

## AUDIT SISTEM INFORMASI PERPUSTAKAAN UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR MENGGUNAKAN FRAMEWORK COBIT 5

Fahrullah<sup>1</sup>, Dewi Agushinta R<sup>2</sup>,

<sup>1</sup>Magister Teknik Informatika Universitas AMIKOM Yogyakarta

fahrullah@spb.ac.id,

<sup>2</sup>Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadharma

dewiar@gmail.com,

### ABSTRAK

Universitas Muhammadiyah Kalimantan Timur telah menerapkan penggunaan teknologi informasi sebagai penunjang dalam hal pelayanan akademik yang diperuntukan bagi seluruh civitas akademika, salah satu sistem informasi yang telah diterapkan adalah sistem informasi perpustakaan yang ditangani oleh Perpustakaan Universitas Muhammadiyah Kalimantan Timur. Untuk mengatur sistem informasi itu sendiri memerlukan audit yang bertujuan untuk mengevaluasi dan memastikan pemenuhannya ditinjau dari pendekatan objektif dari suatu standar. Sistem Informasi Perpustakaan di Universitas Muhammadiyah Kalimantan Timur memerlukan audit untuk mengevaluasi, menilai kapabilitas, dan menyusun rekomendasi terhadap sistem informasi yang dipakai. *Framework* audit yang digunakan adalah COBIT 5 domain DSS (*Deliver, Service, dan Support*) yang fokus pada penilaian pengiriman dan layanan teknologi informasi serta dukungannya termasuk pengelolaan masalah agar keberlanjutan layanan tetap terjaga.

**Kata Kunci:** audit, COBIT 5, domain DSS, Sistem Informasi Perpustakaan, Universitas Muhammadiyah Kalimantan Timur.

### I. PENDAHULUAN

Saat ini Teknologi informasi (TI) menjadi suatu bagian yang sangat penting bagi perusahaan atau lembaga – lembaga yang berskala *enterprise*. Perusahaan atau lembaga menempatkan teknologi sebagai suatu hal yang dapat mendukung pencapaian rencana strategis perusahaan untuk mencapai sasaran visi, misi dan tujuan perusahaan atau lembaga tersebut. Perusahaan atau lembaga tersebut berupaya untuk menerapkan suatu sistem informasi yang dapat memenuhi kebutuhan perusahaan dalam mencapai tujuannya misalnya untuk meningkatkan kegiatan operasional kerja. Fungsi teknologi

informasi tidak hanya untuk meningkatkan operasional kerja tetapi juga memberi nilai tambah dan keuntungan kompetitif.

Sistem informasi perpustakaan merupakan sebuah sistem terintegrasi untuk menyediakan informasi yang mengandung operasi, manajemen, dan fungsi pengambilan keputusan dalam suatu perpustakaan.

Audit teknologi informasi memiliki beberapa standar yang digunakan untuk penelitian. Contoh standar tersebut adalah ITIL dan COBIT 5. ITIL memiliki fokus pada layanan untuk pelanggan dan tidak memberikan proses penyesuaian strategi perusahaan terhadap strategi teknologi

informasi yang dikembangkan. COBIT 5 merupakan standar komprehensif yang membantu perusahaan dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif. COBIT 5 menyediakan kerangka kerja *IT Governance* dan *control objectives* yang rinci bagi manajemen, pemilik proses bisnis, pemakai dan *auditor*, karena mengelola teknologi informasi secara menyeluruh sehingga nilai yang diberikan oleh teknologi informasi dapat tercapai optimal dengan memperhatikan segala aspek tata kelola teknologi informasi mulai dari sisi *people, skills, competencies, services, infrastructure*, dan *applications* yang merupakan bagian dari *enabler* suatu tata kelola teknologi informasi. COBIT 5 menyediakan kerangka kerja yang lengkap. Terdapat 5 domain dan 37 proses pada COBIT 5 yang dapat digunakan untuk melakukan audit. Maka dari itu COBIT 5 dianggap sesuai dan dapat membantu dalam proses audit teknologi informasi karena mencakup semua elemen pada teknologi informasi yang dipakai.

## II. LANDASAN TEORI

### 2.1 Sistem

Menurut Swastika, I Putu Agus (2016:3), Kata 'sistem' mengandung arti 'kumpulan dari komponen-komponen yang memiliki unsur keterkaitan antara satu dan lainnya'. [1]

### 2.2 Informasi

Menurut Swastika, I Putu Agus (2016:2), Definisi kata 'Informasi' sendiri secara internasional telah disepakati sebagai 'hasil dari pengolahan data' yang secara prinsip memiliki nilai yang lebih dibandingkan dengan data mentah. [1]

### 2.3 Sistem Informasi

Menurut Swastika, I Putu Agus (2016:3), "Sistem informasi merupakan suatu kumpulan dari komponen-komponen dalam perusahaan atau organisasi yang

berhubungan dengan proses penciptaan dan pengaliran informasi. [1]

### 2.4 Audit

Menurut Hall, James A. and Singeton, Tommie (2007:2), "Audit adalah proses sistematis mengenai mendapatkan dan mengevaluasi secara objektif (bukti yang berkaitan dengan penilaian mengenai berbagai kegiatan dan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara penilaian-penilaian tersebut dan membentuk kriteria serta menyampaikan hasilnya ke para pengguna yang berkepentingan" [2].

### 2.5 Audit Sistem Informasi

Menurut Swastika, I Putu Agus (2016:1), "Audit sistem informasi merupakan suatu cara untuk menilai sejauh mana suatu sistem informasi telah mencapai tujuan organisasi. [1]

### 2.6 COBIT

Menurut Sarno (2009), "COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengatur keselarasan TI dengan bisnis. Selain itu, kerangka kerja juga memastikan bahwa TI memungkinkan bisnis, memaksimalkan keuntungan, resiko TI dikelola secara tepat, dan sumber daya TI digunakan secara bertanggung jawab". [3] COBIT adalah salah satu framework yang digunakan untuk standar audit, COBIT merupakan standar yang dinilai lengkap dan cakupan yang menyeluruh sebagai framework audit. COBIT dikembangkan secara berkala oleh ISACA. Didalam COBIT ini terdapat beberapa Domain yang digunakan untuk proses audit.

### 2.7 Pemetaan Hubungan *Enterprise Goals, IT – Related Goals, dan Proses control*

Pemetaan hubungan ini digunakan untuk melakukan penilaian tingkat kapabilitas, beberapa tahap hubungan pemetaan tersebut diantaranya adalah:

- 1) Pemetaan *Enterprise Goals* dengan tujuan perusahaan.

Pemetaan dilakukan ke dalam perspektif *IT Balanced Scorecard (IT BSC)*. Jika hubungan keterkaitan antara tujuan perusahaan yang menjadi objek dengan *enterprise goals* pada COBIT 5 sangat kuat, maka diberi tanda “P” yang berarti *primary*. Jika terdapat hubungan yang tidak dominan, maka diberi tanda “S” yang berarti *secondary*. Jika tidak ada hubungan sama sekali maka dikosongkan.

| BSC Dimension       | Enterprise Goal                                       | Relation to Governance Objectives |                   |                      |
|---------------------|-------------------------------------------------------|-----------------------------------|-------------------|----------------------|
|                     |                                                       | Benefits Realization              | Risk Optimization | Resource Utilization |
| Financial           | 1. Stakeholder value of business investments          | P                                 |                   | S                    |
|                     | 2. Portfolio of competitive products and services     |                                   | P                 | S                    |
|                     | 3. Managed business risk (safeguarding of assets)     |                                   | P                 | S                    |
|                     | 4. Compliance with external laws and regulations      |                                   | P                 |                      |
| Customer            | 5. Financial transparency                             | P                                 | S                 | S                    |
|                     | 6. Customer-oriented service culture                  |                                   |                   | S                    |
|                     | 7. Business service continuity and availability       |                                   | P                 |                      |
|                     | 8. Agile responses to a changing business environment | P                                 |                   | S                    |
| Internal            | 9. Information-based strategic decision making        | P                                 | P                 | P                    |
|                     | 10. Optimization of service delivery costs            | P                                 |                   | P                    |
|                     | 11. Optimization of business process functionality    | P                                 |                   | P                    |
|                     | 12. Optimization of business process costs            | P                                 |                   | P                    |
|                     | 13. Managed business change programmes                | P                                 | P                 | S                    |
|                     | 14. Operational and staff productivity                | P                                 |                   | P                    |
|                     | 15. Compliance with internal policies                 |                                   | P                 | P                    |
| Learning and Growth | 16. Skilled and motivated people                      | S                                 | P                 | P                    |
|                     | 17. Product and business innovation culture           | P                                 |                   |                      |

Gambar 1. Pemetaan *enterprise goals* dengan tujuan perusahaan

2) Pemetaan *enterprise goals* dengan *IT – Related Goals*.

Pemetaan yang dilakukan pada hubungan sama dengan yang dilakukan pada hubungan *enterprise goals* dengan Tujuan perusahaan. Jika hubungan keterkaitan antara *IT – Related Goals* yang menjadi objek dengan *enterprise goals* yang terpilih pada COBIT 5 sangat kuat, maka diberi tanda “P” yang berarti *primary*. Jika terdapat hubungan yang tidak dominan, maka diberi tanda “S” yang berarti *secondary*. Jika tidak ada hubungan sama sekali maka dikosongkan.

|                     | Enterprise Goal | IT-related Goal |   |   |          |   |   |          |  |  |                     |  |  |  |  |  |  |  |
|---------------------|-----------------|-----------------|---|---|----------|---|---|----------|--|--|---------------------|--|--|--|--|--|--|--|
|                     |                 | Financial       |   |   | Customer |   |   | Internal |  |  | Learning and Growth |  |  |  |  |  |  |  |
| Financial           | 01              | P               | P | S |          |   |   |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 02              |                 |   |   | P        |   |   |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 03              |                 |   |   | P        | S | P |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 04              |                 |   |   | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 05              |                 |   |   | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
| Customer            | 06              |                 |   |   | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 07              |                 |   |   | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 08              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 09              |                 |   |   | S        | P | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 10              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
| Internal            | 11              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 12              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 13              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 14              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 15              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
| Learning and Growth | 16              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                     | 17              |                 |   |   | S        | S | S |          |  |  |                     |  |  |  |  |  |  |  |

Gambar 2. Pemetaan *enterprise goals* dengan *IT-Related Goals*

3) Pemetaan *IT – Related Goals* dengan Proses domain DSS

Pemetaan ini dilakukan untuk mendapat proses-proses domain DSS mana sajakah yang masuk dalam ruang kegiatan audit. Setiap tujuan TI memiliki masing-masing proses TI yang relevan. Setelah dilakukan *mapping* terhadap tujuan bisnis perusahaan dengan tujuan TI, selanjutnya dilakukan *mapping* tujuan TI dengan proses TI.

|                               | IT-related Goal | COBIT 5 Process |   |   |          |   |   |          |  |  |                     |  |  |  |  |  |  |  |
|-------------------------------|-----------------|-----------------|---|---|----------|---|---|----------|--|--|---------------------|--|--|--|--|--|--|--|
|                               |                 | Financial       |   |   | Customer |   |   | Internal |  |  | Learning and Growth |  |  |  |  |  |  |  |
| Business and Environment      | BAK1            | P               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK2            | P               | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK3            | S               | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK4            | S               | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK5            | S               | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK6            |                 | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK7            |                 | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK8            |                 | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK9            |                 | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
|                               | BAK10           |                 | S | S | S        | P | S | S        |  |  |                     |  |  |  |  |  |  |  |
| Data and Information          | DAK1            | P               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DAK2            | P               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DAK3            | S               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DAK4            | P               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DAK5            | S               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DAK6            | P               | S | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
| Delivery, Service and Support | DSS01           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DSS02           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DSS03           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DSS04           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DSS05           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |
|                               | DSS06           | S               | P | S | P        | S | S |          |  |  |                     |  |  |  |  |  |  |  |

Gambar 3. Pemetaan *IT-Related Goals* dengan Proses Domain DSS

### 2.8 Diagram RACI

Diagram RACI adalah bagian dari *Responsibility Assignment Matrix (RAM)*, yaitu bentuk pemetaan antara sumberdaya dengan aktivitas dalam setiap prosedur.

RACI merupakan singkatan dari R (*Responsible*), A (*Accountable*), C (*Consulted*), dan I (*Informed*). Untuk melakukan penilaian dengan domain DSS, maka dilakukan mapping antara *sub control objectives* dan sumber daya manusia yang ada pada pelaksanaan sistem informasi.

Berikut contoh dari diagram RACI pada DSS05:

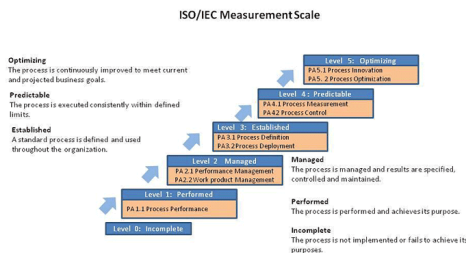
| Key Management Practice                                         | Head | Chief Financial Officer | Chief Information Officer | Chief Privacy Officer | Business Executive | Business Process Owner | Business Process Controller | Business Process Analyst | Business Process Designer | Business Process Tester | Business Process Auditor | Business Process Monitor | Business Process Reviewer | Business Process Approver | Business Process Signer | Business Process Approver | Business Process Signer |
|-----------------------------------------------------------------|------|-------------------------|---------------------------|-----------------------|--------------------|------------------------|-----------------------------|--------------------------|---------------------------|-------------------------|--------------------------|--------------------------|---------------------------|---------------------------|-------------------------|---------------------------|-------------------------|
| 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 digital devices         |      |                         |                           |                       |                    |                        |                             |                          |                           |                         |                          |                          |                           |                           |                         |                           |                         |
| DSS05.07 Monitor the infrastructure for security-related events |      |                         |                           |                       |                    |                        |                             |                          |                           |                         |                          |                          |                           |                           |                         |                           |                         |

Gambar 4. Diagram RACI

Mapping tersebut dilakukan untuk seluruh *control objective* yang ada pada domain DSS. Dalam *mapping* tersebut diberi suatu nilai berupa *Responsible/Accountable/Consulted/Informed*

### 2.9 Proses Capability Model

ISO/IEC 15504-2 mendefinisikan pengukuran untuk penilaian kemampuan proses dari framework COBIT. *Process capability* didefinisikan pada 6 level poin dari 0 sampai 5, yang mempresentasikan peningkatan *capability* dari proses yang diimplementasikan.



This figure is reproduced from ISO/IEC 15504-2, with the permission of ISO/IEC at www.iso.org. Copyright remains with ISO/IEC.

Gambar 5. Level Capability

Berikut adalah penjelasan level dari *process capability*:

- Level 0 (Incomplete)**  
Proses tidak melaksanakan atau gagal untuk mencapai tujuan proses. Pada tingkat ini, ada sedikit atau tidak sama sekali bukti (*evidence*) dari setiap pencapaian tujuan proses.
- Level 1 (Perfomed)**  
Proses diimplementasikan untuk mencapai tujuan bisnisnya.
- Level 2 (Managed)**  
Proses yang diimplementasikan dikelola (*plan, monitor, and adjusted*) dan hasilnya ditetapkan dan dikontrol.
- Level 3 (Established)**  
Proses didokumentasikan dan dikomunikasikan (untuk efisiensi organisasi).
- Level 4 (Predictable)**  
Proses dimonitor, diukur, dan diprediksi untuk mencapai hasil.
- Level 5 (Optimizing)**  
Sebelumnya proses telah di prediksi kemudian ditingkatkan untuk memenuhi tujuan bisnis yang relevan dan tujuan yang akan datang.

Setiap proses yang dinilai akan menghasilkan 4 level rating point, yaitu:

- Not achieved*, apabila hasil penilaian antara 0% - 15%
- Partially achieved*, apabila hasil penilaian >15% - 50%
- Largely achieved*, apabila hasil penilaian >50% - 85%
- Fully achieved*, apabila hasil penilaian >85% - 100%

## III. METODOLOGI PENELITIAN

### 3.1 Jenis, Sifat dan Pendekatan Penelitian

Sifat dari penelitian ini adalah deskriptif, yaitu prosedur pemecahan masalah yang diselidiki dengan menggambarkan/melukiskan keadaan subyek/obyek

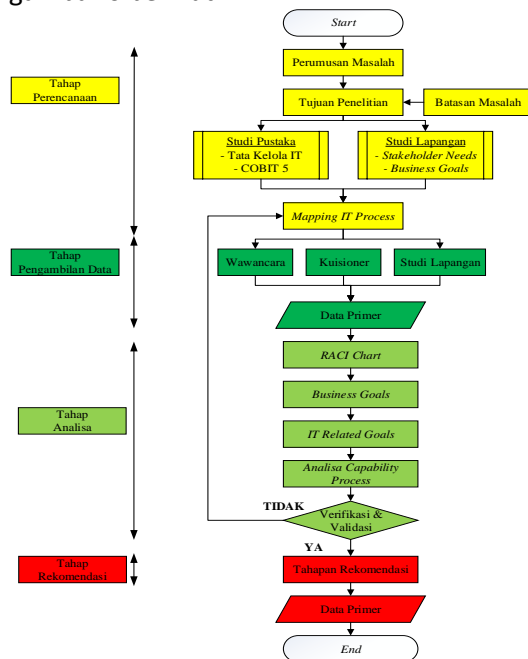
penelitian (seseorang, lembaga, masyarakat dan lain-lain) pada saat sekarang berdasarkan fakta-fakta yang tampak atau sebagaimana adanya. Data yang dikumpulkan berupa kata-kata, gambar, dan bukan angka-angka. Data tersebut mungkin berasal dari naskah wawancara, catatan-lapangan, foto, video *tape*, dokumen pribadi, catatan atau memo, dan dokumen resmi lainnya. Untuk memperoleh sampel dari populasi yang ada digunakan model RACI.

### 3.2 Metode Analisis Data

Secara keseluruhan penelitian ini menggunakan teknik analisis data secara deskriptif-kuantitatif. Desain deskriptif-kuantitatif yang digunakan, yaitu desain deskriptif kuisioner.

### 3.3 Alur Penelitian

Adapun alur penelitian terdapat pada gambar 6 berikut ini:



Gambar 6. Alur penelitian

## IV. IMPLEMENTASI

### 4.1 Pengumpulan Evidence dan kondisi existing

#### 4.1.1 Pengumpulan dan deskripsi Evidence

Dalam penentuan suatu kondisi yang di dapat sudah valid atau belum, dalam audit ini dilakukan dengan pengumpulan bukti-bukti yang sudah ditetapkan pada COBIT 5 Domain DSS (*Deliver, Service, and Support*). Hasil bukti yang di dapat diperiksa dengan kesesuaian kondisi *existing* yang telah dapat dan menjadi alat ukur tersendiri.

#### 4.1.2 Penilaian kondisi existing

##### 4.1.2.1 Kondisi Existing DSS01

Berdasarkan audit yang dilakukan pada domain DSS, maka didapatkan kondisi *existing* dari DSS01:

- 1) Dalam menjalankan prosedur operasional telah dilakukan dengan baik, dan ada beberapa aktivitas-aktivitas tertulis di *Standard Operating Procedure (SOP)* dan *roadmap* yang berdasarkan kalender akademik.
- 2) Dalam *manage enviroentment* Perpustakaan UMKT menjalankan kehendak sesuai dengan yang di tetapkan oleh HRD.
- 3) Dalam menjaga fasilitas yang dimiliki, tidak ada penilaian terhadap fasilitas yang ada.

##### 4.1.2.2 Kondisi Existing DSS02

- 1) Dalam menjalankan layanan insiden dan permintaan layanan telah dibuatkan skema layanan/ SOP tentang request insiden.
- 2) Aplikasi sistem informasi yang dimiliki Perpustakaan UMKT dapat digunakan dalam merekap insiden-insiden yang terjadi, laporan insiden yang terjadi, laporan status insiden yang sedang dikerjakan, dan laporan insiden yang sudah selesai.

##### 4.1.2.3 Kondisi Existing DSS03

- 1) Perpustakaan UMKT melakukan pengklasifikasian terhadap permasalahan yang muncul, dan tertulis dalam SLA
- 2) Terdapat pencatatan dari kejadian error terhadap Sistem Informasi

Perpustakaan, dan juga dilaporkan saat rapat besar 3 bulan Perpustakaan UMKT

- 3) Dalam menyelesaikan masalah dan menutup masalah dikomunikasikan dalam RTM dan dilakukan dengan baik, direkap dan dijaga dengan baik.

#### **4.1.2.4 Kondisi Existing DSS04**

- 1) Perpustakaan UMKT membuat antisipasi terhadap gangguan dari skenario insiden yang ada dengan meresolusi gangguan secara teknis dan menyelesaikan gangguan non teknis dengan kebijakan.
- 2) Tidak dilakukannya *Bussines Plan Continuity* untuk pengembangan implementasi proses bisnis di Perpustakaan UMKT, hal ini sedang dalam tahap perencanaan, belum berlangsung.
- 3) Adanya pelatihan yang dilakukan terhadap staff untuk pengembangan skill setiap 1 tahun sekali. Hasil pelatihan dilaporkan dalam bentuk laporan kegiatan.

#### **4.1.2.5 Kondisi existing DSS05**

- 1) Melakukan riset terhadap ancaman-ancaman yang potensial.
- 2) Terdapat pemantauan dari aktifitas pengaksesan pada sistem informasi perpustakaan.
- 3) Setiap perangkat sensitif dan perangkat-perangkat yang ada di inventarisasi dengan baik kebagian rumah tangga dan umum.
- 4) Terdapat penentuan karakteristik keamanan dalam memonitoring keamanan infrastruktur yang di tentukan dalam rapat dan terdapat *security incident ticket* dalam sistem informasi *helpdesk*.

#### **4.1.2.6 Kondisi Existing DSS06**

- 1) Penyelarasan aktivitas kontrol yang ada di proses bisnis dengan tujuan Perpustakaan UMKT sudah berlangsung

baik. Dilengkapi laporan tinjauan dan juga analisis terhadap akar permasalahan yang muncul

- 2) Peran, tanggungjawab, hak akses dan level otoritas telah didefinisikan dan terdokumentasi dalam sistem *dashboard* yang bersifat *private*.
- 3) Telah dilakukannya koreksi yang dilakukan oleh pihak BPM untuk mengetahui kesalahan-kesalahan kemudian dianalisis dan dilaporkan saat RTM.
- 4) Terdapat rekaman di sistem informasi *helpdesk* yang dapat digunakan untuk memastikan jejak kegiatan informasi dan pertanggung jawabannya.

#### **4.1.3 Analisis Hasil Kuisiner**

Dalam menentukan kondisi pada level manakah aktifitas-aktifitas yang terdapat pada form kerja audit itu berada, maka dilakukan analisis berupa mencari level yang tepat pada form hasil kuisiner. Penentuan level di tiap aktifitas ini dilakukan dengan memilih nilai modus atau nilai yang paling banyak muncul pada tiap aktifitasnya. Dan apabila nilai yang muncul itu terdapat 2 level atau mungkin lebih, maka yang di pilih adalah nilai level yang terkecil diantaranya, misalkan pada DSS01-01 pada aktifitas ke 3 terdapat 9 responden, kemudian dari 9 responden yang memilih di level 2 adalah 4 orang, di level 4 adalah 4 orang, dan di level 5 adalah 1 orang. Maka level yang terpilih adalah pada level 3, karena diartikan juga berarti 4 orang yang memilih di level 4 tersebut juga merasa bahwa pada aktifitas ke 3 telah berada pada level 3.

##### **4.1.3.1 Rekapitulasi Nilai Capability**

Setelah dilakukan analisis hasil kuisiner maka di dapatkanlah hasil nilai-nilai pada tiap aktifitas yang ada pada domain DSS (*Deliver, service, and Support*) dan di masukan ke dalam form kerja audit.

Tindakan selanjutnya yang dilakukan adalah mencari rata-rata nilai pada tiap proses untuk mengetahui bagaimana kondisi tiap proses yang ada. Berikut adalah hasil rekapitulasi nilai proses pada domain DSS:

Tabel 1. Rekapitulasi nilai capability

| Proses Domain                                             | Level rata-rata | Pembulatan level |
|-----------------------------------------------------------|-----------------|------------------|
| DSS-01 Mengelola operasi                                  | 3,82            | 3                |
| DSS-02 Mengelola permintaan layanan dan mengelola insiden | 4,29            | 4                |
| DSS-03 Mengelola masalah                                  | 3,69            | 3                |
| DSS-04 Mengelola keberlanjutan                            | 3,4             | 3                |
| DSS-05 Mengelola layanan keamanan                         | 3,4             | 3                |
| DSS-06 Mengelola kontrol-kontrol proses bisnis            | 3,06            | 3                |

Dari *Capability level* yang didapat 4.36 dilakukan pembulatan untuk memudahkan mencari kondisi terkini berdasarkan kriteria *capability level* yang telah ditetapkan.

Dalam melakukan pembulatan tersebut menggunakan konsep penentuan *capability process* tertentu, yaitu suatu proses akan mencapai level k jika semua atribut sebelum level k terpenuhi secara *fully achieved* dan semua atribut di level k telah terpenuhi secara *largely* (>50% hingga 85%) atau *fully achieved* (>85%). Disini penulis menggunakan pilihan yang terpenuhi secara *fully achieved* atau level terpenuhi dengan nilai >85%, yang di rasa akan lebih akurat dalam menilai atau menggambarkan kondisi yang *existing* yang ada.

#### 4.2 Analisis Gap

Analisis *gap* ini dilakukan untuk mencari selisih dari *level capability* yang didapat dengan level target yang ingin dicapai. Dalam penentuan level target, ditentukan dengan level yang sedang dituju dari level

rata-rata yang didapat. Contoh untuk DSS01 di peroleh level rata-rata 3,82 maka DSS01 sedang dalam tahap menuju level capability 4 dan masih mencapai 0,82 atau 82% di atas level 3 atau kurang dari 0,18 atau 18% menuju level capability 4. Sehingga ditetapkan level targetnya adalah level 4.

##### 4.2.1 Analisis keseluruhan Gap

Berikut ini adalah hasil dari pelaksanaan audit, diperolehnya hasil *capability level* untuk keseluruhan proses adalah sebagai berikut:

Tabel 2. Analisis keseluruhan *gap*

| Proses Domain                                             | Level Existing | Level Target | Gap |
|-----------------------------------------------------------|----------------|--------------|-----|
| DSS-01 Mengelola operasi                                  | 3              | 4            | 1   |
| DSS-02 Mengelola permintaan layanan dan mengelola insiden | 4              | 5            | 1   |
| DSS-03 Mengelola masalah                                  | 3              | 4            | 1   |
| DSS-04 Mengelola keberlanjutan                            | 3              | 4            | 1   |
| DSS-05 Mengelola layanan keamanan                         | 3              | 4            | 1   |
| DSS-06 Mengelola kontrol-kontrol proses bisnis            | 3              | 4            | 1   |

#### 4.3 Rekomendasi

##### 4.3.1 Rekomendasi DSS01

Berdasarkan analisis *gap* pada DSS01, maka berikut adalah beberapa rekomendasi:

- 1) Menindak lanjuti hasil audit independent terhadap kualitas layanan, lingkungan dan dengan pihak luar yang menjalin kerjasama, apabila dari audit independent tidak ada maka ditambahkan sendiri.
- 2) Melakukan analisis perangkat IT untuk mencegah ancaman yang timbul dari tindakan manusia seperti pencurian, dan juga terlindung dari ancaman dari hal-hal lain misalkan kebocoran, akan hujan, bahaya kebakaran karena korsleting dll.

- 3) Melakukan penilaian terhadap infrastruktur yang dimiliki dan dibuat dokumentasinya untuk bahan evaluasi kedepan.
- 4) Menjaga dan memonitoring infrastruktur dengan baik, karena telah disediakan CCTV namun tidak ada yang mengoperasikannya, lebih baik disediakan staff yang bertugas untuk memonitoringnya, misalkan satpam.

#### 4.3.2 Rekomendasi DSS02

Berdasarkan analisis *gap* pada DSS02, maka berikut adalah beberapa rekomendasi:

- 1) Membuat klasifikasi terhadap jenis-jenis layanan dan insiden yang dilayani, sehingga mudah untuk dipetakan ke bagian atau divisi yang akan langsung menyelesaikan layanan atau insiden tersebut.
- 2) Membuat strategi-strategi dalam permintaan layanan dan pemecahan insiden baik dalam bentuk kebijakan ataupun tindakan penanganan langsung seperti sistem.
- 3) Melakukan review terhadap SLA yang dibuat minimal tiap satu tahun untuk mengetahui ketidaksesuaian yang terjadi dan melakukan inovasi terhadap SLA yang sudah ada.
- 4) Memberikan wadah untuk kritik dan saran kepada konsumen untuk menilai pelayanan, kepuasan konsumen dan pengembangannya.
- 5) Membuat inovasi strategi terhadap insiden yang belum terselesaikan, menganalisis dan mengevaluasi kembali inovasi strategi yang dibuat.
- 6) Mendokumentasikan resolusi atau solusi alternative terhadap pemecahan insiden dan mengevaluasinya.
- 7) Mengembangkan sistem yang dapat melaporkan kecenderungan masalah atau insiden yang dihadapi sehingga pihak Perpustakaan UMKT dapat

mengetahui kesalahan-kesalahan yang didapatkan.

- 8) Mendefinisikan batas waktu pemecahan masalah dalam klasifikasi insiden dan mengevaluasi minimal tiap bulan sekali.

#### 4.3.3 Rekomendasi DSS03

Berdasarkan analisis *gap* yang didapat dan dengan level target yang ingin dicapai pada DSS03, maka berikut adalah beberapa rekomendasi yang dapat penulis berikan:

- 1) Melakukan pemantauan terhadap kinerja penyelesaian masalah yang telah ditentukan.
- 2) Mendokumentasikan dan mengalisa kembali laporan masalah yang ada baik yang sudah terselesaikan maupun yang belum terselesaikan.
- 3) Menganalisa akar-akar permasalahan yang muncul dan pemecahan masalah, kemudian mendokumentasikannya supaya tidak terjadi masalah yang sama.
- 4) Membuat sistem/skema yang dapat mengetahui jalannya penyelesaian pemecahan masalah yang ada agar dapat dipantau oleh pihak atasan.
- 5) Membuat dokumentasi terkait solusi-solusi dalam pemecahan masalah.
- 6) Melakukan analisa pembiayaan untuk menyelesaikan masalah, melakukan pemantauan dan didokumentasikan.
- 7) Menganalisa pengalokasian sumberdaya yang akan digunakan untuk mengoptimalkan *resource* yang dimiliki.

#### 4.3.4 Rekomendasi DSS04

Berdasarkan analisis *gap* pada DSS04, maka berikut adalah beberapa rekomendasi:

- 1) Melakukan pengukuran keberlangsungan proses bisnis untuk mengetahui tingkat kematangannya dan kesenjangan proses bisnis, didokumentasikan dan dievaluasi.



- 2) Mengukur kesesuaian kebijakan yang dibuat dalam keberlangsungan proses bisnis.
- 3) Menganalisis dan membuat skema/SOP tentang terjadinya gangguan dalam skenario proses bisnis yang ditetapkan.
- 4) Mengevaluasi kebutuhan keberlanjutan proses bisnis yang berlangsung.
- 5) Menetapkan ukuran-ukuran terhadap ancaman-ancaman yang dapat mengganggu jalannya proses bisnis.
- 6) Membuat skema atau sistem yang berisi respon terhadap insiden dan komunikasinya, mendokumentasikan dan dievaluasi.
- 7) Membuat *business continuity plan* (BCP) untuk pengembangan proses bisnis dan dokumentasikan.
- 8) Melakukan pengukuran dan evaluasi terhadap tujuan pelatihan.
- 9) Melakukan penjaminan keamanan terhadap distribusi data yang bersifat rahasia.
- 10) Membuat ketetapan ukuran-ukuran untuk pengembangan latihan sumberdaya manusia yang dimiliki, dan dipantau keberlangsungannya.

#### 4.3.5 Rekomendasi DSS05

Berdasarkan analisis *gap* pada DSS05, maka berikut adalah beberapa rekomendasi:

- 1) Membuat kebijakan terkait dengan *bug* pada aplikasi, didokumentasikan dan dievaluasi.
- 2) Menetapkan sistem yang digunakan untuk mengevaluasi ancaman-ancaman yang akan timbul, didokumentasikan dan dimonitoring.
- 3) Melakukan evaluasi rutin, minimal tiap semester terhadap sistem informasi yang dikhawatirkan dapat timbul potensi ancaman baru.
- 4) Memberikan peringatan kepada semua staff akan kesadarannya terhadap keamanan sistem dan perangkat yang dimiliki.
- 5) Membuat laporan mengenai ujicoba sistem keamanan yang diterapkan dan dievaluasi.
- 6) Mengukur kualitas sistem keamanan dan hak akses yang diberikan.
- 7) Mengevaluasi atau memantau hak akses yang diberikan untuk terjaga dari ancaman-ancaman yang potensial.

#### 4.3.6 Rekomendasi DSS06

Berdasarkan analisis *gap* pada DSS06, maka berikut adalah beberapa rekomendasi:

- 1) Menetapkan ukuran-ukuran *goal* dari proses bisnis, mendokumentasikan dan dievaluasi.
- 2) Membuat laporan dari kontrol pemrosesan agar mudah diketahui gejala-gejala yang timbul.
- 3) Memantau dan mengevaluasi prosedur keamanan untuk melindungi aset informasi.
- 4) Membuat kebijakan dalam penentuan peran yang berwenang untuk mengakses aktivitas atau data yang bersifat sensitif, dijelaskan secara rinci dan didokumentasikan.
- 5) Mereview penyimpangan-penyimpangan yang terjadi dalam keberlangsungan proses bisnis, mendokumentasikan dan dievaluasi
- 6) Membuat kebijakan terhadap pemberian hukuman kepada staff yang melakukan pelanggaran-pelanggaran dalam pemantauan kegiatan proses bisnis.
- 7) Menyimpan/mengarsipkan data dengan baik, seperti sumber informasi, rekaman transaksi untuk dijadikan bukti dalam pengukuran penilaian keberlangsungan proses bisnis dan dapat sebagai rekomendasi.
- 8) Mengidentifikasi jenis-jenis data yang bersifat rahasia, membuat prosedur

penyimpanan dan penghapusan yang tepat.

## V. KESIMPULAN

### 5.1 Kesimpulan

- 1) Pada tahap Pra audit telah diperoleh 6 proses domain DSS COBIT 5 yang dimana merupakan keseluruhan proses dari domain DSS yang sesuai dengan kondisi tata kelola Perpustakaan UMKT dan digunakan sebagai ruang lingkup dan standar audit yaitu DSS01, DSS02, DSS03, DSS04, DSS05, dan DSS06.
- 2) Dari hasil audit, diketahui ada 1 proses yang mempunyai level kapabilitas 4 yaitu DSS02, ada 5 proses yang mempunyai level kapabilitas 3 yaitu DSS01, DSS03, DSS04, DSS05 dan DSS06.
- 3) Menurut level kapabilitas masing-masing proses, ditentukan level target masing-masing proses yaitu berupa 1 level di atas level kapabilitas, yang ditentukan berdasar analisis dan juga persetujuan dengan stakeholder, sehingga didapat level target untuk DSS01, DSS03, DSS04, DSS05 dan DSS06 adalah level 4, untuk DSS02 adalah level 5.
- 4) Level *capability* keseluruhan yang diperoleh berdasarkan keseluruhan rata-rata adalah 3, yang berarti sebagian besar aktifitas pada domain DSS untuk Perpustakaan UMKT telah dilakukan, ada standar penerapan dalam melakukan proses tersebut, terdokumentasi dan komunikasi berjalan dengan baik.

### 5.2 Saran

Berikut adalah saran yang dapat disampaikan dalam penelitian ini adalah:

- 1) Penilaian tingkat kapabilitas terkait Perpustakaan UMKT dalam penelitian ini dapat dilanjutkan lagi pada modul-modul lain menggunakan COBIT 5.
- 2) Dapat ditambahkan pembobotan dalam terkait pengumpulan bukti/*evidence* yang dicari, untuk memperjelas pemberian rekomendasi.
- 3) Metode dalam penghitungan validasi dan penentuan level *capability* tiap aktifitas dapat dilakukan dengan metode yang berbeda.

### DAFTAR PUSTAKA

- Swastika, I Putu Agus. 2016. *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*. Yogyakarta: Andi.
- Dewi Fitriyani (Penterjemah). 2007. *Audit Teknologi Informasi dan Assurance*. Jakarta: Salemba Empat.
- Sarno, Riyanarto. 2009. *Audit Sistem & Teknologi Informasi*. Surabaya: ITS Press.
- Universitas Muhammadiyah Kalimantan Timur. 2017. *Visi Misi Universitas Muhammadiyah Kalimantan Timur* <http://umkt.ac.id/visi-misi-umkt/>