Perbanas International Conference on Economics, Business, Management, Accounting and IT (PROFICIENT) 2026

"Integrity-Driven Innovation: Reimagining Business, Finance, and Digital Transformation for Sustainable Impact"

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Information Systems Audit of Perbanas Institute Library Using COBIT-5 Framework: Domains DSS01, DSS02, and DSS05

Aidan Fitrah Wardoyo[1,a)], Muhammad Rafly Harsia Ramadhan[2,b)], Meylinda Dewi Risma[3,c)], Deden Prayitno[4,d)]

[1,2,3,4] *Information Systems Study Program, Faculty of Information Technology, Perbanas Institute, Jakarta, Indonesia*

[a] Corresponding author: aidan.fitrah21@perbanas.id
[b)]muhammad.rafly08@perbanas.id
[c)]meylinda.dewi06@perbanas.id
[d)]deden@perbanas.id

Abstract. *Perbanas Institute Library has implemented a Library Management Information System (LMIS) to support the academic services of the Perbanas Institute community. However, several operational issues have been identified, including system instability, unstructured incident handling, and the absence of documented information security policies. This study aims to measure the maturity level of LMIS governance using the COBIT 5 framework, focusing on three sub-domains of Deliver, Service, and Support (DSS): DSS01 (Manage Operations), DSS02 (Manage Service Requests and Incidents), and DSS05 (Manage Security Services). Data were collected through observation, in-depth interviews, and questionnaires distributed to respondents identified based on the COBIT 5 RACI Chart. The measurement results show that DSS01 achieved a Maturity Level of 2.96, DSS02 scored 2.43, and DSS05 scored 2.43, with an overall average of 2.52, categorized as Managed (Level 2). The target level set for all sub-domains is Level 3 (Established). Gap analysis identified remaining deficiencies in several sub-controls, particularly in DSS02 and DSS05. Based on these findings, this study formulates specific technical and managerial recommendations to close the gaps and improve the quality of IT service governance in the library.*

Keywords: Information Systems Audit, COBIT 5, Maturity Level, Library Management Information System, Perbanas Institute

INTRODUCTION

Information technology has become the operational backbone of various sectors, including higher education. In this context, university libraries play a strategic role as academic resource centers supporting teaching, research, and scholarly publication. Perbanas Institute, as a higher education institution in the field of economics and business, has implemented a Library Management Information System (LMIS) encompassing modules for book circulation, online cataloguing (OPAC), membership management, and digital repository access.

However, the implementation of an information system does not automatically guarantee optimal service quality. Based on initial observations, several recurring issues were identified: (1) system instability caused by infrastructure disruptions without standardised recovery procedures; (2) informal and unrecorded handling of user complaints; (3) the absence of documented information security policies; and (4) a lack of written Standard

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Operating Procedures (SOPs) for IT operational activities. These conditions indicate a gap between the actual IT governance capability and the best practices that should be in place (Riyandi et al., 2020).

This study employs the COBIT 5 framework because it offers an ideal combination of broad governance coverage, in-depth process detail, and comprehensive best-practice guidance (Iqbal Agselmora et al., 2022)(Panjaitan & Zuraidah, 2023). The Deliver, Service and Support (DSS) domain was selected because the library LMIS is in an operational phase—not a development phase—making the focus on operational management (DSS01), incident handling (DSS02), and security services (DSS05) most relevant to the identified problems (Panjaitan & Zuraidah, 2023) (Nuraeni & Syarif Haryana, 2016).

Related research has been conducted by Silalahi et al. (2024) on the Library Clearance Information System at UIN North Sumatra using COBIT 5 domains DSS01 and DSS02, yielding an average maturity level of 4.81, categorised as Fully Achieved (Silalahi et al., 2024). Another study by Nuraeni and Haryana (2016) assessed IT governance including security elements at an educational institution using COBIT 5 DSS domain, finding that most subdomains were at capability level 1 (Nuraeni & Syarif Haryana, 2016). The present study extends this body of work by incorporating domain DSS05 and focusing on the context of a financial institution library such as Perbanas Institute.

The objectives of this study are: (1) to measure the governance maturity level of LMIS Perbanas Institute across sub-domains DSS01, DSS02, and DSS05; (2) to analyse the gap between the current state and the target level; and (3) to formulate improvement recommendations that can be implemented by library management.

METHODS

Research Stages

This research was conducted through the following systematic stages: (a) problem identification within LMIS Perbanas Institute; (b) literature review on COBIT 5 and information systems auditing; (c) data collection through observation, interviews, questionnaires, and documentation; (d) data processing using the COBIT 5 DSS domain framework; and (e) presentation of results, gap analysis, and formulation of recommendations.

Problem Identification

The problems identified within LMIS Perbanas Institute include: (1) a system capability level that has not yet been formally measured; (2) uncertainty regarding the monitoring and evaluation of system operations; and (3) the absence of a comprehensive assessment of system security and performance.

Data Collection Method

This study adopts a descriptive-quantitative approach. Data were collected through four methods: (1) direct observation of LMIS usage; (2) interviews with system operators and relevant parties; (3) questionnaires distributed to selected respondents identified via the COBIT 5 RACI Chart; and (4) documentation review of available policies, SOPs, and operational records. Respondent selection was based on the COBIT 5 RACI Chart, as presented in Table 1.

TABLE 1. Respondent Mapping Based on COBIT 5 RACI Chart

Sub-Domain	RACI Role	Respondent Position	Total	RACI Code
DSS01	Responsible, Accountable	Head of Library Division, IT Staff	3	R, A
DSS02	Responsible, Consulted, Informed	IT Staff, Circulation Staff	4	R, C, I
DSS05	Responsible, Accountable, Consulted	Head of IT Division, Head of Library Division, IT Staff	4	R, A, C

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Evaluated Sub-Domains

This study evaluates the three DSS sub-domains most relevant to the operational conditions of LMIS Perbanas Institute, as shown in Table 2.

TABLE 2. Evaluated DSS Sub-Domains

Domain	Sub-Domain	Description
DSS01	DSS01.01	Perform operational procedures
	DSS01.02	Manage outsourced IT services
	DSS01.03	Monitor IT infrastructure
	DSS01.04	Manage the environment
	DSS01.05	Manage facilities
DSS02	DSS02.01	Define incident and service request classification schemes
	DSS02.02	Record, classify and prioritize requests and incidents
	DSS02.03	Verify, approve and fulfil service requests
	DSS02.04	Investigate, diagnose and allocate incidents
	DSS02.05	Resolve and recover from incidents
	DSS02.06	Close service requests and incidents
	DSS02.07	Track and produce reports
DSS05	DSS05.01	Protect against malware
	DSS05.02	Manage network and connectivity security
	DSS05.03	Manage endpoint security
	DSS05.04	Manage user identity and logical access
	DSS05.05	Manage physical access to IT assets
	DSS05.06	Manage sensitive documents and output devices
	DSS05.07	Monitor the infrastructure for security-related events

Data Processing and Maturity Level Analysis

Data processing uses the COBIT 5 Maturity Model approach with a scale of 0–5. The formulas applied are:

$$\textit{Maturity Index} = \Sigma \textit{ Questionnaire Responses} / \Sigma \textit{ Process Domains}$$

$$\textit{Maturity Index} = (\%\ \textit{Achievement / Work Product}) \times \textit{Questionnaire Index}$$

$$\textit{Maturity Level} = \Sigma \textit{ Domain Maturity Index} / \Sigma \textit{ Process Domains}$$

TABLE 3. COBIT 5 Maturity Model Scale

Score Range (Decimal)	Rounded Level	Organizational Capability Status Description
4.51 – 5.00	**Level 5**	**Optimizing**: The process is highly mature, continuously improving, and innovating automatically.
3.51 – 4.50	**Level 4**	**Predictable**: The process operates under defined limits, is well-controlled, and is measured using quantitative data/KPIs.
2.51 – 3.50	**Level 3**	**Established**: The process is standardized, documented in official SOPs, and implemented across all enterprise departments.
1.51 – 2.50	**Level 2**	**Managed**: The process is planned, monitored, and adjusted, but its implementation remains local (per division).
0.51 – 1.50	**Level 1**	**Performed**: The basic process is implemented and achieves its goals, but its execution is still unorganized (ad-hoc).
0.00 – 0.50	**Level 0**	**Incomplete**: The process is not implemented at all or completely fails to achieve its intended purpose.

RESULTS AND DISCUSSION

System Profile and Respondent Characteristics

LMIS Perbanas Institute is accessed by students, lecturers, and staff through a web interface encompassing modules for borrowing, returning, OPAC, and membership management. Data were collected from 8 respondents comprising the Head of Library Division (1 person), Head of IT Division (1 person), IT Staff (2 persons), and Circulation Staff (2 persons). All respondents had been employed for at least one year and had direct operational knowledge of LMIS.

DSS01 Maturity Level – Manage Operations

DSS01 measures the organisation's ability to execute routine IT operational procedures. The measurement results for 5 sub-controls are presented in Table 4.

TABLE 4. Maturity Level DSS01 – Manage Operations

Control Name	Sub-Control	Maturity Index	Status
DSS01	DSS01.01 – Perform operational procedures	3,20	L
	DSS01.02 – Manage outsourced IT services	2,40	P
	DSS01.03 – Monitor IT infrastructure	3,00	L
	DSS01.04 – Manage the environment	3,40	L
	DSS01.05 – Manage facilities	2,80	P
Total Maturity Index		**14,80**	
Maturity Level = 14,80 / 5		**2,96**	**Level 3**

The DSS01 measurement yielded a Maturity Level of 2.96, categorised as Level 3 (Established). This indicates that operational procedures are being carried out but have not yet been fully formalised through documentation. Sub-control DSS01.04 (Manage the environment) scored highest (3.40) because physical management of the server room is relatively well maintained. Conversely, DSS01.02 (Manage outsourced IT services) scored lowest (2.40) due to the absence of a comprehensive written Service Level Agreement (SLA) with the campus network vendor.

DSS02 Maturity Level – Manage Service Requests and Incidents

DSS02 evaluates the organisation's ability to record, classify, and resolve incidents and service requests. The measurement results for 7 sub-controls are presented in Table 5.

TABLE 5. Maturity Level DSS02 – Manage Service Requests and Incidents

Control Name	Sub-Control	Maturity Index	Status
DSS02	DSS02.01 – Define incident classification schemes	2,20	P
	DSS02.02 – Record, classify and prioritize incidents	2,00	P
	DSS02.03 – Verify and fulfil service requests	3,00	L
	DSS02.04 – Investigate and allocate incidents	2,2	P
	DSS02.05 – Resolve and recover from incidents	3,20	L
	DSS02.06 – Close service requests and incidents	2,1	P
	DSS02.07 – Track and produce reports	2,3	P
Total Maturity Index		**17.00**	
Maturity Level = 17,00 / 7		**2,43**	**Level 2**

DSS02 is the sub-domain whose score still requires improvement (Maturity Level 2.43 – Managed). Several sub-controls, such as DSS02.03 (Verify and fulfil service requests, 3.00) and DSS02.05 (Resolve and recover from incidents, 3.20), have already reached the Level 3 (Established) target. However, the incident closure mechanism (DSS02.06 = 1.60) and reporting (DSS02.07 = 1.40) remain very weak, as there is no formal incident recording system and no structured incident summary reporting.

DSS05 Maturity Level – Manage Security Services

DSS05 evaluates the implementation of information security measures to protect IT infrastructure, data, and services. The measurement results for 7 sub-controls are presented in Table 6.

TABLE 6. Maturity Level DSS05 – Manage Security Services

Control Name	Sub-Control	Maturity Index	Status
DSS05	DSS05.01 – Protect against malware	3,40	L
	DSS05.02 – Manage network and connectivity security	2,40	P
	DSS05.03 – Manage endpoint security	2,60	P
	DSS05.04 – Manage user identity and logical access	2,00	P
	DSS05.05 – Manage physical access to IT assets	3,20	L
	DSS05.06 – Manage sensitive documents and output devices	1,80	P
	DSS05.07 – Monitor infrastructure for security events	1,60	N
Total Maturity Index		**17,00**	
Maturity Level = 17,00 / 7		**2,43**	**Level 2**

DSS05 achieved a Maturity Level of 2.43 (Managed). Physical protection (DSS05.05 = 3.20) and anti-malware controls (DSS05.01 = 3.40) have reached the Level 3 (Established) target, as antivirus software is properly installed and the server room is adequately secured. However, identity and logical access management (DSS05.04 = 2.00) remains weak due to the absence of a formal written password policy. Sensitive document management (DSS05.06 = 1.80) and security event monitoring (DSS05.07 = 1.60) are areas that still require significant improvement.

Overall Maturity Level

Table 7 summarises the overall maturity levels of the three evaluated sub-domains.

TABLE 7. Overall Maturity Level of LMIS Perbanas Institute

Domain	Total Maturity Index	Maturity Level	Target Level	Gap
DSS01	14,80	2,96	3,00	0,04
DSS02	15,20	2,43	3,00	0,57
DSS05	17,00	2,43	3,00	0,57
TOTAL	47,00	7,82	9,00	1,44
Average Maturity Level of LMIS Perbanas		**2,61**	**3,00**	**0,48**

Overall, the average maturity level of LMIS Perbanas Institute is 2.52, categorised as Managed (Level 2). This indicates that procedures exist and are consistently repeated, but have not yet been fully documented and formally standardised. DSS01 has the relatively highest score (Level 2.96) and is closest to the target, followed by DSS05 (Level 2.43) and DSS02 (Level 2.43). Several sub-controls in DSS01 and DSS05 have already met the Level 3 (Established) target; however, certain sub-controls still require improvement, particularly in the areas of reporting and sensitive document management.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

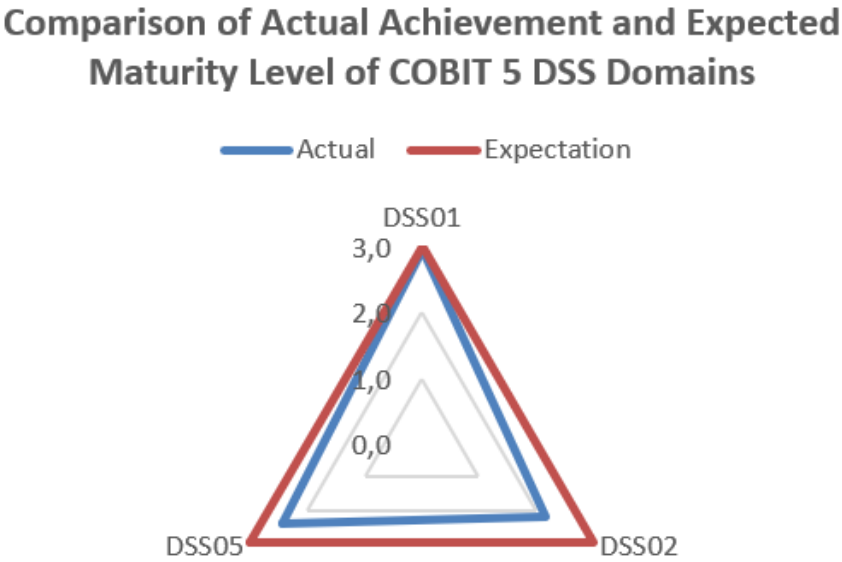

FIGURE 1. Comparison of Actual Achievement and Expected Maturity Level of COBIT 5 DSS Domains

Gap Analysis

The gap analysis compares the actual maturity level against the established target level. Table 8 presents the GAP per sub-control across all sub-domains.

TABLE 8. GAP Capability Level per Sub-Control

Domain	Sub-Control	Maturity Level	Target Level	GAP
DSS01	DSS01.01 – Perform operational procedures	3,20	3,00	+0,20
	DSS01.02 – Manage outsourced IT services	2,40	3,00	-0,60
	DSS01.03 – Monitor IT infrastructure	3,00	3,00	0,00
	DSS01.04 – Manage the environment	3,40	3,00	+0,40
	DSS01.05 – Manage facilities	2,80	3,00	-0,20
DSS02	DSS02.01 – Define incident classification	2,20	3,00	-0,80
	DSS02.02 – Record and prioritize incidents	2,00	3,00	-1,00
	DSS02.03 – Verify service requests	3,00	3,00	0,00

Domain	Sub-Control	Maturity Level	Target Level	GAP
	DSS02.04 – Investigate and allocate incidents	1,80	3,00	-1,20
	DSS02.05 – Resolve and recover	3,20	3,00	+0,20
	DSS02.06 – Close requests and incidents	1,60	3,00	-1,40
	DSS02.07 – Track and produce reports	1,40	3,00	-1,60
DSS05	DSS05.01 – Protect against malware	3,40	3,00	+0,40
	DSS05.02 – Network and connectivity security	2,40	3,00	-0,60
	DSS05.03 – Endpoint security	2,60	3,00	-0,40
	DSS05.04 – User identity and logical access	2,00	3,00	-1,00
	DSS05.05 – Physical access to IT assets	3,20	3,00	+0,20
	DSS05.06 – Sensitive documents management	1,80	3,00	-1,20
	DSS05.07 – Monitor security events	1,60	3,00	-1,40

The GAP analysis reveals that several sub-controls have reached or exceeded the Level 3 target: DSS01.01 (+0.20), DSS01.03 (0.00), DSS01.04 (+0.40), DSS02.03 (0.00), DSS02.05 (+0.20), DSS05.01 (+0.40), and DSS05.05 (+0.20). The largest remaining gaps are in DSS02.07 (Track and produce reports, GAP −1.60) and DSS02.06 (Close service requests, GAP −1.40). In DSS05, the largest gaps are in DSS05.06 (−1.20) and DSS05.07 (−1.40), reflecting the need for improvement in sensitive document management and proactive security monitoring.

Recommendations

Recommendations for DSS01 – Manage Operations

Sub-Domain	Sub-Control	Recommendation
DSS01	DSS01.02 – Manage outsourced IT services	Establish a written Service Level Agreement (SLA) with the Perbanas IT Directorate as the internal network vendor, covering minimum uptime (≥99%), incident response time (≤2 hours), and escalation procedures.
	DSS01.05 – Manage facilities	Conduct routine maintenance of IT supporting facilities, including periodic inspection of UPS units, cooling systems, and physical access controls to the server room. Develop a documented monthly maintenance checklist.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Recommendations for DSS02 – Manage Service Requests and Incidents

Sub-Domain	Sub-Control	Recommendation
DSS02	DSS02.01 – Define incident classification	Implement a web-based incident ticketing system (such as the free tier of Freshdesk or a Google Form integrated with Spreadsheet) to formally record all service requests and incidents, along with a classification scheme based on impact and urgency.
	DSS02.02 – Record and prioritize incidents	Establish internal resolution time targets (SLA): Critical <2 hours, High <4 hours, Medium <1 business day, Low <3 business days. Appoint an Incident Owner from the library IT staff with an escalation path to the IT Directorate.
	DSS02.04 – Investigate and allocate incidents	Develop documented incident investigation procedures, including initial diagnosis guidelines and mechanisms for allocating handling to the appropriate staff. Maintain active communication with users throughout the resolution process.
	DSS02.06 – Close requests and incidents	Establish a process for verifying and confirming incident closure with users, ensuring that every completed service request is recorded as closed with confirmation evidence from the requester.
	DSS02.07 – Track and produce reports	Prepare monthly incident summary reports for the Head of Library Division, covering the number of incidents, categories, average resolution times, and recurring incident trends as input for periodic evaluation.

Recommendations for DSS05 – Manage Security Services

Sub-Domain	Sub-Control	Recommendation
DSS05	DSS05.02 – Manage network security	Conduct periodic network security evaluations, including vulnerability assessments of the systems and networks used by LMIS, and implement documented firewall policies.
	DSS05.03 – Manage endpoint security	Establish security configuration standards for all endpoint devices (PCs, laptops, printers) connected to LMIS, including regular operating system updates and security patches.
	DSS05.04 – Manage user identity and logical access	Develop and formalise a Library Information Security Policy covering: password policy (minimum 8 characters, alphanumeric, renewal every 90 days), prohibition of account sharing, and implementation of Role-Based Access Control (RBAC) adhering to the principle of least privilege.
	DSS05.06 – Manage sensitive documents	Develop procedures for managing sensitive documents (membership data, borrowing history)

Sub-Domain	Sub-Control	Recommendation
		in accordance with the need-to-know principle, including data disposal procedures for records no longer required and classification of data confidentiality levels.
	DSS05.07 – Monitor security events	Activate and manage system activity logs (audit trail) to record all login activities, data modifications, and sensitive transactions, with a minimum retention period of 6 months. Implement an automated notification system for suspicious activities.

CONCLUSIONS

This study has conducted an information systems audit of LMIS Perbanas Institute using the COBIT 5 framework across three DSS sub-domains. The measurement results indicate that DSS01 (Manage Operations) achieved a Maturity Level of 2.96, DSS02 (Manage Service Requests and Incidents) reached Level 2.43, and DSS05 (Manage Security Services) reached Level 2.43. The overall average is 2.52, categorised as Managed (Level 2)—with an average gap of 0.48 towards the Level 3 (Established) target.

DSS02 is the most critical sub-domain, as incident handling is entirely informal with no recording system, categorisation scheme, or structured reporting. DSS05 exhibits an interesting pattern: physical protection is relatively adequate, but logical security policy and proactive monitoring aspects are very weak. DSS01 has the relatively best condition overall, yet still requires procedure standardisation and formalisation of SLAs with IT partners.

The primary recommendations produced include: implementation of an incident ticketing system, development of an information security policy, adoption of Role-Based Access Control (RBAC), standardisation of operational SOPs, activation of audit trails, and delivery of security awareness training. All recommendations are designed for phased implementation in line with the library's available resources. Future research is recommended to extend coverage to the APO and MEA domains, as well as to conduct a re-assessment following the implementation of these recommendations.

References

Iqbal Agselmora, D., Prasetyo Utomo, A., Stikubank Semarang, U., & Tri Lomba Juang Mugassari, J. (2022). Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(4). http://jurnal.

Ningsih, Y., Alyunita Mega Lestari, S., Kelana Sari, I., Andini, S., & Kaputama, S. (2024). Audit Sistem Informasi Pelayanan Perpustakaan Binjai Menggunakan Framework Cobit 5. *Jurnal Informatika Dan Sains Teknologi*, *1*(3).

Nuraeni, A., & Syarif Haryana, K. M. (2016). PENILAIAN TATA KELOLA TEKNOLOGI INFORMASI DENGAN MENAMBAHKAN UNSUR KEAMANAN MENGGUNAKAN FRAMEWORK COBIT 5 PADA DOMAIN DSS. *Jurnal Computech & Bisnis*, *10*(2), 89–105.

Panjaitan, E. N., & Zuraidah, E. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Audit Sistem Informasi Aplikasi Digipop OOH Menggunakan Framework Cobit 5. *Media Online)*, *4*(2), 864–876. https://doi.org/10.30865/klik.v4i2.1066

Randy Suryono, R., Darwis, D., & Indra Gunawan, S. (2018). AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 (STUDI KASUS: BALAI BESAR PERIKANAN BUDIDAYA LAUT LAMPUNG). In *Jurnal TEKNOINFO* (Vol. 12, Number 1).

Riyandi, A., Sudibyo, A., Wijonarko, B., Rinaldi, M., & Fahleyi, M. F. (2020). Analisa Audit Sistem Informasi Perpustakaan Menggunakan Cobit Frame Work. *Jurnal Sistem Dan Teknologi Informasi (Justin)*, *8*(3), 296. https://doi.org/10.26418/justin.v8i3.41167

Silalahi, A. G., Maharani, A., Abrianisyah, D. K., Dito Siregar, E., Sains, F., & Teknologi, D. (2024). *Audit Sistem Informasi Bebas Pustaka Menggunakan Framework Cobit-5 Domain DSS01 dan DSS02* (Vol. 3, Number 2). Online.

Suban, I. B., Wahju, A., & Emanuel, R. (2020). *Peran Framework ITIL V3 Mengukur Kualitas Layanan TI (Studi Kasus : Perpustakaan UAJY)*. *5*(2).