Tugas Kelompok	Dosen Pembimbing
Tata Kelola Teknologi Informasi	Teddie Darmizal, ST, MTI

AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 4.1

(STUDI KASUS: DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU)

UIN SUSKA RIAU

Oleh:

AGITRY WAHYU NUGRAHA	**11551102671**
DEDEH SARTIKA	**11551200570**
JIHAD BENASTEY	**11551102648**
RAHMAD NIRWANDI	**11551104702**

JURUSAN TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SULTAN SYARIEF KASIM RIAU

PEKANBARU

2019

A. MASALAH

Beberapa permasalahan berdasarkan hasil wawancara
• Pendaftaran anggota masih belum ada fitur pendaftaran secara *online* di aplikasinya • Tidak memiliki katalog *online* • Aplikasi tidak menyediakan fitur *booking* buku secara *online*

Dari beberapa permasalahan di atas dapat disimpulkan bahwa perlu di adakan perbaikan dalam bidang aplikasi.

B. BUSINESS GOALS

	No	**Business Goals**	**IT Goals**
Customer Perspective	4	*Improve Customer orientation and service*	3, 23

C. IT GOALS

No	**IT Goals**	**IT Process**
3	*Ensure satisfaction of end users with service offerings and service level.*	P08, AI4, DS1, DS2, DS7, DS8, DS10, DS13
23	*Make sure that IT services are available as required.*	DS3, DS4, DS8, DS13

D. IT PROCESS

IT Process	**COBIT IT Resources**			
	People	**Information**	**Application**	**Infrastructure**
PO8 ***Manage Quality***	✓	✓	✓	✓
AI4 ***Enable Operation and Use***	✓		✓	✓
DS1 ***Define and Manage Service Levels***	✓	✓	✓	✓

DS2 ***Manage Third-party Services***	✓	✓	✓	✓
DS3 ***Manage Performance and Capacity***			✓	✓
DS4 ***Ensure Continuous Service***	✓	✓	✓	✓
DS7 ***Educate and Train Users***	✓			
DS8 ***Manage Service Desk and Incidents***	✓		✓	
DS10 ***Manage Problems***	✓	✓	✓	✓
DS13 ***Manage Operations***	✓	✓	✓	✓

Dari sekian banyak IT *Process* kita mendapatkan IT *Process* yang berfokus pada penilaian dalam bidang *application* yaitu PO8, AI4, DS1, DS2, DS3, DS4, DS4, DS8, DS10, DS13

E. COBIT PROCESS

Penilaian akan menggunakan sub process dari setiap proses yang terpilih, dalam hal ini setiap sub process akan di seleksi sesuai dengan kebutuhan penilaian..

	Process	**Subprocess**
P08	***Manage Quality***	**PO8.1** ***Quality Management System*** **PO8.2** ***IT Standards and Quality Practices*** **PO8.3** ***Development and Acquisition Standards*** **PO8.4** ***Customer Focus*** **PO8.5** ***Continuous Improvement*** **PO8.6** ***Quality Measurement, Monitoring and Review***
AI4	***Enable Operation and Use***	**AI4.1** ***Planning for Operational Solutions*** **AI4.2** ***Knowledge Transfer to Business Management*** **AI4.3** ***Knowledge Transfer to End Users*** **AI4.4** ***Knowledge Transfer to Operations and Support Staff***
DS1	***Define and Manage Service Levels***	**DS1.1** ***Service Level Management Framework*** **DS1.2** ***Definition of Services*** **DS1.3** ***Service Level Agreements*** **DS1.4** ***Operating Level Agreements*** **DS1.5** ***Monitoring and Reporting of Service Level Achievements*** **DS1.6** ***Review of Service Level Agreements and Contracts***
DS2	***Manage Third-party Services***	**DS2.1** ***Identification of All Supplier Relationships*** **DS2.2** ***Supplier Relationship Management*** **DS2.3** ***Supplier Risk Management*** **DS2.4** ***Supplier Performance Monitoring***

DS3	***Manage Performance and Capacity***	**DS3.1** ***Performance and Capacity Planning*** **DS3.2** ***Current Performance and Capacity*** **DS3.3** ***Future Performance and Capacity*** **DS3.4** ***IT Resources Availability*** **DS3.5** ***Monitoring and Reporting***
DS4	***Ensure Continuous Service***	**DS4.1** ***IT Continuity Framework*** **DS4.2** ***IT Continuity Plans*** **DS4.3** ***Critical IT Resources*** **DS4.4** ***Maintenance of the IT Continuity Plan*** **DS4.5** ***Testing of the IT Continuity Plan*** **DS4.6** ***IT Continuity Plan Training*** **DS4.7** ***Distribution of the IT Continuity Plan*** **DS4.8** ***IT Services Recovery and Resumption*** **DS4.9** ***Offsite Backup Storage*** **DS4.10** ***Post-resumption Review***
DS8	***Manage Service Desk and Incidents***	**DS8.1** ***Service Desk*** **DS8.2** ***Registration of Customer Queries*** **DS8.3** ***Incident Escalation*** **DS8.4** ***Incident Closure*** **DS8.5** ***Reporting and Trend Analysis***
DS10	***Manage Problems***	**DS10.1** ***Identification and Classification of Problems*** **DS10.2** ***Problem Tracking and Resolution*** **DS10.3** ***Problem Closure*** **DS10.4** ***Integration of Configuration, Incident and Problem Management***
DS13	***Manage Operations***	**DS13.1** ***Operations Procedures and Instructions*** **DS13.2** ***Job Scheduling*** **DS13.3** ***IT Infrastructure Monitorin*** **DS13.4** ***Sensitive Documents and Output Devices*** **DS13.5** ***Preventive Maintenance for Hardware***

F. COBIT SUBPROCESS

NO	**Subprocess**	**Definition**
1	**PO8.1 Quality Management System**	Establish and maintain a QMS that provides a standard, formal and continuous approach regarding quality management that is aligned with business requirements. The QMS should identify quality requirements and criteria; key IT processes and their sequence and interaction; and the policies, criteria and methods for defining, detecting, correcting and preventing non-conformity. The QMS should define the organisational structure for quality management, covering the roles, tasks and responsibilities. All key areas should develop their quality plans in

		line with criteria and policies and record quality data. Monitor and measure the effectiveness and acceptance of the QMS, and improve it when needed
2	**PO8.2 IT Standards and Quality Practices**	Identify and maintain standards, procedures and practices for key IT processes to guide the organisation in meeting the intent of the QMS. Use industry good practices for reference when improving and tailoring the organisation's quality practices.
3	**PO8.3 Development and Acquisition Standards**	Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.
4	**PO8.4 Customer Focus**	Focus quality management on customers by determining their requirements and aligning them to the IT standards and practices. Define roles and responsibilities concerning conflict resolution between the user/customer and the IT organisation.
5	**PO8.5 Continuous Improvement**	Maintain and regularly communicate an overall quality plan that promotes continuous improvement.
6	**PO8.6 Quality Measurement, Monitoring and Review**	Define, plan and implement measurements to monitor continuing compliance to the QMS, as well as the value the QMS provides. Measurement, monitoring and recording of information should beused by the process owner to take appropriate corrective and preventive actions.
7	**AI4.1 Planning for Operational Solutions**	Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and

		maintain the automated solutions can exercise their responsibility.
8	**AI4.2 Knowledge Transfer to Business Management**	Transfer knowledge to business management to allow those individuals to take ownership of the system and data, and exercise responsibility for service delivery and quality, internal control, and application administration.
9	**AI4.3 Knowledge Transfer to End Users**	Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes.
10	**AI4.4 Knowledge Transfer to Operations and Support Staff**	Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.
11	**DS1.1 Service Level Management Framework**	Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.
12	**DS1.2 Definition of Services**	Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach.
13	**DS1.3 Service Level Agreements**	Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative

		metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.
14	**DS1.4 Operating Level Agreements**	Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.
15	**DS1.5 Monitoring and Reporting of Service Level Achievements**	Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.
16	**DS1.6 Review of Service Level Agreements and Contracts**	Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.
17	**DS2.1 Identification of All Supplier Relationships**	Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.
18	**DS2.2 Supplier Relationship Management**	Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs)

19	**DS2.3 Supplier Risk Management**	Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.
20	**DS2.4 Supplier Performance Monitoring**	Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.
21	**DS3.1 Performance and Capacity Planning**	Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources.
22	**DS3.2 Current Performance and Capacity**	Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.
23	**DS3.3 Future Performance and Capacity**	Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.

24	**DS3.4 IT Resources Availability**	Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.
25	**DS3.5 Monitoring and Reporting**	Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: • To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition • To report delivered service availability to the business, as required by the SLAs
26	**DS4.1 IT Continuity Framework**	Develop a framework for IT continuity to support enterprisewide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.
27	**DS4.2 IT Continuity Plans**	Develop IT continuity plans based on the framework and designed to reduce the

		impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.
28	**DS4.3 Critical IT Resources**	Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.
29	**DS4.4 Maintenance of the IT Continuity Plan**	Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.
30	**DS4.5 Testing of the IT Continuity Plan**	Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

31	**DS4.6 IT Continuity Plan Training**	Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.
32	**DS4.7 Distribution of the IT Continuity Plan**	Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.
33	**DS4.8 IT Services Recovery and Resumption**	Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.
34	**DS4.9 Offsite Backup Storage**	Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise’s media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.
35	**DS4.10 Post-resumption Review**	Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function

		after a disaster, and update the plan accordingly
36	**DS8.1 Service Desk**	Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritisation of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services.
37	**DS8.2 Registration of Customer Queries**	Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries.
38	**DS8.3 Incident Escalation**	Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.
39	**DS8.4 Incident Closure**	Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report

		unresolved incidents (known errors and workarounds) to provide information for proper problem management.
40	**DS8.5 Reporting and Trend Analysis**	Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.
41	**DS10.1 Identification and Classification of Problems**	Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorise problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organisational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff.
42	**DS10.2 Problem Tracking and Resolution**	Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering: •All associated configuration items •Outstanding problems and incidents •Known and suspected errors • Tracking of problem trends Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of

		the (RFC or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.
43	**DS10.3 Problem Closure**	Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.
44	**DS10.4 Integration of Configuration, Incident and Problem Management**	Integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements.
45	**DS13.1 Operations Procedures and Instructions**	Define, implement and maintain procedures for IT operations, ensuring that the operations staff members are familiar with all operations tasks relevant to them. Operational procedures should cover shift handover (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to support agreed-upon service levels and ensure continuous operations.
46	**DS13.2 Job Scheduling**	Organise the scheduling of jobs, processes and tasks into the most efficient sequence, maximising throughput and utilisation to meet business requirements.
47	**DS13.3 IT Infrastructure Monitoring**	Define and implement procedures to monitor the IT infrastructure and related events. Ensure that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.
48	**DS13.4 Sensitive Documents and Output Devices**	Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special purpose printers or security tokens.

49	**DS13.5 Preventive Maintenance for Hardware**	Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failures or performance degradation.

G. COBIT MATURITY LEVEL

Dengan adanya *maturity level model*, maka organisasi/perusahaan dapat mengetahui posisi kematangannya saat ini, dan secara terus menerus serta berkesinambungan harus berusaha untuk meningkatkan levelnya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan secara efektif. Untuk pengukuran tingkat *maturity level* perprosesnya dapat dilihat di COBIT 4.1.

Tingkat	Skala	Penjelasan
0	0.00 - 0.49	*Non existent* (tidak ada), merupakan posisi kematangan terendah, yang merupakan suatu kondisi di mana organisasi merasa tidak membutuhkan adanya mekanisme proses IT *Governance* yang baku, sehingga tidak ada sama sekali pengawasan terhadap IT *Governance* yang dilakukan oleh organisasi.
1	0.50 - 1.49	*Initial* (inisialisasi), sudah ada beberapa inisiatif mekanisme perencanaan, tata kelola, dan pengawasan sejumlah IT *Governance* yang dilakukan, namun sifatnya masih *ad hoc*, sporadis, tidak konsisten, belum formal, dan reaktif.
2	1.50 - 2.49	*Repeatable* (dapat diulang), kondisi di mana organisasi telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola IT *Governance* dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.
3	2.50 - 3.49	*Defined* (ditetapkan), pada tahapan ini prosedur telah distandardisasikan, didokumentasikan, serta dikomunikasikan melalui pelatihan. Namun, implementasinya diserahkan pada

		setiap individu, sehingga kemungkinan besar penyimpangan tidak dapat dideteksi. Prosedur tersebut dikembangkan sebagai bentuk formulasi dari praktik yang ada.
4	3.50 - 4.49	*Managed* (diatur), merupakan kondisi di mana manajemen organisasi telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor efektivitas pelaksanaan manajemen IT *Governance*.
5	4.50 - 5.00	*Optimised* (dioptimalisasi), level tertinggi ini diberikan kepada organisasi yang telah berhasil menerapkan prinsip-prinsip *governance* secara utuh dan mengacu *best practice*, di mana secara utuh telah diterapkan prinsip-prinsip *governance*, seperti *transparency*, *accountability*, *responsibility*, dan *fairness*.

H. IDENTIFIKASI MATURITY LEVEL

Pada penelitian ini, kami telah membagikan kuesioner yang diisi oleh responden dari Dinas Perpustakaan Dan Kearsipan Provinsi Riau yang sudah terlampir. Hasil yang diperoleh adalah sebagai berikut:

Proses COBIT	Pertanyaan	Maturity Level	Jumlah	Total	Status
PO8.1 Quality Management System	2	2+2	4	2	Repeatable
PO8.2 IT Standards and Quality Practices	2	2+3	5	2.5	Defined
PO8.3 Development and Acquisition Standards	2	4+4	8	4	Managed
PO8.4 Customer Focus	2	2+2	4	2	Repeatable
PO8.5 Continuous Improvement	1	1	1	1	Initial
PO8.6 Quality Measurement, Monitoring and Review	2	2+2	4	2	Repeatable
PO8 Manage Quality			26	2.25	Repeatable
AI4.1 Planning for Operational Solutions	2	3+3	6	3	Defined
AI4.2 Knowledge Transfer to Business Management	2	2+3	5	2.5	Defined
AI4.3 Knowledge Transfer to End Users	2	3+3	6	3	Defined
AI4.4 Knowledge Transfer to Operations and Support Staff	2	3+4	7	3.5	Managed
AI4 Enable Operation and Use			24	3	Defined
DS1.1 Service Level Management Framework	2	2+4	6	3	Defined
DS1.2 Definition of Services	1	1	1	1	Initial
DS1.3 Service Level Agreements	2	3+3	6	3	Defined
DS1.4 Operating Level Agreements	1	3	3	3	Defined
DS1.5 Monitoring and Reporting of Service Level Achievements	2	3+4	7	3.5	Managed
DS1.6 Review of Service Level Agreements and Contracts	1	3	3	3	Defined
DS1 Define and Manage Service Levels			26	2.75	Defined

DS2.1 Identification of All Supplier Relationships	2	3+3	6	3	Defined
DS2.2 Supplier Relationship Management	2	3+2	5	2.5	Defined
DS2.3 Supplier Risk Management	2	3+4	7	3.5	Defined
DS2.4 Supplier Performance Monitoring	1	3	3	3	Defined
DS2 Manage Third-party Services			21	3	Defined
DS3.1 Performance and Capacity Planning	2	2+3	5	2.5	Defined
DS3.2 Current Performance and Capacity	1	2	2	2	Repeatable
DS3.3 Future Performance and Capacity	2	3+3	6	3	Defined
DS3.4 IT Resources Availability	1	3	3	3	Defined
DS3.5 Monitoring and Reporting	2	3+3	6	3	Defined
DS3 Manage Performance and Capacity			22	2.7	Defined
DS4.1 IT Continuity Framework	2	2+0	2	1	Initial
DS4.2 IT Continuity Plans	2	3+1	4	2	Repeatable
DS4.3 Critical IT Resources	2	1+0	1	0.5	Initial
DS4.4 Maintenance of the IT Continuity Plan	2	1+1	2	1	Initial
DS4.5 Testing of the IT Continuity Plan	2	1+3	4	2	Repeatable
DS4.6 IT Continuity Plan Training	2	3+3	6	3	Defined
DS4.7 Distribution of the IT Continuity Plan	2	3+0	3	1.5	Repeatable
DS4.8 IT Services Recovery and Resumption	2	3+3	6	3	Defined
DS4.9 Offsite Backup Storage	2	3+3	6	3	Defined
DS4.10 Post-resumption Review	2	3+3	6	3	Defined
DS4 Ensure Continuous Service			40	2	Repeatabe
DS8.1 Service Desk	2	3+4	7	3.5	Managed
DS8.2 Registration of Customer Queries	1	2	2	2	Repeatable
DS8.3 Incident Escalation	1	3	3	3	Defined
DS8.4 Incident Closure	1	3	3	3	Defined
DS8.5 Reporting and Trend Analysis	1	4	4	4	Managed
DS8 Manage Service Desk and Incidents			19	3.1	Defined

DS10.1 Identification and Classification of Problems	1	2	2	2	Repeatable
DS10.2 Problem Tracking and Resolution	2	3+3	6	3	Defined
DS10.3 Problem Closure	1	4	4	4	Managed
DS10.4 Integration of Configuration, Incident and Problem Management	1	3	3	3	Defined
DS10 Manage Problems			15	3	Defined
DS13.1 Operations Procedures and Instructions	2	3+3	6	3	Defined
DS13.2 Job Scheduling	2	3+3	6	3	Defined
DS13.3 IT Infrastructure Monitorin	2	3+5	8	4	Managed
DS13.4 Sensitive Documents and Output Devices	2	4+5	9	4.5	Optimised
DS13.5 Preventive Maintenance for Hardware	2	4+4	8	4	Managed
DS13 Manage Operations			37	3.7	Managed

BUSINESS GOALS	**PERHITUNGAN**	**JUMLAH**
4	$\frac{TOTAL\ POIN\ MATURITY}{TOTAL\ PERTANYAAN}$	2,84

IT GOALS	**PERHITUNGAN**	**JUMLAH**
3	$\frac{TOTAL\ POIN\ MATURITY\ IT\ GOALS}{TOTAL\ PERTANYAAN}$	3,01
23	$\frac{TOTAL\ POIN\ MATURITY\ IT\ GOALS}{TOTAL\ PERTANYAAN}$	2,86
	Rata-rata	2.935

Business goals adalah total poin *maturity* level yang di ceklis dibagi total pertanyaan. *IT goals* adalah total poin *maturity* level proses di *IT goals* dibagi total pertanyaan proses di *IT goals.*

Dari tabel diatas dapat diketahui bahwa *maturity level* dari tabel *Business Goals* adalah 2.84 berada pada level *Defined* dan *maturity level* dari tabel *IT Goals* adalah 2.935 juga berada pada level *Defined.*

I. KESIMPULAN

Adapun didapat kesimpulan dari proses audit yang sudah dilakukan di Dinas Perpustakaan dan Kearsipan Provinsi Riau dengan pokok permasalahan IT yang terletak pada aplikasi adalah sebagai berikut :

1. Banyaknya aktivitas yang masih dilakukan secara manual ataupun aktivitas yang tersedia tidak didukung oleh aplikasi yang ada sehingga dapat menurunkan efektivitas kinerja yang ada pada Dinas Perpustakaan dan Kearsipan Provinsi Riau.
2. Dinas Perpustakaan dan Kearsipan Provinsi Riau kurang dalam layanan TI untuk mengatasi masalah dalam waktu yang cepat dan belum adanya persiapan bila terjadi bencana atau kerusakan.
3. Dinas Perpustakaan dan Kearsipan Provinsi Riau belum dapat menyelaraskan kualitas pada pelanggan dan belum menetapkan target pelayanan untuk pelanggan.

J. SARAN

Adapun saran yang dapat kami berikan adalah :

1. Menyediakan *software* atau aplikasi yang dibutuhkan untuk mendukung efektivitas kinerja yang ada pada Dinas Perpustakaan dan Kearsipan Provinsi Riau.
2. Menyediakan layanan TI untuk mengatasi masalah dalam waktu yang cepat, persiapan bila terjadi bencana dan kerusakan dengan mem-*backup* data secara berkala.
3. Menyediakan kualitas dan target pelayanan untuk pelanggan dengan adanya perbaikan dalam aplikasi.