*Telematika: Jurnal Informatika dan Teknologi Informasi*
*Vol. 20, No. 3, Oktober 2023, pp.442-456*
*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v20i3.11867*

# *Evaluation of IT Risk Management in DISKOMINFO of Magelang Regency using COBIT Framework 2019 Objectve EDM03 & APO12*

Evaluasi Manajemen Risiko IT pada DISKOMINFO Kabupaten Magelang menggunakan *Framework* COBIT 2019 *Objective* EDM03 & APO12.

**Resti Ayunda Sari[1], Juwairiah[2]**

[1,2] Sistem Informasi, Universitas Pembangunan Nasional Veteran Yogyakarta, Indonesia

[1]restiayunda2604@gmail.com, [2*]juwairiah@upnyk.ac.id
**: Penulis korenspondensi* (*corresponding author*)

***Informasi Artikel***
*Received: July 2023*
*Revised: August 2023*
*Accepted: September 2023*
*Published: October 2023*

***Abstract***

*Purpose: This research aims to measure the current condition level (capability level) of DISKOMINFO and then conduct a Gap analysis so that it can provide recommendations for improving IT governance related to IT risk management.*
*Design/methodology/approach: The framework used is COBIT 2019, which will focus on 2 objectives: EDM03 (Evaluate, Direct, and Monitor) & APO12 (Align, Plan, and Organize). The data used in this study were obtained through interviews, observation, and distribution of questionnaires which had been mapped using the RACI Chart.*
*Findings/result: The results of the assessment show that the capability level/capability level according to DISKOMINFO is level 2 for each objective. Recommendations focus on making documentation of risk management activities in the form of risk guidelines, risk acceptance, activities for risk management methods, as well as the application of risk management evaluation of IT which is used by DISKOMINFO on a regular basis.*
*Originality/value/state of the art:From various types of risk management research with different frameworks, this research will use the COBIT 2019 performance standards to carry out information technology risk management. Where COBIT 2019 is the latest version of COBIT which was prepared to help companies manage and manage resources to achieve existing goals. COBIT 2019 has a broader scope than ISO SO/IEC 17799:2005 which includes a combination of principles that have been embedded and known as*

*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v20i3.11867*

*reference models (such as COSO), and are aligned with IT standard infrastructure.*

*Keywords: COBIT 2019, IT Risk Management, Capability Level, DISKOMINFO*
Kata kunci: COBIT 2019, Manajemen Risiko IT, Capability Level, DISKOMINFO

**Abstrak**

Tujuan: Penelitian ini bertujuan untuk mengukur tingkat kondisi (capability level) DISKOMINFO saat ini dan kemudian melakukan analisis Gap sehingga dapat memberikan rekomendasi perbaikan tata kelola TI terkait manajemen risiko TI.
Desain/metoded/pendekatan: Framework yang digunakan adalah COBIT 2019 yang fokus pada 2 tujuan: EDM03 (Evaluate, Direct, and Monitor) & APO12 (Align, Plan, and Organize). Data yang digunakan dalam penelitian ini diperoleh melalui wawancara, observasi, dan penyebaran kuesioner yang telah dipetakan menggunakan RACI Chart.
Hasil: Hasil penilaian menunjukkan bahwa tingkat kapabilitas/capability level menurut DISKOMINFO adalah level 2 untuk setiap tujuan. Rekomendasi fokus pada pendokumentasian kegiatan manajemen risiko berupa pedoman risiko, penerimaan risiko, kegiatan metode manajemen risiko, serta penerapan evaluasi manajemen risiko TI yang digunakan DISKOMINFO secara berkala.
Keaslian/*state of the art*: Dari berbagai jenis penelitian manajemen risiko dengan kerangka berbeda, penelitian ini akan menggunakan standar kinerja COBIT 2019 untuk melaksanakan manajemen risiko teknologi informasi. Dimana COBIT 2019 merupakan versi terbaru dari COBIT yang dipersiapkan untuk membantu perusahaan mengelola dan mengelola sumber daya untuk mencapai tujuan yang ada. COBIT 2019 memiliki cakupan yang lebih luas dibandingkan ISO SO/IEC 17799:2005 yang mencakup kombinasi prinsip-prinsip yang telah tertanam dan dikenal sebagai model referensi (seperti COSO), serta diselaraskan dengan infrastruktur standar TI.

## 1. Pendahuluan

Dalam era digital, perkembangan Teknologi Informasi sudah menjadi salah satu bagian penting yang harus diimplementasikan untuk sebagian besar organisasi perusahaan termasuk lembaga pemerintahan maupun swasta. Teknologi Informasi dapat diartikan sebagai bagian atau penentu keberhasilan dimana sebelumnya hanya difungsikan sebagai pendukung (support) organisasi. Implementasi teknologi informasi yang sesuai pada sebuah organisasi perusahaan dinilai sebagai sebuah solusi untuk dapat meningkatkan kompetensi yang dimiliki sebuah organisasi, sehingga peran dari tata kelola teknologi informasi (Information Technology governance) dapat dikatakan berhasil dalam menunjang efektivitas dan efisiensi organisasi. Dengan adanya tata kelola IT yang baik maka akan sangat membantu dalam menunjang pencapaian dari tujuan

*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v20i3.11867*

organisasi terutama dalam masing-masing proses bisnis [1]. Penerapan IT governance saat ini dapat dilihat dari munculnya berbagai pelayanan publik berbasis teknologi agar dapat memberikan kenyamanan, meningkatkan akurasi informasi dan transparansi tentunya akan membantu dalam mendorong keberhasilan pembangunan pemerintahan [2]-[4]. Salah satu lembaga yang menerapkan penggunaan IT yaitu Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Magelang.

Risiko IT merupakan risiko yang dihasilkan karena pemanfaatan teknologi informasi dimana ini berpotensi menimbulkan dampak negatif, dan untuk mengatasi hal tersebut diperlukan manajemen risiko yang sesuai [1]. Manajemen risiko IT merupakan penerapan dari manajemen risiko terhadap penggunaan IT pada suatu organisasi terkait dan dilakukan oleh tenaga ahli yang menguasai bidang tersebut [5]. Bentuk dari manajemen risiko dapat berupa melakukan identifikasi risiko, melakukan kajian, pengembangan strategi terkait pencegahan risiko, dan melakukan komunikasi terhadap pihak lain untuk melakukan identifikasi masalah IT yang berpotensi dalam menimbulkan dampak negatif pada organisasi. Manajemen risiko yang baik dapat dijadikan bahan pertimbangan bagi organisasi dalam mengambil suatu keputusan untuk mencegah atau mengatasi risiko yang terjadi. Hal ini akan mengurangi dampak dari risiko yang timbul dan mencegah risiko baru muncul di kemudian hari. Namun dari wawancara yang sudah dilakukan didapatkan informasi bahwa DISKOMINFO belum pernah melakukan kajian terkait manajemen risiko sehingga perlu dilakukan identifikasi potensi risiko yang mungkin terjadi yang dapat membantu dalam melakukan pengelolaan risiko dan meminimalisir risiko IT perusahaan.

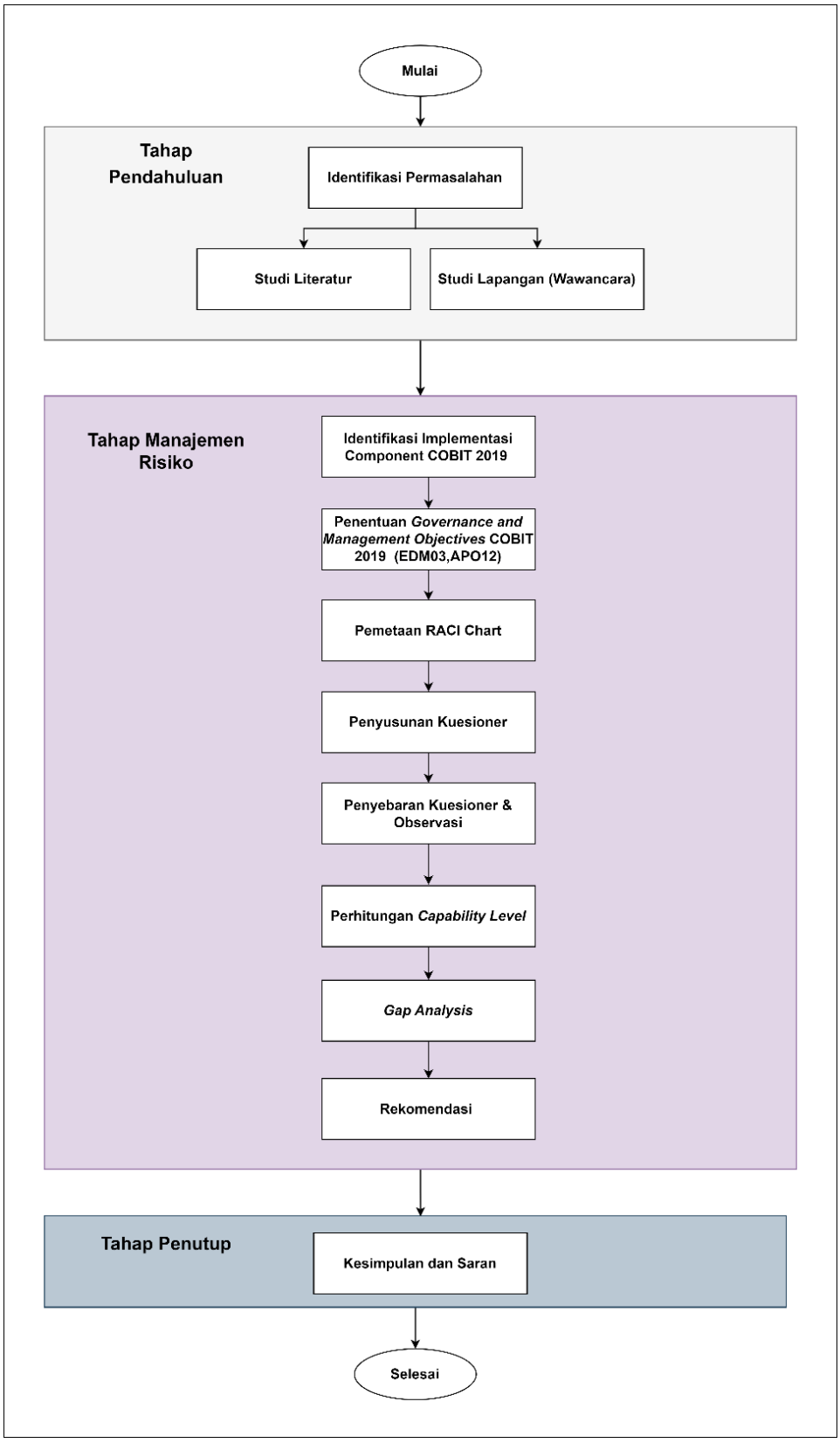
Dalam melakukan identifikasi risiko dibutuhkan framework yang tepat agar hasil yang diperoleh dapat dijadikan sebagai rekomendasi langkah dalam melakukan mitigasi risiko dan dapat dijadikan panduan sesuai dengan risiko yang muncul. Beberapa framework yang dapat digunakan untuk melakukan identifikasi risiko adalah Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management (ERM), Control Objective for Information and related Technology (COBIT), National Institute of Standards and Technology (NIST) Special Publication (SP), dan ISO 31000:2018.

Dalam COBIT 2019 terdapat 5 *objective* yaitu APO (Align, Plan, Organise), BAI (Build, Acquire, Implement), DSS (Deliver, Service, Support), MEA (Monitor, Evaluate, Assess), dan EDM (Evaluate, Direct, Monitor) [6]-[9]. COBIT 2019 merupakan evolusi dari COBIT sebelumnya yaitu COBIT 5 [10]-[12]. COBIT 2019 untuk manajemen risiko merupakan kerangka kerja yang dapat digunakan perusahaan dalam mengelola sumber daya IT dimana didalamnya akan membahas manajemen risiko. Pada COBIT 2019 and Management Risk memiliki kategori skenario risiko dan tipe risiko yang akan membantu ketika melakukan identifikasi risiko positif maupun negatif pada organisasi terkait, sehingga diharapkan dapat menjadi pedoman dalam melakukan pengelolaan IT menjadi lebih efektif dan efisien. Fokus penelitian ini adalah melakukan evaluasi tatakelola dan manajemen risiko TI menggunakan objective EDM03 (Ensure Risk Optimisation) [13] dan AP012 (Manage Risk) [14]. EDM03 akan digunakan sebagai objective yang memastikan optimasi risiko dan APO12 untuk pengelolaan terkait risiko IT.

## 2. Metode/Perancangan

Tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut:

*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v20i3.11867*




**Gambar 1**. Tahapan Penelitian

### 2.1. Identifikasi Permasalahan

Pada tahap ini dilakukan identifikasi permasalahan yang ada pada DISKOMINFO sebagai latar belakang masalah yang diangkat.

### 2.2. Studi Literatur

Studi Literatur dilakukan dengan mengumpulkan, memahami, dan melakukan analisis dari berbagai sumber terkait termasuk penelitian-penelitian terdahulu yang dapat digunakan sebagai referensi dan pendukung terhadap topic penelitian yang diambil.

### 2.3. Studi Lapangan

Studi Lapangan dilakukan dengan melakukan pengamatan terkait objek yang akan diteliti berupa mempelajari struktur organisasi DISKOMINFO Kabupaten Magelang, mempelajari fungsi dan tugas yang dilakukan oleh organisasi terkait, serta melihat secara langsung kondisi terkini dari organisasi tersebut sehingga dapat melakukan analisis yang dapat dijadikan tambahan informasi untuk melakukan penanganan terkait risiko yang akan dilakukan

### 2.4. Identifikasi Implementasi *Component* COBIT 2019

Tahap manajemen risiko yang pertama kali dilakukan adalah mengidentifikasi gambaran secara umum manajemen risiko dari DISKOMINFO Kabupaten Magelang. Ini mengacu pada panduan ISACA – COBIT 2019 *Framework Governance and Management* dimana terdapat 7 component yang ada pada COBIT 2019

### 2.5. Penentuan *Governance and Management Objectives COBIT 2019*

Penelitian ini akan berfokus pada kegiatan manajemen risiko untuk menghindari kerusakan infrastruktur dan layanan IT pada instansi tersebut dengan menggunakan *Governance and Management Objectives* EDM03 *(Ensure Risk Optimisation)* dan AP012 *(Manage Risk*. Kedua *objective* ini digunakan untuk membatasi ruang lingkup yang akan diteliti pada penelitian ini. Selain itu kedua proses ini juga digunakan untuk melakukan pengukuran, analisis *capability,* penilaian risiko, dan pemberian rekomendasi mitigasi risiko.

### 2.6. Pemetaan RACI Chart

Pada tahap ini akan dilakukan pemetaan organisasi berdasarkan domain *objective* yang akan digunakan. Pemetaan ini mengacu pada standar RACI *Chart* COBIT 2019. Penggunaan RACI *Chart* ini merupakan salah satu implementasi dari structur yang ada dalam COBIT 2019. Dimana RACI *Chart* merupakan salah satu komponen yang ada dan telah digambarkan sesuai dengan domain yang akan digunakan.

### 2.7. Penyusunan Kuesioner

Pada langkah ini domain yang akan digunakan sudah ditentukan sehingga penyusunan kuesioner dilakukan dengan menyusun beberapa pertanyaan dengan acuan *framework* yang digunakan yaitu COBIT 2019 domain APO12 dan EDM03. Kuesioner berupa pertanyaan dengan jawaban ya atau tidak. Kuesioner yang dibuat memiliki tingkatan level yang nantinya akan disesuaikan dengan kondisi terkini dari organisasi.

### 2.8. Penyebaran Kuesioner

Pada tahap ini dilakukan pengumpulan data sesuai pemetaan RACI *Chart* yang sudah dilakukan sebelumnya. Diharapkan tahap ini dapat memberikan rekapitulasi distribusi dari jawaban dan melakukan identifikasi output dari responden. Pengumpulan data juga dilakukan dengan menggunakan kuesioner dimana kuesioner berisi beberapa pertanyaan yang sudah dibuat pada tahap sebelumnya

## 2.9. Perhitungan Capability level

Setelah data didapatkan maka akan dilakukan pengolahan data dimana data yang sudah terkumpul pada tahap sebelumnya dihitung untuk mengetahui capaian *capability level* pada kondisi saat ini pada *objective* yang digunakan yaitu EDM03 dan APO12. Penilaian *capability level* dilakukan dengan menilai setiap proses menggunakan acuan model tingkat kapabilitas skala rating berdasarkan standar ISO/IEC 15504.

Setiap level kapabilitas proses dapat dicapai jika level di bawahnya sudah penuh dicapai. Penilaian tingkat kapabilitas dimulai dari level 2 karena pada COBIT 2019 organisasi dianggap telah melakukan aktivitas pada level sebelumnya [10]. Pengelolaan dan perhitungan data kuesioner dalam menentukan tingkat kapabilitas COBIT 2019 dari masing-masing aktivitas dihitung dan diolah dengan menggunakan rumus berikut:

a. Perhitungan persentase aktivitas *capability level* 1 per *objective*

$$\text{Persentase Aktivitas} = \frac{Aktivitas\ Terlaksana}{Total\ Aktivitas}\ x\ 100\ \% \quad (1)$$

b. Perhitungan persentase *output capability level* 1 per *objective*

$$\text{Persentase Output} = \frac{Output\ yang\ Terdefinisi}{Total\ Output}\ x\ 100\ \% \quad (2)$$

c. Perhitungan persentase proses *outcome level* 1 per *objective*

$$\text{Presentasi Proses Outcome} = \frac{Persentase\ Aktivitas + Persentase\ Output}{2}\ x\ 100\ \% \quad (3)$$

d. Perhitungan persentase proses atribut *capability* per level, level 2 hingga level 5

$$\text{Presentasi Proses Atribut} = \frac{Proses\ Atribut\ Terlaksana}{Total\ Proses\ Atribut}\ x\ 100\ \% \quad (4)$$

**Tabel 1** Rating Levels

| Abberviation | Description | %Achieved |
|---|---|---|
| N | *Not Achieved* | 0% - 15% *achievement* |
| P | *Partially Achieved* | >15% - 50% *achievement* |
| L | *Largely Achieved* | >50% - 85% *achievement* |
| F | *Fully Achieved* | >85% - 100% *achievement* |

Dari *rating levels* dan tingkat kapabilitas yang digunakan pada proses evaluasi maka didapatkan pemetaan sebagai berikut :

**Tabel 2** Capability level Process Assesment Model

| Capability level Process Assesment Model | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| *Level 0 Incomplete* | | | | | |
| *Level 1 Performed* | L/F | F | F | F | F |
| *Level 2 Managed* | | L/F | F | F | F |
| *Level 3 Established* | | | L/F | F | F |
| *Level 4 Predictable* | | | | L/F | F |
| *Level 5 Optimizing* | | | | | L/F |

Pencapaian tingkat kapabilitas dapat diketahui jika proses tersebut sudah mencapai tingkat *Largely Achieved*. jika seluruh proses sudah berada di posisi *Fully Achieved* maka penilaian dapat dilakukan pada level selanjutnya.

### 2.10. Gap Analysis

Setelah diketahui tingkat kapabilitas dari kondisi perusahaan saat ini maka akan didapatkan juga hasil kesenjangan*(Gap)* untuk setiap *objective* yang digunakan. *Gap* ini diperoleh dari kemampuan yang ada pada perusahaan saat ini *(as-is)* dan tingkat kemampuan yang ingin dicapai oleh perusahaan *(to-be*).

### 2.11. Rekomendasi

Tahap ini merupakan hasil akhir dari penilaian *capability level* dan tingkat kemampuan yang ingin dicapai oleh perusahaan dan akan digunakan sebagai acuan untuk melakukan identifikasi rekomendasi yang sesuai dengan kebutuhan sehingga dapat mencapai tingkat kemampuan yang diinginkan oleh DISKOMINFO .

## 3. Hasil dan Pembahasan

Pada bagian ini akan dilakukan terkait pembahasan proses pengambilan dan pengolahan data berupa kuesioner yang sudah ada, sehingga akan memuat hasil berupa *level capability* yang dicapai oleh DISKOMINFO saat ini. Data yang diolah berupa hasil kuesioner wawancara terhadap responden yang sudah dipetakan berdasarkan tabel RACI yang berupa *base practice* dan juga *output work product* berupa dokumen yang ada didalam instansi tersebut.

**Tabel 3** Daftar Responden

| Kode Responden | Jabatan | Objective |
|---|---|---|
| R1 | Kepala Dinas | EDM03, APO12 |
| R2 | Sekretariat | APO12 |
| R3 | Bidang Informatika | APO12 |
| R4 | Bidang Informasi dan Komunikasi Publik | APO12 |
| R5 | Bidang Statistik dan Persandian | EDM03, APO12 |

### 3.1. Hasil Kuesioner dan Identifikasi *Work Product Objective* EDM03 *(Ensure Risk Optimisation)*

a. Rekapitulasi hasil kuesioner *Capability level* EDM03 Level 2

**Tabel 4** Rekapitulasi Jawaban Responden untuk *Objective* EDM03 level 2 (*Base Practice*)

| No | Sub *Objective* | Aktivitas Tata Kelola | R1 | R2 |
|---|---|---|---|---|
| 1 | EDM03.01.a | Memahami organisasi dan konteksnya yang berkaitan dengan risiko Teknologi dan Informasi | 1 | 1 |
| 2 | EDM03.01.b | Menentukan pilihan risiko organisasi, yakni tingkat risiko terkait Teknologi dan Informasi yang bersedia diambil oleh perusahaan dalam mencapai tujuan perusahaan. | 1 | 1 |
| 3 | EDM03.01.c | Menentukan tingkat toleransi risiko terhadap pilihan risiko organisasi, yaitu penyimpangan sementara yang dapat diterima dari pilihan risiko perusahaan. | 0 | 1 |
| 4 | EDM03.01.d | Menentukan sejauh mana keselarasan strategi antara risiko Teknologi dan Informasi dengan strategi risiko perusahaan, | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| | | serta memastikan pilihan risiko berada di bawah kapasitas risiko organisasi. | | |
| 5 | EDM03.02.a | Mengarahkan proses penerjemahan dan integrasi strategi risiko Teknologi dan Informasi ke dalam praktik manajemen risiko dan kegiatan operasional. | 1 | 1 |
| 6 | EDM03.02.b | Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan). | 0 | 0 |
| 7 | EDM03.02.c | Menerapkan secara langsung mekanisme yang sesuai untuk merespon dengan cepat terhadap perubahan risiko dan segera melaporkan ke tingkat manajemen yang sesuai, dengan didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, serta bagaimana). | 1 | 1 |
| 8 | EDM03.02.d | Mengarahkan bahwa risiko, peluang, masalah, maupun kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa saja kepada pihak yang bertanggungjawab kapan pun itu. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan serta diteruskan ke pengambil keputusan terkait. | 1 | 1 |
| 9 | EDM03.03.a | Melaporkan setiap masalah manajemen risiko kepada dewan atau komite eksekutif | 1 | 1 |
| **Rata-Rata Per Responden** | | | **77,8%** | **88,8%** |
| **Total Rata-Rata** | | | **83,3%** | |

Keterangan: Ya= 1, Tidak = 0
Responden 1 : Kepala Dinas DISKOMINFO
Responden 2 : Kepala Bidang Persandian dan Statistik

b. Hasil Identifikasi *Output Work Product* EDM03 Level 2

Dibawah ini merupakan hasil dari identifikasi *work product* yaitu dari dokumentasi kegiatan yang dilakukan pada *objective* EDM03 *(Ensure Risk Optimisation)* :

**Tabel 5** Hasil Identifikasi *Output Work Product* EDM03 Level 2

| **No** | ***Work Product* (WPs)** | ***Output*** | **Deskripsi Dokumen** | **Y/T** |
|---|---|---|---|---|
| 1 | EDM03-WP1 | Panduan Selera Risiko *(Risk appetite guidance)* | Panduan tingkat risiko yang dapat diterima oleh DISKOMINFO | **T** |
| 2 | EDM03-WP2 | Kegiatan evaluasi manajemen risiko*(Evaluation of risk management activities)* | Dokumen kegiatan dalam rangka audit internal maupun external untuk evaluasi manajemen risiko | **Y** |
| 3 | EDM03-WP3 | Level toleransi risiko yang disetujui *(Approved risk tolerance levels)* | Dokumen tingkat toleransi risiko yang disetujui pada DISKOMINFO | **Y** |
| 4 | EDM03-WP4 | Proses penilaian manajemen risiko yang telah disetujui*(Approved process for measuring risk management)* | Dokumen yang menggambarkan penilaian pada manajemen risiko yang telah disetujui pada DISKOMINFO | **T** |
| 5 | EDM03-WP5 | Tujuan utama yang harus dipantau untuk manajemen risiko *(Key objectives to be monitored for risk management)* | Dokumen yang menyatakan tujuan utama dari penilaian manajemen risiko sehingga harus terus dipantau dalam proses implementasi | **Y** |
| 6 | EDM03-WP6 | Kebijakan Manajemen Risiko *(Risk management policies)* | Dokumen yang menyatakan kebijakan atau prosedur terkait | **Y** |

| | | | | |
|---|---|---|---|---|
| | | | manajemen risiko di beberapa aktivitas/sistem yang ada pada DISKOMINFO | |
| 7 | EDM03-WP7 | Tindakan perbaikan untuk mengatasi penyimpanagan manajemen risiko *(Remedial actions to address risk management deviations)* | Dokumen yang menggambarkan tindakan yang harus dilakukan untuk menangani penyimpangan manajemen risiko | **Y** |
| 8 | EDM03-WP8 | Isu manajemen risiko kepada Kepala Dinas*(Risk management issues for the board)* | Dokumen berupa laporan terkait insiden yang terjadi, laporan audit kepada kepala dinas | **Y** |
| Rata- rata skor | | | | **75%** |

Dari hasil perhitungan *t*ersebut maka dilakukan perhitungan skor rata-rata dari kedua instrumen tersebut untuk memperoleh nilai akhir dari *capability level objective* EDM03. Hasil yang diperoleh dari rekapitulasi yang dilakukan didapatkan presentase yang didapat pada level 2 adalah sebagai berikut :

**Tabel 6** Rekapitulasi *Capability Level Objective* EDM03

| **No** | **Atribut** | **Skor** |
|---|---|---|
| 1. | Base Practice | 83,3% |
| 2. | Work Product | 75% |
| **Rata – Rata Perhitungan Capability Level EDM03** | | **79,15 %** |
| **Rating Level** | | **Largely Achieved** |

Berdasarkan hasil yang diperoleh pada perhitungan *capability level* 2 yang menunjukkan nilai tersebut berada pada level ***Largely achieved***, dimana ini berarti penilaian *capability level* tidak dilanjutkan ke tahap selanjutnya sesuai dengan ketentuan pada *rating score activities*. Penilaian dapat dilanjutkan jika level 2 dicapai secara *Fully achieved* oleh DISKOMINFO.

### 3.2. Hasil Kuesioner dan Identifikasi *Work Product Objective* APO12 (*Managed Risk)*

a. Rekapitulasi hasil kuesioner *Capability level* APO12 Level 2

**Tabel 7** Rekapitulasi Jawaban Responden untuk Objective APO12

| **No** | **Sub Objective** | **Aktivitas Tata Kelola** | **R1** | **R2** | **R3** | **R4** | **R5** |
|---|---|---|---|---|---|---|---|
| 1 | APO12.01.a | Menetapkan dan mempertahankan metode dalam pengumpulan, klasifikasi, dan analisis data terkait risiko IT | 1 | 1 | 0 | 1 | 0 |
| 2 | APO12.01.b | Merekam data terkait risiko IT yang relevan dan signifikan pada lingkungan operasi internal maupun eksternal perusahaan | 1 | 1 | 1 | 1 | 1 |
| 3 | APO12.03.a | Menginventarisasi proses bisnis dan melakukan dokumentasi atas ketergantungannya pada proses manajemen layanan IT dan infrastruktur sumber daya IT. Identifikasi ini dapat berupa staff | 1 | 1 | 1 | 0 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | pendukung, aplikasi yang digunakan, infrastruktur yang berkaitan dengan IT, catatan penting yang bersifat manual, vendor , pemasok, dan agen outsourcing. | | | | | |
| 4 | APO12.03.b | Menentukan dan menyepakati layanan IT serta sumber daya infrastruktur yang penting untuk mempertahankan operasi bisnis proses. Melakukan analisis dependensi serta identifikasi tautan yang lemah. | 1 | 1 | 1 | 0 | 1 |
| 5 | APO12.03.c | Menggabungkan scenario risiko saat ini berdasarkan kategori, lini bisnism dan area fungsional | 1 | 1 | 1 | 1 | 1 |
| 6 | APO12.05.a | Memelihara inventarisasi aktivitas pengendalian yang ada untuk mengelola risiko dan yang memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke pernyataan risiko TI tertentu dan agregasi risiko TI. | 1 | 1 | 1 | 0 | 1 |
| **Rata-Rata Per Responden** | | | **100%** | **100%** | **83,3%** | **50%** | **83,3%** |
| **Total Rata-Rata** | | | **83,3%** | | | | |

b. Hasil Identifikasi *Output Work Product* APO12 Level 2

Hasil dari identifikasi *work product* yaitu dari dokumentasi kegiatan yang dilakukan pada *objective* APO12 *(Manage Risk)* :

**Tabel 8** Hasil Identifikasi *Output Work Product* APO12 Level 2

| **No** | ***Work Product* (WPs)** | ***Output*** | **Deskripsi Dokumen** | **Y/T** |
|---|---|---|---|---|
| 1 | APO12-WP1 | Masalah dan faktor risiko yang muncul *(Emerging risk issues and factors)* | Dokumen yang berisi masalah dan faktor penyebab risiko muncul pada DISKOMINFO | Y |
| 2 | APO12-WP2 | Data kejadian risiko dan faktor penyebabnya *(Data on risk events and contributing factors)* | Dokumen seluruh kejadian risiko IT dan penyebab terjadinya | Y |
| 3 | APO12-WP3 | Data tentang lingkungan operasi yang berkaitan dengan risiko *(Data on the operating environment relating to risk)* | Dokumen tentang lingkup operasi DISKOMINFO yang memiliki kaitannya dengan risiko yang terjadi | T |
| 4 | APO12-WP4 | Hasil analisis risiko *(Risk analysis results)* | Dokumen yang memberikan gambaran terkait hasil analisis risiko IT yang pernah terjadi | T |
| 5 | APO12-WP5 | Skenario risiko I&T *(I&T risk scenarios)* | Dokumen yang menggambarkan skenario yang harus dijalankan untuk menangani risiko IT pada DISKOMINFO | T |
| 6 | APO12-WP6 | Lingkup upaya analisis risiko *(Scope of risk analysis efforts)* | Dokumen yang berisi batasan terkait analisis risiko sebagai upaya penanganan masalah | Y |

| | | | | |
|---|---|---|---|---|
| 7 | APO12-WP7 | Profil risiko gabungan, termasuk status tindakan manajemen risiko *(Aggregated risk profile, including status of risk management actions)* | Dokumen yang berisi profil risiko dan telah dikelompokkan dimana terdapat status tindakan manajemen risiko yang terjadi/ urgensi disetiap kejadian | T |
| 8 | APO12-WP8 | Skenario risiko terdokumentasi berdasarkan lini bisnis dan fungsi *(Documented risk scenarios by line of business and function)* | Dokumen scenario risiko berdasarkan lini bisnis dan fungsinya | T |
| 9 | APO12-WP9 | Analisis risiko dan laporan profil risiko untuk pemangku kepentingan *(Risk analysis and risk profile reports for stakeholders)* | Dokumen yang berisi hasil analisis risiko dan profil risiko dan akan diberikan kepada pemangku kepentingan | Y |
| 10 | APO12-WP10 | Hasil penilaian risiko pihak ketiga *(Results of third-party risk assessments)* | Dokumen hasil penilaian risiko IT dari pihak ketiga yang bekerja sama dengan DISKOMINFO | Y |
| 11 | APO12-WP11 | Peluang untuk menerima risiko yang lebih besar *(Opportunities for acceptance of greater risk)* | Dokumen yang berisi gambaran peluang dalam penerimaan selera risiko lebih tinggi dengan tujuan tertentu | Y |
| 12 | APO12-WP12 | Proposal proyek untuk mengurangi risiko *(Project proposals for reducing risk)* | Dokumen proposal proyek yang akan dikembangkan untuk mengurangi dampak risiko yang terjadi | T |
| 13 | APO12-WP13 | Komunikasi dampak risiko *(Risk impact communication)* | Dokumen berupa komunikasi yang terdokumentasi berupa dampak dari masing-masing risiko IT | T |
| 14 | APO12-WP14 | Akar penyebab terkait risiko *(Risk-related root causes)* | Dokumen yang menggambarkan masing-masing penyebab dari risiko IT yang terjadi | T |
| 15 | APO12-WP15 | Rencana respons insiden terkait risiko *(Risk-related incident response plans)* | Dokumen yang akan memberikan gambaran terkait rencana apa untuk menangani insiden terkait risiko | T |
| **Rata- rata skor** | | | **40%** | |

**Tabel 9** Rekapitulasi *Capability Level Objective* APO12

| **No** | **Atribut** | **Skor** |
|---|---|---|
| 1. | Base Practice | 83,3% |
| 2. | Work Product | 40% |
| **Rata – Rata Perhitungan Capability Level APO12** | | **61,7%** |
| **Rating Level** | | **Largely Achieved** |

Berdasarkan hasil yang diperoleh pada perhitungan *capability level* 2 yang menunjukkan nilai tersebut berada pada level ***Largely achieved***, dimana ini berarti penilaian *capability level* tidak dilanjutkan ke tahap selanjutnya sesuai dengan ketentuan pada *rating score activities*. Penilaian dapat dilanjutkan jika level 2 dicapai secara *Fully achieved* oleh DISKOMINFO.

### 3.3. Validasi *Output Work Product*

Dari hasil kuesioner w*ork product* yang sudah dilakukan sebelumnya, maka dapat disimpulkan bahwa dokumen yang didapatkan adalah sebagai berikut:

**Tabel 10** Dokumen Work Product Capability level

| Kode Dokumen | Nama Dokumen |
|---|---|
| DPA-RFK | Dokumen Realisasi Anggaran – Realisasi Fisik Keuangan |
| ADT-1 | Instrumen Audit Keamanan Informasi |
| LAP-1 | Laporan Insiden Keamanan Informasi |
| PPI-1 | Panduan Penanganan Insiden Serangan *SQL Injection* |
| PPI-2 | Panduan Penanganan Insiden *Web Defacement* |
| PPI-3 | Panduan Penanganan Insiden Serangan DDOS |
| PPI-4 | Panduan Penanganan Insiden Serangan *Phising* |
| PPI-5 | Panduan Penanganan Insiden Serangan *Malware* |

Dokumen yang dicantumkan adalah dokumen yang ada dan berkaitan dengan manajemen risiko IT dari DISKOMINFO dan beberapa dokumen memiliki sifat rahasia sehingga pada penelitian ini tidak dapat secara langsung menampilkan dan mengamati dokumen terkait.

### 3.4. Analisis Tingkat Kesenjangan *Capability level (Gap Capability level )*

Dari hasil perhitungan data kuesioner untuk objective EDM03 dan APO12 didapat *capability level as-is,* kemudian dilakukan wawancara dengan responden untuk menentukan Level yang diinginkan (to-be), maka dilakukan analisis gap.

**Tabel 11** Hasil Analisis *Gap Capability Level*

| Objective | As-is | To-be | Gap |
|---|---|---|---|
| EDM03 | 2 | 3 | 1 |
| APO12 | 2 | 3 | 1 |

Nilai *Gap* yang diperoleh untuk level saat ini dari masing-masing *objective* adalah 1. Supaya proses pada *objective* EDM03 dan APO12 mencapai level yang diharapkan yaitu level 3 maka pihak DISKOMINFO harus memenuhi aktivitas-aktivitas yang belum tercapai pada level 2 dan juga mendokumentasikan segala bentuk data yang berkaitan dengan risiko sehingga hasil akhirnya dapat mencapai presentase >85 – 100% yang termasuk dalam *Fully Achieved. Gap* yang diperoleh dari *objective* EDM03 adalah belum melakukan pengarahan terhadap pengembangan komunikasi risiko untuk seluruh tingkatan perusahaan serta belum melakukan dokumentasi terhadap panduan selera risiko. Untuk *Gap* yang diperoleh pada APO12 terdapat pada tidak tersedianya beberapa dokumen terkait yang sudah dipetakan pada COBIT 2019.

### 3.5. Rekomendasi Perbaikan

Pembahasan ini akan memberikan rekomendasi kepada DISKOMINFO dalam menyempurnakan aktivitas pada *capability level* yang dicapai serta *melaksanakan capability level* yang diharapkan. Adapun rekomendasi untuk penyempurnaan tingkat kapabilitas dan langkah untuk mencapai keinginan yang diharapkan pada *objective* EDM03 adalah sebagai berikut.

**Tabel 12** Rekomendasi Perbaikan *Objective* EDM03

| **Melengkapi level 2** |
|---|
| **Rekomendasi** |
| Mengoptimalkan penggunaan CSIRT dengan sosialisasi dan adanya panduan terkait penggunaan CSIRT |
| Membuat dokumen yang berisikan jumlah dan jenis risiko yang dapat diterima dalam risiko IT oleh DISKOMINFO |
| Melakukan penilaian pada risiko IT yang muncul pada DISKOMINFO menggunakan ISO 31000:2018 atau standar lain yang dapat digunakan seperti dari BSSN. |
| **Mencapai Level 3** |
| **Rekomendasi** |
| Melakukan audit untuk mengevaluasi dan mengetahui faktor dari risiko IT. |
| Membentuk team khusus di bawah Departemen Statistik dan Persandian yang bertugas untuk mengelola dan mengkoordinasikan penerapan manajemen IT, khususnya sistem CSIRT dan sistem lain yang terintegrasi |
| Memberikan pelatihan terkait penerapan manajemen risiko teknologi informasi untuk meningkatkan kompetensi SDM. |
| Menyusun dokumen yang berisi proses untuk mengelola dan menyelesaikan setiap risiko IT |
| Memonitoring pengelolaan risiko IT yang ada beserta tindakan yang telah diidentifikasi sebelumnya |

**Tabel 13** Rekomendasi Perbaikan *Objective* APO12

| **Melengkapi level 2** |
|---|
| **Rekomendasi** |
| Menggunakan metode *quantitative* untuk menentukan jumlah risiko dan melakukan pengkategoriannya. Selain itu analisis risiko IT dapat disesuaikan dengan standar BSSN. |
| Membuat dokumen tertulis yang berfokus pada pedoman dan prosedur penerapan manajemen risiko IT khususnya pada sistem yang digunakan dan informasi yang diterima. |
| Memastikan skenario risiko yang dibuat sejalan dengan visi dari DISKOMINFO yaitu "Terwujudnya Masyarakat Informasi melalui Teknologi Informasi dan Komunikasi dengan memperhatikan Kearifan Lokal untuk menuju Kepemerintahan yang Baik" |
| Proposal proyek terkait risiko IT harus terus dikembangkan dan terdokumentasi dengan baik. |
| **Mencapai Level 3** |
| **Rekomendasi** |
| Menentukan kategori risiko yang ada berdasarkan dampak yang diterima untuk masing-masing bidang. |
| Membuat dokumen yang berfokus pada dokumentasi setiap kejadian dan penanganan yang dilakukan terkait risiko IT. |
| Melakukan perhitungan *Cost Benefit Analysis* untuk memperkirakan kerugian dan keuntungan dalam menangani risiko yang ada |
| Melakukan audit pada teknologi informasi yang digunakan untuk memperbarui kemungkinan risiko IT yang muncul. |
| Membuat dokumen tertulis yang membahas mengenai mitigasi risiko, *Business continuity Plan, Disaster Recovery Plan,* dan *risk respond* dari seluruh risiko terkait dengan penerapan teknologi informasi. |
| Membuat dokumen tertulis yang berbentuk seperti Profil Risiko namun secara khusus menampung hasil identifikasi risiko, analisis risiko (baik berupa analisis sumber, penyebab dan akibat dari risiko), evaluasi penilaian risiko dan pengendalian atau penanganan risiko terkait dengan risiko teknologi informasi. |
| Melaporkan terkait hasil analisis risiko IT kepada Kepala Dinas, dimana ini berisi dokumen yang sudah dibuat sebagai pendukung keputusan secara berkala. |
| Meningkatkan intensitas kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi dari pegawai DISKOMINFO |
| Menyusun dan menetapkan proposal proyek untuk meminimalisir risiko yang berisi biaya/manfaat,dampak, serta peraturan yang diimplementasikan saat ini dimana ini berkaitan dengan manajemen tata kelola risiko IT. |
| Mengoptimalkan penggunaan CSIRT dalam melakukan pengelolaan risiko teknologi informasi |

| |
|---|
| Menerapkan rencana respon tanggap untuk mengatasi risiko IT yang terjadi sesuai dengan rencana respon yang sudah dibuat. |

Dari hasil analisis yang telah dilakukan maka terdapat 23 rekomendasi yang harus dilakukan oleh DISKOMINFO. Rekomendasi yang dibuat pada proses EDM03 dan APO12 berpedoman pada buku *Governance and Management Objective*s [7] dalam penerapan aktivitas sesuai dengan *Capability Level* untuk proses EDM03 dan APO12.

## 4. Kesimpulan dan Saran

Berdasarkan penelitian yang telah dilakukan maka diperoleh kesimpulan yaitu sebagai berikut. Hasil penelitian pada evaluasi manajemen risiko IT pada DISKOMINFO menunjukan bahwa tingkat kemampuan (*Capability Level* ) yang dapat dicapai saat ini dari hasil wawancara, observasi, dan penyebaran kuesioner kepada responden sesuai dengan pemetaan RACI *Chart* menunjukkan bahwa *Capability Level* yang dicapai pada *objective* EDM03 *(Ensure Risk Optimisation)* berada pada level 2 dengan kondisi bahwa DISKOMINFO telah berhasil menerapkan kegiatan dasar yang lengkap dalam pengelolaan IT. Hal ini dibuktikan dengan penerapan aktivitas yang ada pada penilaian *Capability Level* 2. Selain itu pada *objective* APO12 *Capability Level* berada pada level 2 yang dimana aktivitas dasar pada APO12 telah diimplementasikan oleh DISKOMINFO. Namun DISKOMINFO tetap ingin untuk meningkatkan performanya dengan tingkat kapabilitas yang lebih optimal. Dalam hal ini didapati *Gap* sebesar 1 dengan level target adalah *Capability Level* 3. Selain itu diperoleh rekomendasi berjumlah 30 kegiatan. Pada *objective* EDM03 terdapat 3 rekomendasi sebagai bentuk penyempurnaan level 2 serta untuk mencapai level 3 maka terdapat 5 rekomendasi aktivitas dan output yang harus diberikan oleh DISKOMINFO. Selain itu untuk *objective* APO12 tahap penyempurnaan level 2 terdapat 4 rekomendasi yang harus dilakukan serta untuk mencapai level 3 maka terdapat 18 rekomendasi aktivitas. Masing – masing rekomendasi dideskripsikan sesuai dengan penilaian yang harus dipenuhi pada COBIT 2019. Saran yang dapat diberikan oleh penulis dalam pengembangan lebih lanjut terkait penelitian berikutnya yaitu sebagai diharapkan untuk penelitian yang akan dilakukan kedepannya dapat mengambil fokus selain proses yang telah dilakukan peneliti.

## Daftar Pustaka

[1] J. Juminovario, et al., "Manajemen Risiko Divisi Sistem Informasi Pada Universitas Bina Insan Menggunakan Framework Cobit 5," CogITo Smart Journal, vol. 8, pp. 491-500, 2022.

[2] D. F. Tanjung, A. Oktaviana, & A. P. Widodo, "Analisis Manajemen Risiko startup Pada Masa pandemi COVID-19 Menggunakan COBIT® 2019," Jurnal Teknologi Informasi Dan Ilmu Komputer, vol. 8, no. 3, pp. 635, 2021.

[3] A. Ariesta, S. Suprapto, S, & A. Perdanakusuma, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12," Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, vol. 6, no. 12, pp. 5736-5745, 2023. [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/11984

[4] J. Ar Rajjani, B. Hanggara, & Y. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12," Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, vol. 5, no. 5, pp. 1734-1744, 2021. [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/8982

[5] Putu, et al., "Judul Artikel Terkait Manajemen Risiko IT," Jurnal Manajemen Risiko, vol. 15, pp. 123-145, 2020.

[6] ISACA, "COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution," ISACA, United States of America, 2018.

[7] ISACA, "COBIT 2019 Framework Governance and Management Objectives," ISACA, United States of America, 2018.

[8] ISACA, "COBIT 2019 Framework Introduction and Methodology," ISACA, United States of America, 2018.

[9] ISACA, "COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution," ISACA, United States of America, 2018.

[10] ISACA, "COBIT 5: Enabling processes," ISACA, 2012.

[11] ISACA, "COBIT 5: Process assessment model (PAM): Using COBIT 5," ISACA, 2013.

[12] ISACA, "COBIT 5: For risk," ISACA, 2016.

[13] F. T. Riadi, A. D. Manuputty, and A. Saputra, "Evaluasi Manajemen Risiko Keamanan Informasi Dengan Menggunakan Framework Cobit 5 Subdomain Edm03 (Ensure Risk Optimisation)," Jurnal Terapan Teknologi Informasi, vol. 2, no. 1, pp. 12–21, 2018. [Online]. Available: https://doi.org/10.21460/jutei.2018.21.53

[14] H. A. Sari, Y. Rahardja, and H. P. Chernovita, "Analisis Manajemen Risiko ti pada DISKOMINFO Salatiga Menggunakan Cobit5 Dengan domain APO12," JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), vol. 8, no. 4, pp. 1772–1784, 2021. [Online]. Available: https://doi.org/10.35957/jatisi.v8i4.1089

[15] R. Anugrah, E. Utami, and A. H. Muhammad, "Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis cobit 2019 dengan pertimbangan domain APO12," Jurnal Ilmiah Universitas Batanghari Jambi, vol. 22, no. 2, p. 991, 2022.