**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 6, No. 12, Desember 2022, hlm. 5755-5764 http://j-ptiik.ub.ac.id

# Evaluasi Tata Kelola Manajemen Risiko Teknologi Informasi pada PT XYZ menggunakan Kerangka Kerja COBIT 2019

**Firza Zukhriadna Afriliandra[1], Suprapto[2], Andi Reza Perdanakusuma[3]**

Program Studi Sistem Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]firzazukh@student.ub.ac.id, [2]spttif@ub.ac.id, [3]andireza@ub.ac.id

**Abstrak**

PT XYZ merupakan perusahaan berbasis TI di Kota Malang yang menyediakan pelayanan sebagai penyelesaian permasalahan klien. Sebagai penyedia jasa, perusahaan perlu mengelola manajemen risiko TI dengan baik karena terdapat kemungkinan terjadinya risiko TI dari sistem milik klien yang sedang dikembangkan. Untuk menjaga kualitas sistem, perusahaan menerapkan layanan Sentry.io untuk membantu developer dalam memonitoring sistem sehingga error yang terjadi dapat segera diperbaiki. Namun terkadang dalam penerapannya masih ditemui permasalah atau hambatan. Saat ini perusahaan belum melakukan pendokumentasian risiko TI yang teridentifikasi, hal tersebut perlu dilakukan guna menentukan skenario risiko TI untuk mencegah risiko terulang kembali. Padatnya kinerja kegiatan dalam perusahaan menyebabkan aktivitas pengelolaan risiko TI perlu dioptimalkan agar tidak mempengaruhi jalannya proses bisnis. Penelitian ini bertujuan untuk mengidentifikasi *capability level* terkait kondisi pengelolaan manajemen risiko TI pada perusahaan. Setelah dilakukan evaluasi, didapatkan rekomendasi perbaikan berdasarkan analisis *gap*. Penelitian berfokus pada proses EDM03 dan APO12 kerangka kerja COBIT 2019. Data yang digunakan dalam penelitian dikumpulkan melalui tahap wawancara, penyebaran kuesioner, serta observasi. Berdasarkan hasil analisis data, *capability level* yang dicapai oleh PT XYZ berada di level 1 pada proses EDM03 dan APO12. Pemberian rekomendasi berfokus pada aktivitas yang dapat membantu perusahaan dalam memperbaiki penerapan manajemen risiko teknologi informasi.

**Kata kunci**: COBIT 2019, Manajemen Risiko TI, *Capability Level*, Analisis Kesenjangan (*Gap*), EDM03, APO12.

***Abstract***

*PT XYZ is an IT-based company in Malang City that provides services as a solution to client problems. As a service provider, companies need to manage IT risk management well because there is a possibility of IT risk occurring from the client's system being developed. To maintain service quality, the company implements the Sentry.io service to assist developers in monitoring the system so that errors that occur can be corrected immediately. But sometimes there are still problems or obstacles in its application. Currently the company has not documented identified IT risks, this needs to be done in order to determine IT risk scenarios to prevent the risk from reoccurring. The tight performance of activities within the company means that IT risk management activities need to be optimized so as not to affect the running of business processes. This study aims to identify the capability level related to the condition of managing IT risk management in companies. After evaluation, recommendations for improvement based on gap analysis were obtained. The research focused on the EDM03 and APO12 processes of the 2019 COBIT framework. The data used in the study were collected through interviews, distributing questionnaires, and observation. Based on the results of data analysis, the capability level achieved by PT XYZ is at level 1 in the EDM03 and APO12 processes. Provision of recommendations focuses on activities that can help improve the implementation of information technology risk management at PT XYZ.*

***Keywords**: COBIT 2019, IT Risk Management, Capability Level, Gap Analysis, EDM03, APO12.*

## 1. PENDAHULUAN

Dewasa ini Teknologi Informasi sudah tidak lagi dapat dipisahkan dengan berbagai aspek pendukung kehidupan (Kurnia, et al., 2018). Tidak hanya bagi perorangan, teknologi kini sudah menjadi salah satu kebutuhan dasar bagi hampir semua organisasi karena manfaatnya yang cukup signifikan dalam membantu peningkatan efektifitas kinerja. Dalam pengelolaan suatu organisasi, dibutuhkan tata kelola TI yang berperan sebagai pendukung berbagai aktivitas dari organisasi dalam mencapai tujuannya (Sofa, Suryanto, Suryono, 2020). Salah satu perusahaan yang menerapkan penggunaan teknologi informasi adalah PT XYZ yang merupakan sebuah perusahaan berbasis TI di Kota Malang yang berfokus dalam *fully customised IT solution* menggunakan metode *Agile* untuk melayani berbagai klien. Dalam menjalankan bisnisnya, perusahaan menerapkan teknologi informasi berupa situs web dalam menyebarkan informasi terkait profil perusahaan, portofolio proyek dan layanan yang ditawarkan. Sebagai salah satu elemen tata kelola yang penting dalam berjalannya proses bisnis perusahaan, penerapan manajemen risiko dapat mempermudah penilaian terhadap kemungkinan risiko yang dapat terjadi (Anugrah, Utami, & Muhammad, 2022). Karena bergerak di bidang jasa, perusahaan juga perlu melakukan pengelolaan terkait risiko TI yang dapat terjadi pada sistem milik klien yang sedang dikembangkan seperti aplikasi tidak dapat diakses, terdapat fitur yang tidak bisa digunakan, server mati, dan lain sebagainya.

Untuk menjaga kualitas sistem, perusahaan menerapkan layanan Sentry.io untuk membantu developer dalam memperbaiki error dan optimasi performa sistem. Namun terkadang dalam penerapannya masih ditemui permasalah iatau hambatan. Saat ini perusahaan belum melakukan pendokumentasian terkait risiko TI yang teridentifikasi, hal tersebut perlu dilakukan guna menentukan skenario risiko TI sebagai acuan dalam mencegah risiko terulang kembali serta imembantu dalam iaktivitas *maintenance* sistem. Kinerja kegiatan dalam perusahaan yang sangat padat menyebabkan aktivitas terkait pengelolaan manajemen risiko perlu dioptimalkan agar tidak mempengaruhi kelancaran jalannya proses bisnis. Karena setiap aktivitas pada perusahaan dapat menimbulkan risiko, maka dari itu dibutuhkan pemetaan untuk mengetahui dampak yang dapat ditimbulkan dari risiko tersebut (Firdaus & Suprapto, 2018). Evaluasi terhadap manajemen risiko teknologi informasi dilakukan untuk mengetahui tingkat kemampuan (*capability level*) sesuai dengan aktivitas yang diterapkan di perusahaan yang kemudian digunakan untuk menentukan nilai kesenjangan (*gap*) sesuai dengan capaian aktivitas yang diharapkan perusahaan. Hasil akhir dari penelitian ini adalah pemberian rekomendasi perbaikan yang dapat digunakan untuk mencapai *capability level* yang diharapkan perusahaan pada proses EDM03 (*Ensured Risk Optimization*) serta APO12 (*Managed Risk*) menggunakan kerangka kerja COBIT 2019.

## 2. LANDASAN KEPUSTAKAAN

Penulis melakukan kajian pustaka pada penelitian yang dilakukan oleh Jauhar Sirajuddin Ar Rajjani dengan judul Evaluasi Manajemen Risiko Teknologi Informasi pada *Department of ICT* PT Semen Indonesia (Persero) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12. Penelitian dilakukan untuk mengetahui tingkat kemampuan Department of ICT dalam mengelola penggunaan TI di perusahaan. Didapatkan hasil bahwa perusahaan mencapai level 3 pada domain EDM03 dan level 2 pada domain APO12 dengan *gap* masing-masing 1 pada setiap prosesnya.

Penelitian ini menggunakan kerangka kerja COBIT yang merupakan suatu kerangka kerja audit tata kelola teknologi informasi yang diterbitkan oleh ISACA serta digunakan sebagai acuan untuk tata kelola dan manajemen teknologi informasi (Rajjani, et al., 2021). COBIT 2019 adalah peningkatan dan pembaharuan dari versi sebelumnya yaitu COBIT 5. *Framework* COBIT 2019 memiliki 6 prinsip utama yaitu *provide stakeholder value* (memberikan nilai atau manfaat bagi pemangku kepentingan), *dynamic governance system* (sistem tata kelola yang dinamis), *holistic approach* (pendekatan secara menyeluruh), *governance distinct from management* (tata kelola yang berbeda dari manajemen), *tailored to enterprise needs* serta *end-to-end governance system* (sistem tata kelola yang mencakup seluruh aspek organisasi)(ISACA, 2019).

Dalam buku *Framework* COBIT 2019 : *Introduction and Methodolgy*, terdapat dua metode dalam menilai tingkat penerapan dari suatu proses yaitu *capability level* dan *maturity*

*level*. *Capability level* terbagi menjadi 6 tingkatan yang mana pada setiap tingkatnya menggambarkan seberapa baik kondisi penerapan dari suatu proses dimulai dari level 0 hingga 5. Tingkat capaian aktivitas dapat dinilai menggunakan pengkategorian skala penilaian yang terbagi menjadi 4 yaitu :

1. Skala N atau *Not* dengan capaian < 15%
2. Skala P atau *Partially* dengan capaian antara 15% - 50%
3. Skala L atau *Largely* dengan capaian antara 50% - 85%
4. Skala F atau *Fully* dengan capaian > 80%.

*Goals Cascade* digunakan untuk menyelaraskan antara tujuan perusahaan dengan tujuan yang berkaitan dengan tujuan yang berkaitan dengan TI. Goals Cascade terdiri dari empat tahap yaitu : *Stakeholder Drivers and Needs,nEnterprise Goals,nAlignment Goals* dan *Governance andnManagement Objectives* yang terdiri dari 1 domain *governance area* dan 3 domain *management area.* Objektif proses dari COBIT 2019 yang membahas tentang manajemen risiko adalah proses EDM03 (*Ensured Risk Optimization*) dengan tiga *governance practice* serta APO12 (*Managed Risk*) dengan enam *management practice*. Proses EDM03 memastikan bahwa tingkatan risiko dan toleransi yang dapat diterima perusahaan telah dipahami dan dikomunikasikan dengan baik, serta memastikan apakah risiko TI telah diidentifikasi dan dikelola dengan baik. Sedangkan APO12 digunakan untuk mengidentifikasi dan menilai risiko TI agar tidak melebihi batasan tingkat toleransi yang telah ditentukan organisasi.

RACI *Chart* digunakan untuk mengidentifikasi peran serta tanggung jawab dari pihak-pihak yang berkaitan dalam sebuah aktivitas. Pendefinisian peran dalam RACI *Chart* terbagi menjadi empat yaitu *Responsible* (R),n*Accountable* (A),n*Consulted* (C) dan *Informed* (I). Pada kerangka kerja COBIT 2019, hanya orang dengan posisi *Responsibleni*(R) dan *Accountablemi*(A) yang dapat dijadikan narasumber pada penelitian. Dalam menganalisis data, aktivitas dapat dikatakan tercapai apabila telah dilengkapi dengan dokumen atau artefak pendukung sesuai *outputs* yang tertuang dalam komponen *informations flows and items* pada buku *Framework* COBIT 2019 : *Governance and Management Objective*. Karena penelitian berfokus pada proses EDM03 dan APO12, maka berikut adalah informasi dan artefak pendukung yang harus dimiliki untuk mendukung kelengkapan capaian aktivitas pada proses EDM03.

Tabel 1. Outputs Proses EDM03
Sumber : (ISACA, 2018)

| *Governance Practice* | Outputs |
|---|---|
| EDM03.01 | Panduan risiko yang dapat diterima (*risk appetite*) |
| | Aktivitas evaluasi manajemen risiko |
| | Batas tingkat toleransi dari risiko TI yang telah disetujui |
| EDM03.02 | Proses pengukuran manajemen risiko yang telah disetujui |
| | Tujuan utama yang dipantau untuk manajemen risiko |
| | Aturan manajemen risiko |
| EDM03.03 | Tindakan remedial untuk memperbaiki kesalahan dari penelolaan manajemen risiko |
| | Laporan isu manajemen risiko bagi dewan atau komite eksekutif |

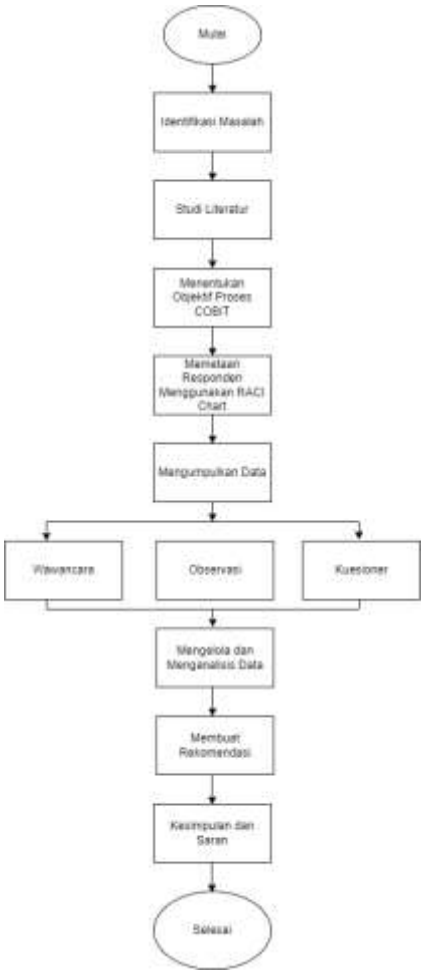
Selanjutnya terdapat *outputs* mendukung kelengkapan capaian aktivitas pada proses APO12.

Tabel 2. Outputs Proses APO12
Sumber : (ISACA, 2018)

| *Management Practice* | Outputs |
|---|---|
| APO12.01 | Masalah dan faktor penyebab risiko yang muncul |
| | Data kejadian risiko beserta faktor penyebabnya |
| | Data pada lingkungan operasi yang berhubungan dengan risiko |
| APO12.002 | Hasil analisis risiko |
| | Skenario risiko teknologi informasi |
| | Ruang lingkup upaya analisis risiko |
| APO12.03 | Profil risiko, termasuk status tindakan manajemen risiko |
| | Dokumen skenario risiko berdasarkan kategori lini bisnis dan fungsi |
| APO12.04 | Dokumen skenario risiko berdasarkan lini bisnis dan fungsi |
| | Hasil penaksiran risiko dari pihak ketiga |
| | Potensi atau peluang dalam menerima risiko yang lebih besar |
| APO12.05 | Proposal proyek untuk meminimalisir risiko |
| APO12.06 | Komunikasi dampak risiko |
| | Penyebab utama risiko |

| | |
|---|---|
| | Rencana respon terkait insiden risiko |

## 3. METODOLOGI




Gambar 1. Metodologi Penelitian

Pertama penulis melakukan identifikasi masalah guna mendapatkan pemahaman terkait gambaran umum terkait kondisi perusahaan serta fokus permasalahan yang ada disana. Kedua, melakukan studi literatur untuk mengumpulkan dasar-dasar teori sebagai gambaran dasar serta referensi terkait topik dan studi kasus yang dipilih. Ketiga, menentukan objektif proses menggunakan *Goals Cascade* sesuai buku panduan *Framework* COBIT 2019 : *Introduction and Methodology*. Peneliti memetakan visi misi perusahaan dengan *enterprise goals* dan *alignment goals* hingga mendapatkan *management objective* yang sesuai dengan kebutuhan perusahaan. Keempat, memetakan responden penelitian menggunakan RACI *Chart* pada proses EDM03 dan APO12. Kelima, melakukan pengumpulan data primer melalui kegiatan wawancara, observasi, dan penyebaran kuesioner. Kuesioner dibagikan sesuai dengan *level* dari proses sesuai buku COBIT 2019 : *Governance and Management Objectives*. Setiap tingkat berisi pertanyaan yang berbeda sesuai dengan *activity* yang ada pada *level* tersebut. Keenam, melakukan pengelolaan data dilakukan dengan memetakan kondisi antara aktivitas dari proses EDM03 dan APO12 dengan aktivitas perusahaan untuk menentukan tingkat kemampuan (*capability level*) perusahaan saat ini serta nilai *gap* dari kondisi yang diharapkan. Penilaian dilakukan secara bertahap dan akan berhenti apabila penerapan aktivitas yang tercapai < 85%. Ketujuh, melakukan penyusunan rekomendasi perbaikan berdasarkan hasil analisis terhadap tingkat kemampuan (*capability level*) dan *gap*. Hasil rekomendasi diharapkan mampu membantu perusahaan dalam mencapai keadaan yang diharapkan. Terakhir, membuat kesimpulan dan saran yang berisi hasil *capability level* manajemen risiko teknologi informasi beserta rekomendasinya dan juga saran pagi penelitian selanjutnya.

## 4. HASIL

Pada tahap ini akan dilakukan penentuan *governance and management objectives* yang akan digunakan dalam penelitian menggunakan *Goals Cascade* sesuai buku panduan *Framework* COBIT 2019 : Introduction and Methodology *dengan* menggali *Stakeholder Drivers and Needs* menggunakan visi dan misi perusahaan, memetakan *Enterprise Goals* (tujuan perusahaan), kemudian disesuaikan dengan *Alignment Goals* serta *Governance and Management Objectives.*

### 4.1 *Enterprise Goals*

Mengidentifikasi tujuan bisnis dari PT XYZ yang akan diselaraskan dengan *Enterprise Goals* sesuai visi dan misi perusahaan.

Tabel 3. *Mapping Enterprise Goals*

| *Tujuan* | *Enterprise Goals* | *Kode* |
|---|---|---|
| Visi | Portofolio produk dan layanan kompetitif | EG01 |
| | Inovasi produk dan bisnis | EG13 |
| | Risiko bisnis terkelola | EG02 |
| Misi | Keberlanjutan dan ketersediaan layanan bisnis | EG06 |
| | Kualitas informasi manajemen | EG07 |
| | Keterampilan staf, motivasi dan produktivitas | EG10 |
| | Budaya layanan berorientasi pelanggan | EG05 |

### 4.2 *Alignment Goals*

Selanjutnya, melakukan identifikasi *Alignment Goals* berdasarkan hasil *Enterprise Goals*. *Alignment Goals* ditentukan menggunakan *mapping table* dari *Enterprise Goals* yang mendapat nilai "**P**" yang berarti *Primer.*

Tabel 4. *Mapping Alignment Goals*

| EG | *Alignment Goals* | Kode |
|---|---|---|
| 01 | Penyampaian layanan IT sejalan dengan kebutuhan bisnis | AG05 |
| | Kelincahan untuk mengubah persyaratan bisnis menjadi solusi operasional | AG06 |
| | Mengaktifkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi | AG08 |
| | Penyampaian program tepat waktu, sesuai anggaran dan memenuhi persyaratan dan standar kualitas | AG09 |
| | Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis | AG13 |
| 02 | Risiko terkait IT yang dikelola | AG02 |
| | Keamanan informasi, infrastruktur pemrosesan, aplikasi dan privasi | AG07 |
| 05 | Mengaktifkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi | AG08 |
| 06 | Keamanan informasi, infrastruktur pemrosesan, aplikasi dan privasi | AG07 |
| 07 | Kualitas informasi keuangan terkait teknologi | AG04 |
| | Kualitas informasi manajemen IT | AG10 |
| 10 | Staf yang kompeten dan termotivasi dengan pemahaman bersama tentang teknologi dan bisnis | AG12 |
| 13 | Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis | AG13 |

### 4.3 *Governance and Management Objective* (GMO)

Tahap selanjutnya yaitu memetakan *Governance and Management Objective* sesuai hasil identifikasi *Alignment Goals.* GMO ditentukan melalui penggunaan *mapping table* dari *Alignment Goals* yang bernilai "**P**" sesuai dengan kerangka kerja COBIT 2019.

Tabel 5. *Mapping Governance and Management Objective*

| *Alignment Goals* | Proses COBIT 2019 dengan skala prioritas (P) |
|---|---|
| AG02 | EDM03, APO12, DSS05 |
| AG04 | APO06, BAI08 |
| AG05 | APO05, APO08, APO09, APO10, BAI02, BAI03, DSS02, DSS03, DSS04, MEA01 |
| AG06 | APO03, APO04, APO08, BAI02, BAI03, BAI06, BAI07, BAI11 |
| AG07 | EDM03, APO12, APO13, BAI10, DSS04, DSS05 |
| AG08 | APO02, APO03, BAI05, DSS06 |
| AG09 | EDM04, APO06, APO11, BAI01, BAI02, BAI03, BAI05, BAI11 |
| AG10 | EDM05, APO11, APO14, MEA01 |
| AG12 | APO07, APO08, BAI08 |
| AG13 | APO04, APO07, APO08, BAI08 |

Berdasarkan hasil pemetaan *Governance and Management Objective* dari *Alignment Goals*, AG02 dinilai selaras dengan rencana strategis PT XYZ dalam mewujudkan tujuan perusahaan yaitu menjadi perusahaan terdepan dalam industri teknologi informasi / TI yang tak terbatas dengan mengelola kemungkinan risiko yang dapat terjadi sehingga dapat terus mempertahankan kualitas sistem serta kepercayaan dari para pemangku kepentingan dan juga pelanggan. Proses EDM03 dan APO12 akan digunakan sebagai proses yang akan dievaluasi sebagai batasan ruang lingkup penelitian yang hanya berfokus pada tata kelola manajemen risiko TI.

### 4.4 RACI *Chart*

Langkah selanjutnya adalah melakukan pemetaan RACI *Chart* untuk menentukan responden penelitian. Berikut adalah hasil pemetaan RACI *Chart* dengan struktur organisasi perusahaan pada proses EDM03 dan APO12.

Tabel 6. Pemetaan RACI *Chart* EDM03

| Pihak | Struktur RACI COBIT 2019 | Struktur Organisasi |
|---|---|---|
| R | *Chief Risk Officer* | *Project Director* |
| A | *Board* | *Business Director* |

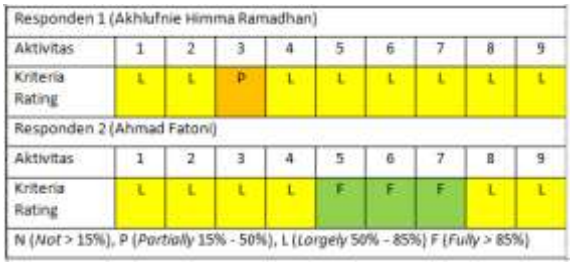
Tabel 7. Pemetaan RACI *Chart* APO12

| Pihak | Struktur RACI COBIT 2019 | Struktur Organisasi |
|---|---|---|
| R | *Business Process Owners* | *Business Director* |
| A | *Chief Risk Officer* | *Project Director* |

Berdasarkan hasil pemetaan RACI *Chart* proses EDM03 dan APO12, maka responden yang akan terlibat dalam penelitian ini adalah *Business Director* dan *Project Director.*

### 4.5 Hasil Kuesioner Responden

Pengisian kuesioner dilakukan untuk mendapatkan gambaran terkait pengelolaan risiko yang ada di perusahaan sesuai sudut pandang responden. Pengisian kuesioner dilakukan dengan memberikan skala penilaian (N, P, L, F) terhadap aktivitas pada *capability level* 2 oleh *Business Director* yang berperan sebagai responden 1 dan *Project Director* yang berperan sebagai responden 2.



| Responden 1 (Akhlufnie Himma Ramadhan) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Aktivitas | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Kriteria Rating | L | L | P | L | L | L | L | L | L |
| Responden 2 (Ahmad Fatoni) | | | | | | | | | |
| Aktivitas | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Kriteria Rating | L | L | L | L | F | F | F | L | L |

N (*Not* > 15%), P (*Partially* 15% - 50%), L (*Largely* 50% - 85%) F (*Fully* > 85%)

Gambar 2. Hasil Kuesioner EDM03

Hasil pengisian kuesioner oleh dua responden pada proses EDM03 menunjukkan bahwa responden menilai penerapan aktivitas *capability level* 2 pada perusahaan telah mencapai > 50% dengan mayoritas rating L namun belum sepenuhnya mencapai rating *Fully*. Terdapat satu aktivitas yang penerapannya dinilai < 50%. Sedangkan hasil kuesioner untuk proses APO12 dapat dilihat pada gambar dibawah.

| Responden 1 | | | | | | |
|---|---|---|---|---|---|---|
| Aktivitas | 1 | 2 | 3 | 4 | 5 | 6 |
| Kriteria Rating | F | P | P | L | L | L |
| Responden 2 | | | | | | |
| Pernyataan | 1 | 2 | 3 | 4 | 5 | 6 |
| Kriteria Rating | L | P | P | P | L | L |

N (*Not* > 15%), P (*Partially* 15% - 50%), L (*Largely* 50% - 85%) F (*Fully* > 85%)

Gambar 3. Hasil Kuesioner APO12

Pada proses APO12, responden menilai penerapan aktivitas *capability level* 2 pada perusahaan belum sepenuhnya mencapai > 50% yang mana terlihat dari adanya beberapa aktivitas yang penerapannya masih < 50% dengan ratng P. Namun hasil kuesioner masih harus disesuaikan kembali dengan penerapan aktivitas serta dokumen pendukung untuk mengetahui tingkat kemampuan (*capability level*) yang sebenarnya dicapai oleh perusahaan.

### 4.6 Penilaian Tingkat Kemampuan (*Capability Level*)

Selanjutnya dilakukan penilaian proses EDM03 (*Ensured Risk Optimization*) dan APO12 (*Managed Risk*) untuk memvalidasi kondisi antara aktivitas dari proses EDM03 dan APO12 pada *capability level* 2 dengan aktivitas yang sebenarnya terjadi di perusahaan berdasarkan hasil wawancara yang telah dilakukan bersama responden serta hasil observasi berupa dokumen bukti yang diberikan. Komponen *outputs information flow and items* digunakan sebagai acuan pendukung dari kelengkapan informasi dan dokumen yang berkaitan dengan pelaksanaan aktivitas *capability level* 2 sesuai buku panduan COBIT 2019 : *Governance and Management Objectives*.

Tabel 8. Pemetaan Aktivitas *Capability Level* 2 EDM03

| Akti-vitas | *Outputs* | Kondisi pada Organisasi |
|---|---|---|
| *Governance Practice* EDM03.01 | | |
| 1 | Panduan risiko yang dapat diterima (*risk appetite*) | Belum teridentifikasi<br>Dok : - |
| 2 | Panduan risiko yang dapat diterima (*risk appetite*) | Belum teridentifikasi<br>Dok : - |
| 3 | Tingkat toleransi risiko yang telah disetujui | Belum terdokumentasi<br>Dok : - |
| 4 | Aktivitas evaluasi manajemen risiko | Belum teridentifikasi<br>Dok : - |
| *Governance Practice* EDM03.02 | | |
| 1 | Proses pengukuran manajemen risiko yang telah disetujui | Terdefinisikan melalui pelaksanaan UAT dan skenario tes<br>Bukti : Dokumen UAT dan tes skenario |
| 2 | Aturan manajemen risiko | Teridentifikasi melalui kegiatan *daily meeting* dan penerapan Sentry.io<br>Bukti : Catatan *Error Monitoring* |
| 3 | Aturan manajemen risiko | Mengimplementasikan mekanisme respon risiko melalui penerapan Sentry.io<br>Bukti : Catatan *Error Monitoring* |
| 4 | Aturan manajemen risiko | Mengarahkan pengidentifikasian risiko dan pelaporannya melalui layanan Sentry.io<br>Bukti : Catatan *Error Monitoring* |
| *Governance Practice* EDM03.03 | | |
| 1 | Laporan isu manajemen risiko untuk dewan atau komite eksekutif | Belum terdokumentasi<br>Dok : - |

Dari pemetaan didapatkan hasil bahwa terdapat 4 aktivitas yang dikategorikan tercapai yaitu aktivitas pada *governance practice* EDM03.02 yang mana dalam memonitoring risiko perusahaan dibantu dengan penggunaan

layanan Sentry.io. Selanjutnya dilakukan penentuan skala rating proses sesuai buku pedoman COBIT 2019 : *Framework Introduction and Methodology* yang diterbitkan oleh ISACA. Penilaian skala rating diperoleh melalui perhitungan jumlah aktivitas beserta dokumen pendukung yang tercapai dibagi dengan keseluruhan aktivitas pada g*overnance practice* kemudian dikali 100% (Wulandari, Atrinawati, & Putra, 2022). Sehingga hasil akhir untuk proses EDM03 (*Ensured Risk Optimization*) didapatkan persentase sebesar 44,44% dengan skala rating P (*Partially*). Hal ini menandakan bahwa penilaian berhenti pada tingkat kemampuan atau *capabiity level* 2 dengan hasil bahwa tingkat kemampuan (*capability level*) perusahaan berada pada level 1 yaitu proses telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang masih kurang lengkap dan tidak terlalu terorganisir sehingga dapat dikategorikan sebagai langkah intuitif.

Tabel 9. Pemetaan Aktivitas *Capability Level* 2 APO12

| Akti-vitas | *Outputs* | Kondisi pada Organisasi |
|---|---|---|
| *Management Practice* APO12.01 | | |
| 1 | Masalah dan faktor risiko yang muncul | Perusahaan memiliki catatan klasifikasi isu dasar serta tingkat prioritas penanganannya.<br>Bukti : Catatan Klasifikasi Isu |
| 2 | Catatan operasional yang berkaitan dengan risiko | Belum terdokumentasi<br>Bukti : - |
| *Management Practice* APO12.03 | | |
| 1 | Dokumen skenario risiko berdasarkan fungsi dan lini bisnis | Belum teridentifikasi<br>Bukti : - |
| 2 | Profil risiko, termasuk status tindakan manajemen risiko | Belum teridentifikasi<br>Bukti : - |
| 3 | Dokumen skenario risiko berdasarkan fungsi dan lini bisnis | Belum teridentifikasi<br>Bukti : - |
| *Management Practice* APO12.05 | | |
| 1 | Proposal proyek untuk meminimalisir risiko | Teridentifikasi melalui penggunaan Sentry.io dan tes skenario<br>Bukti : *Catatan Error Monitoring* dan Dokumen skenario *testing* |

Dari pemetaan didapatkan hasil bahwa terdapat 2 aktivitas yang dikategorikan tercapai yaitu aktivitas 1 pada *management practice* APO12.01 dan aktivitas 1 pada *management practice* APO12.05. Selanjutnya dilakukan penentuan skala rating proses sesuai buku pedoman *Framework* COBIT 2019 : *Introduction and Methodology*. Skala rating didapatkan melalui perhitungan jumlah aktivitas beserta bukti yang tercapai dibagi dengan total aktivitas g*overnance practice* kemudian dikali 100% (Wulandari, Atrinawati, & Putra, 2022). Sehingga hasil akhir untuk proses APO12 (*Managed Risk*) didapatkan persentase sebesar 33,33% dengan skala rating P (*Partially*). Hal ini menandakan bahwa penilaian berhenti pada tingkat kemampuan atau *capabiity level* 2 dengan capaian bahwa tingkat kemampuan (*capability level*) perusahaan berada pada level 1 yaitu proses telah mencapai tujuannya melalui penerapan serangkaian kegiatan yang masih kurang lengkap dan tidak terlalu terorganisir sehingga dapat dikategorikan sebagai langkah intuitif.

## 5. PEMBAHASAN

Setelah melakukan penelitian terhadap *Capability Level* menggunakan proses EDM03 dan APO12 kerangka kerja COBIT 2019, maka selanjutnya pada bab ini akan dilakukan analisis kesenjangan (Gap) antara *capability level* yang ada saat ini dengan *capability level* yang diharapkan oleh perusahaan. Nantinya selisih dari *Capability Level* tersebut akan digunakan untuk mendapatkan nilai *Gap*. Berdasarkan hasil wawancara, target capaian level yang diharapkan adalah satu tingkat diatas level yang telah berhasil dicapai oleh perusahaan saat ini.

Tabel 10. Analisis Kesenjangan (*Gap*) pada Seluruh Proses

| Proses | Level saat ini | Level target | Gap |
|---|---|---|---|
| EDM03 (*Ensured Risk Optimization*) | 1 | 2 | 1 |
| APO12 (*Managed Risk*) | 1 | 2 | 1 |

### 5.1 Analisis Kesenjangan (*Gap*) EDM03

Berikut adalah aktivitas yang belum diterapkan secara optimal dan perlu diperbaiki oleh perusahaan sehingga belum mencapai level 2 pada proses EDM03 :

1. Belum mengidentifikasi selera risiko yang dapat diambil perusahaan terkait risiko TI.
2. Belum secara tertulis memetakan konteks terkait tingkat toleransi risiko (*risk tolerance*) terhadap selera risiko (*risk appetite*) yang dapat diterima oleh perusahaan sesuai tingkat dampak yang ditimbulkan (*low*, *medium*, atau *high*).
3. Belum menerapkan kegiatan dalam evaluasi untuk meninjau keselarasan antara strategi risiko TI dengan strategi risiko perusahaan.
4. Perlu adanya perbaikan dokumen terkait aturan manajemen risiko TI .
5. Belum menerapkan prosedur secara tertulis terkait pendokumentasian risiko yang terjadi kepada komite eksekutif.

5.2 Analisis Kesenjangan (*Gap*) APO12

Berikut adalah aktivitas yang belum diterapkan secara optimal dan perlu diperbaiki oleh perusahaan sehingga belum mencapai level 2 pada proses EDM03 :

1. Belum mencatat data risiko TI secara konsisten pada lingkungan operasional perusahaan.
2. Belum mengidentifikasi risiko TI dan mendokumentasikannya kedalam profil risiko TI perusahaan.
3. Belum memetakan skenario risiko TI yang telah atau dapat terjadi berdasarkan kategori dan lini bisnis.

5.3 Rekomendasi EDM03 (*Ensured Risk Optimization*)

Berdasarkan hasil penilaian *capability level* yang telah dilakukan, dibuatlah rekomendasi berdasarkan aktivitas yang belum terpenuhi, antara lain :

1. Mengidentifikasi selera risiko TI dalam memenuhi tujuan strategis terkait jumlah dan jenis risiko yang dapat diambil perusahaan serta dampaknya sebagai acuan dalam mengelola risiko.
2. Melakukan pemetaan toleransi risiko TI yang dapat diterima oleh perusahaan. Risiko tersebut kemudian dikategorikan sesuai dengan dampak yang dapat ditimbulkan dan pengaruhnya terhadap aktivitas bisnis perusahaan, apakah risiko tersebut berdampak rendah, sedang, hingga tinggi. Pemetaan dilakukan dengan mempertimbangkan segala aspek yang berkaitan dengan tingkat stabilitas kegiatan operasional, ketersediaan, perlindungan hingga perbaikan layanan TI yang dapat mengakibatkan kerusakan atau mengurangi nilai perusahaan.
3. Menentukan metode atau aktivitas yang sesuai untuk memantau dan mengevaluasi penerapan risiko sehingga tidak melebihi kapasitas yang mampu diterima perusahaan. Perusahaan dapat melakukan pembentukan strategi pengelolaan risiko TI yang meliputi kondisi atau keadaan yang membutuhkan tindakan, urutan tindakan dari tinggi ke rendah, waktu pelaksanaan, isu-isu yang muncul, personil yang terlibat hingga prosedur pelaksanaan. Hal tersebut dilakukan sebagai langkah agar risiko TI tidak melebihi tingkat toleransi risiko serta selaras dengan strategi risiko perusahaan.
4. perusahaan harus mampu mendokumentasikan dengan lengkap dan terstruktur terkait aturan manajemen risiko TI yang mengatur mekanisme komunikasi risiko dari seluruh aktivitas bisnis perusahaan. Setelah dipahami dan dikategorikan, strategi manajemen risiko harus dikomunikasikan dengan jelas agar dapat dengan mudah dipahami.
5. Menetapkan persyaratan terkait dokumentasi atau pencatatan risiko TI khususnya pada proses optimasi risiko. Perusahaan setidaknya memiliki prosedur atau persyaratan dalam melakukan pendokumentasian yang baik terutama terkait rincian isi kontennya, seperti gambaran seberapa besar risiko yang terjadi serta toleransi yang mampu diterima oleh perusahaan. Output dari kebijakan ini diharapkan dapat membantu semua pihak yang terlibat dalam memahami seluruh aktivitas khususnya terkait pengelolaan risiko TI dengan lebih baik.

5.4 Rekomendasi APO12 (*Managed Risk*)

Berdasarkan hasil penilaian *capability level* yang telah dilakukan, dibuatlah rekomendasi berdasarkan aktivitas yang belum terpenuhi, antara lain :

1. Menetapkan aktivitas pencatatan risiko Ti yang terjadi pada lingkup operasional perusahaan secara lebih konsisten dan berkala.
2. Mendokumentasikan profil risiko TI beserta

langkah perbaikan serta isu yang muncul secara optimal sehingga dapat digunakan sebagai gambaran terkait berbagai dampak potensial dari risiko TI yang dapat menghambat dan mengganggu aktivitas perusahaan.

3. Memetakan skenario terkait potensi ancaman dan risiko yang berkaitan dengan teknologi informasi. Penting bagi perusahaan untuk menentukan perkiraan kejadian buruk yang dapat timbul saat ini atau di masa depan dalam lingkup bisnis perusahaan serta menganalisa ancaman dan potensi kerentanan terhadap sistem TI yang digunakan serta dampak yang mengarah pada besarnya bahaya atau dampak yang mampu ditimbulkan oleh ancaman tersebut sehingga perusahaan memiliki gambaran terkait tingkat kerentanan komponen sistem TI untuk meminimalkan terjadinya risiko TI.

## 6. KESIMPULAN DAN SARAN

### 6.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, maka dapat diperoleh kesimpulan sebagai berikut :

1. Tingkat kemampuan (*capability level*) berdasarkan hasil penilaian yang telah dilakukan terhadap kondisi tata kelola manajemen risiko yang saat ini diterapkan oleh perusahaan dengan proses pengambilan data melalui kegiatan wawancara, observasi, serta penyebaran kuesioner kepada responden yang ditentukan melalui pemetaan RACI *Chart* mendapatkan hasil khir bahwa tingkat kemampuan (*capability level*) yang dicapai pada obyektif proses EDM03 (*Ensured Risk Optimization*) berada pada level 1 dimana penerapannya kurang lebih telah mencapai tujuan yang dikategorikan sebagai awal atau intuitif melalui penerapan kegiatan yang kurang lengkap dan tidak terorganisir dengan baik. Untuk proses APO12 (*Managed Risk*), PT XYZ berada pada level 1 dimana prosesnya kurang lebih telah mencapai tujuan melalui penerapan layanan Sentry.io untuk proses pemantauan risiko, namun hal yang berkaitan dengan risiko TI masih didokumentasikan secara insidental sehingga dikategorikan sebagai intuitif. Target capaian tingkat kemampuan (*capability level*) yang diharapkan oleh perusahaan berada pada satu tingkat diatas level yang telah berhasil dicapai oleh perusahaan saat ini. Sehingga kesenjangan (*gap*) pada proses EDM03 dan APO12 dalam mencapai level yang diharapkan yaitu level 2 bernilai 1 untuk setiap prosesnya.
2. Tingkat kemampuan yang diharapkan pada proses EDM03 adalah level 2 yaitu satu tingkat diatas capaian tingkat kemampuan saat ini. Untuk mencapai tingkat kemampuan sesai dengan yang diinginkan, perusahaan diharapkan dapat mempertimbangkan beberapa rekomendasi yang dapat diterapkan yaitu mengidentifikasi selera risiko TI dalam memenuhi tujuan strategis perusahaan, memetakan toleransi risiko yang dapat diterima perusahaan, menentukan metode yang tepat untuk memonitor dan mengevaluasi kegiatan pengelolaan dari risiko TI sehingga tidak melebihi kapasitas yang mampu diterima perusahaan, mendokumentasikan dengan lengkap dan terstruktur terkait kebijakan manajemen risiko TI serta menetapkan persyaratan terkait dokumentasi atau pencatatan risiko TI. Selanjutnya pada proses APO12, tingkat kemampuan yang diharapkan adalah satu tingkat diatas capaian tingkat kemampuan satu ini yaitu level 2. Untuk mencapai tingkat kemampuan yang diinginkan, perusahaan diharapkan dapat mempertimbangkan beberapa rekomendasi yang dapat diterapkan yaitu menetapkan aktivitas pencatatan dan pengelolaan risiko TI pada lingkup operasional, mendokumentasikan profil risiko TI beserta langkah perbaikannya sebagai gambaran dampak potensial yang dapat menghambat aktivitas perusahaan serta memetakan skenario potensi ancaman dan risiko TI untuk memperkirakan kejadian buruk yang dapat timbul saat ini atau di masa depan.

### 6.2 Saran

Saran yang dapat diberikan oleh penulis dalam mengembangkan lebih lanjut terkait penelitian evaluasi tata kelola teknologi informasi untuk peneliti selanjutnya adalah sebagai berikut :

1. Penelitian selanjutnya dapat melanjutkan evaluasi terhadap obyektif proses EDM03 dan APO12 seperti yang telah digunakan pada penelitian ini untuk mengetahui perkembangan dari perbaikan terhadap penerapan aktivitas pada proses tersebut kedepannya.

2. Penelitian selanjutnya dapat menggunakan fokus yang berbeda dengan penelitian ini dalam mengevaluasi sebuah perusahaan menggunakan proses yang ada pada kerangka kerja COBIT 2019. Seperti fokus pada keamanan TI menggunakan proses APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*).
3. Mengenai pengembangan penelitian menggunakan fokus yang sama yaitu manajemen risiko TI, dapat menggunakan standar kerangka kerja selain COBIT 2019 seperti ISO 31000 dan ITIL (*Information Technology Infrastructure Library*).

## 7. DAFTAR PUSTAKA


Anugrah, R., Utami, E., & Muhammad, A. (2022). Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO12. *Jurnal Ilmiah Universitas Batanghari Jambi*, 991-995.

Firdaus, N., & Suprapto. (2018). Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 91-100.

ISACA. (2018). Governance and Management Objectives. In COBIT® *2019 Framework.* https://www.isaca.org/resources/cobit

ISACA. (2018). COBIT® 2019 Framework: Introduction & Methodology. In *www.isaca.org/COBITuse*.

Kurnia, H. M., Shofa, R. N. & Rianto. (2018). Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Berdasarkan Domain APO12. *Jurnal Sistem Informasi dan Teknologi*, 1(2), pp. 99-106.

Sofa, K., Suryanto, T., & Suryono, R. (2020). Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus. *Jurnal Teknologi dan Sistem Informasi (JTSI)*, 39-46.

Rajjani, J. S. A., Hanggara, B. T. & Musityo, Y. T. (2021). Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Persero) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 5(5), pp. 1734-1744.

Windasari, I., Rochim, A., Alfiani, S., & Kamalia, A. (2021). Audit Tata Kelola Teknologi Informasi Domain Monitor,Evaluate, and Asses dan Deliver, Service, Support. *Jurnal Sistem Informasi Bisnis (JSINBIS)*, 131-138.

Wulandari, E., Atrinawati, L., & Putra, M. (2022). Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan Framework Cobit 2019 pada PT XYZ Balikpapan. *DoubleClick: Journal of Computer and Information Technology*, 127-138.