worms and spam.

b. DSS05.02 (Manage network and connectivity security)
It is a practice of network management and connectivity security. The governance practice is to use security and related procedures to protect information over connectivity security.

c. DSS05.03 (Manage endpoint security)
It is the practice of managing endpoint security. The governance practice is to ensure that endpoint devices such as laptops, desktops, servers are guaranteed at the same level as or greater than the security procedures that have been defined.

d. DSS05.04 (Manage user identity and logical access)
It is the practice of managing user identity and access rights. The governance practice is to ensure that all users have access to rights information according to their needs.

e. DSS05.05 (Manage physical security)
It is the practice of defining and implementing procedures, restricting and revoking access following business needs and emergencies. Manage the security of access to the place authorized by that access. Monitor people entering the access site including staff, temporary staff, clients, vendors and visitors or third parties.

f. DSS05.06 (Manage sensitive documents and outputs devices)
Is the practice of managing document security. The governance practices undertaken are establishing appropriate physical safeguards, inventory of important documents and managing inventory of IT assets such as securities, security tokens.

g. DSS05.07 (Manage Information Security Incidents)
It is the practice of defining and communicating the characteristics of potential security incidents and providing guidance to process management on how to handle security incidents.

h. DSS05.08 (Manage Information Handling)
Manage the security of information assets throughout the life cycle of the organization.

Of the 8 existing managements, then in this study will be used as a grid of questionnaire instruments tailored to the needs of the study.

Table 5. DSS Instrument Grid 05

Domain	Aim	Management Practice	Activities
DSS05 (Manage security services).	To Manage security services	DSS05.01 (Protect against malware)	Menerapkan dan memelihara pencegahan
			Menerapkan dan memelihara pencegahan
		DSS05.02 (Manage network and connectivity security)	Menggunakan keamanan dan prosedur yang terkait untuk melindungi informasi atas keamanan konektivitas.
		DSS05.03 (Manage enpoint security)	Memastikan keamanan perangkat endpoint
		DSS05.04 (Manage user identity and logical access)	Pengelolaan identitas pengguna dan hak akses.
		DSS05.05 (Manage physical security)	Memantau orang yang memasuki tempat akses
		DSS05.06 (Manage sensitive documents and outputs devices)	Mendefinisikan dan menerapkan prosedur, membatasi dan mencabut akses sesuai dengan kebutuhan bisnis serta keadaan darurat.
		DSS05.07 (Manage Information Security Incidents)	Mengelola keamanan dokumen.
			Pendefinisian dan mengkomunikasikan karakteristik insiden keamanan potensial
		DSS05.08 (Manage Information Handling)	Mengelola keamanan aset informasi seluruh siklus hidup organisasi.

Source: (ISACA. COBIT 5 Process Assessment Model. 2012)

3 RESULTS AND DISCUSSION

3.1 Questionnaire Recapitulation Results

The rekacapulation of questionnaires obtained from the answers of 5 respondents based on the DSS 05 instrument with 15 statements was calculated using the formula provided by COBIT 5 to obtain maturity level results. Calculation of maturity levels with the Cobit 5 equation is:

$$\text{Maturity} = \frac{2.6 + 4 + 4 + 3 + 3.6 + 2.4 + 3 + 2.2 + 2.4 + 2.2 + 4 + 2.4 + 2.6 + 3 + 4}{15}$$

$$\text{Maturity} = \frac{45.4}{15}$$

$$= 3.02$$

The results of the recapitulation questionnaire can be seen in table 6.

Table 6. Questionnaire Recapitulation Results

DOMAIN	NO. STATEMENT	R 1	R 2	R 3	R 4	R 5	TOTAL	AVERAGE ANSWERS	AVERAGE ACTIVITY	LEVEL MATURITY
DSS 05.01	1	3	2	2	3	3	13	2.6	3.3	3.02
	2	4	4	4	4	4	20	4		
DSS 05.02	3	4	4	4	4	4	20	4	3.5	
	4	3	3	3	3	3	15	3		
DSS 05.03	5	4	4	3	3	4	18	3.6	3	
	6	3	3	2	2	2	12	2.4		
DSS 05.04	7	3	3	3	3	3	15	3	2.6	
	8	3	2	2	2	2	11	2.2		
DSS 05.05	9	2	2	3	3	2	12	2.4	2.3	
	10	2	2	3	2	2	11	2.2		
DSS 05.06	11	4	4	4	4	4	20	4	3.2	
	12	3	3	2	2	2	12	2.4		
DSS 05.07	13	2	3	2	3	3	13	2.6	2.8	
	14	3	3	3	3	3	15	3		
DSS 05.08	15	4	4	4	4	4	20	4	4	

3.2 Maturity Level Results

Based on the calculations in table 6 above, it can be explained that the level of security maturity of the Tourism Application Information System in the Tourism Office of Palembang city is at level 3 with Established Process conditions, which means that overall tourism applications have procedures or standards to regulate security management activities up to the current user.

Table 7. Maturity Level Results

Domain Proses	Process Description	Maturity Level	Information
DSS 05	Manage Security Service	3.02	Established Process

Here are the results of the statement of each management activity based on DSS 05, namely:

1. DSS 05.01 is a practice to protect against malware, which means that the Palembang City Tourism Office has had and implemented precautions against attacks or threats on the Application and has protected information and technology from malware such as viruses, spyware worms and spam periodically following procedures. Palembang City Tourism Office application is protected by Bitdefender software for malware security.
2. DSS 05.02 is a practice of network management and connectivity security, which means that the Palembang City Tourism Office has used security following the procedures that have been defined or standardized to protect information over connectivity security on the Application. Palembang City Tourism Office application is protected by Comodo Firewall software for network security.
3. DSS 05.03 is the practice of managing endpoint security, which means that the Palembang City Tourism Office has ensured and guaranteed endpoint devices such as laptops, desktops, servers at the same level as or greater than the security procedures that have been defined for the Application. Users evaluate endpoint security every 3 months; this is evidenced by reports made by users periodically.
4. DSS 05.04 is a practice of managing user identity and access rights, which means that the Palembang City Tourism Office has ensured and guaranteed the management of user identity and access rights, restricting, and revoking access to use following the needs of the Application. The application is only managed by one admin, namely in the tourism information section, for emergency access rights managed by the Planning and Reporting Subsection.
5. DSS 05.05 Is a physical security management practice, restricting and revoking physical access as needed, which means that the Palembang City

Tourism Office has managed access security and monitored people entering the access site including staff, temporary staff, clients, vendors and visitors or third parties. The server for the application is only managed by one admin, when some parties are not related to the management of the application will be assisted and monitored through CCTV.

1. DSS 05.06 is a practice managing document security, which means that the Palembang City Tourism Office has built appropriate document security, defined, and implemented application usage security procedures, inventory of important documents such as managing inventory of IT assets, securities and Application security tokens.
2. DSS 05.07 is a practice of defining and communicating incident characteristics, which means that the Palembang City Tourism Office has defined and communicated the characteristics of security incidents that have the potential to damage data and provide guidance to all staff on how to handle security incidents that occur on the Application.
3. DSS 05.08 Manages the security of information assets, which means that the Palembang City Tourism Office has carried out information asset security management ranging from data to be inputted and processed to output.

4 CONCLUSION

Based on the results of research obtained on the Security of Information System Application of the Tourism Office Palembang city using the Cobit 5 Framework, conclusions can be drawn, namely:

1. The maturity level obtained is 3.02 is at level 3, namely Established Process, which means that the application already has a good security standard.
2. The level of security maturity of the Palembang City Tourism Office Information System has not been following the expected target, namely at level 4. To increase the maturity level from level 3 to level 4 as expected, the authors summarize the overall recommendations of (1) Using the latest antivirus and firewall to prevent potential threats, (2) Adjusting hardware that supports software performance. (3) Standardize policies regarding access rights and SOPs for the use of the Application following the current state of the Application.

REFERENCES

[1] R. T. F. Palar, Y. Rindengan, and S. R. Sentinuwo, “Analisa Kematangan Dinas Komunikasi dan Informatika Kota Manado Menggunakan Framework COBIT 5 Pada Domain Monitor, Evaluate and Assess,” pp. 1–9, 2021.

[2] I. J. Aritonang, E. D. Udayanti, and N. Iksan, “Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13),” ITEJ

(Information Technol. Eng. Journals), vol. 3, no. 2, pp. 6–10, 2018.

[3] C. Santosa and W. Widyawan, "PEMETAAN PENURUNAN TUJUAN COBIT 5 UNTUK AUDIT KEAMANAN SISTEM INFORMASI (STUDI KASUS: SISTEM INFORMASI AKADEMIK SEKOLAH TINGGI XYZ)," ReTII, 2015.

[4] D. Ciptaningrum, E. Nugroho, and D. Adhipta, "COBIT 5 sebagai Metode Alternatif bagi Audit Keamanan Sistem Informasi (Sebuah Usulan untuk diterapkan di Pemerintah Kota Yogyakarta)," SEMNASTEKNOMEDIA ONLINE, vol. 3, no. 1, pp. 1–2, 2015.

[5] P. P. G. P. Pertama and I. W. Ardiyasa, "Audit Keamanan Sistem Informasi Perpustakaan STMIK STIKOM Bali Menggunakan Kerangka Kerja COBIT," J. Sist. dan Inform., vol. 13, no. 2, pp. 77–86, 2019.

[6] D. M. Efendi, S. Mintoro, and I. Septiana, "AUDIT SISTEM INFORMASI PELAYANAN PERPUSTAKAAN MENGGUNAKAN FRAMEWORK COBIT 5.0," J. Inf. dan Komput., vol. 7, no. 2, pp. 31–36, 2019.

[7] Moh. Nazir, "Metode Penelitian," Ghalia Indones. Jakarta, 2011.

[8] D. Sugiyono, "Metode penelitian pendidikan pendekatan kuantitatif, kualitatif dan R&D," 2013.