# Analisis Manajemen Risiko pada PT. XYZ Menggunakan COBIT 2019 dengan Domain EDM03, APO12, APO13, dan DSS05

## *Risk Management Analysis of PT XYZ Using COBIT 2019 with Domain EDM03, APO12, APO13, and DSS05*

**[1]Riskila Yulita*, [2]Johan J.C Tambotoh**
[1,2]Prodi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[1,2]Jl. Dr. O. Notohamidjojo, Blotongan, Kec. Sidorejo, Kota Salatiga, Jawa Tengah 50715, Indonesia
*e-mail: 682020028@student.uksw.edu

(***received*:** 29 July 2024, ***revised*:** 1 August 2024, ***accepted*:** 16 August 2024)

**Abstrak**

Teknologi yang terus berkembang secara tidak langsung memaksa masyarakat untuk beradaptasi terhadap perkembangan tersebut. Peran penting teknologi menjadi semakin terasa di masa pandemi COVID-19 ini ketika seluruh aktivitas dunia lumpuh dan hanya diperbolehkan berkomunikasi secara online. Namun, manfaat teknologi yang begitu besar juga berbanding lurus dengan risiko yang mungkin terjadi. Oleh karena itu, Manajemen Risiko TI sangat dibutuhkan untuk memitigasi sumber potensi yang mengancam. Penelitian ini bertujuan untuk menganalisis manajemen risiko TI dengan mengukur tingkat kapabilitas, analisis gap dan memberikan rekomendasi perbaikan menggunakan kerangka kerja COBIT 2019 untuk mendukung kinerja dan keamanan TI PT XYZ. Peneliti menggunakan metode kualitatif dengan teknik pengumpulan data melalui observasi, wawancara, dan kuesioner. Hasil penelitian menyatakan domain manajemen risiko yang menjadi fokus penelitian yaitu EDM03, APO12, APO13, dan DSS05 memiliki gap antara kapabilitas yang diharapkan dengan yang terjadi di perusahaan. Oleh karena itu, diperlukan rekomendasi perbaikan seperti menentukan tingkat risiko TI dan mensosialisasikannya kepada pemangku kepentingan, melakukan pencatatan kejadian risiko TI, membangun *Information Security Management System* (ISMS), menerapkan mekanisme penyaringan jaringan, dan mengevaluasi secara berkala informasi mengenai potensi ancaman baru dengan meninjau keamanan produk dan layanan vendor atau pihak ketiga.

**Kata kunci:** manajemen risiko, tingkat kapabilitas, faktor desain, COBIT 2019

***Abstract***

*Technology that continues to develop indirectly forces people to adapt to these developments. The vital role of technology is becoming increasingly felt during the COVID-19 pandemic when all world activities are paralyzed and only allowed to communicate online. However, the enormous benefits of technology are also directly proportional to the risks that may occur. Therefore, IT Risk Management is needed to mitigate potential sources of threat. This research aims to analyze IT risk management by measuring the level of capability, gap analysis, and providing recommendations for improvement using the COBIT 2019 framework to support PT XYZ's work performance and IT security. Researchers used qualitative methods with data collection techniques through observation, interviews, and questionnaires. The results showed that the risk management domain that was the research focus EDM03, APO12, APO13, and DSS05 had a gap between the expected capabilities and what was happening in the company. Therefore, improvement recommendations are needed, such as determining the level of IT risk and socializing it with stakeholders, recording IT risk events, building an Information Security Management System (ISMS), implementing a network filtering mechanism, and regularly evaluating information about potential new threats by reviewing product security and vendor or third-party services.*

***Keywords:*** *risk management, capability level, design factors, COBIT 2019*

 ISSN:2302-8149
e-ISSN:2540-9719

## 1 Pendahuluan

Teknologi informasi selalu berkembang membuat berbagai perusahaan melakukan berbagai adaptasi untuk mengikuti perkembangan yang ada. Efek dari adaptasi implementasi terhadap perkembangan teknologi yang sedang terjadi lebih terasa pada era pandemi COVID-19. Selama masa tersebut seluruh sektor usaha di dunia lumpuh dan mengalami penurunan, namun kembali membaik pada pertengahan tahun 2023 setelah COVID-19 ditetapkan tidak lagi menjadi keadaan darurat kesehatan internasional oleh WHO [1]. Pernyataan tersebut menjadi titik balik bagi perusahaan-perusahaan dunia untuk memperbaiki seluruh kerugiannya, sekaligus mengubah pandangan terhadap peran teknologi yang awalnya hanya sebagai unsur pendukung menjadi bagian inti dari proses berkembangnya sebuah perusahaan. Salah satu perusahaan yang terkena dampak besar dari pandemi yaitu PT. XYZ, dikarenakan bergerak pada sektor layanan transportasi bus dalam negeri. Fokus implementasi TI pada PT. XYZ untuk menyediakan informasi pelanggan dan pusat pengelolaan data perusahaan dalam bentuk website. Terdapat dua website, yaitu "*Bus XYZ"* yang dapat diakses pelanggan berisi informasi umum serta layanan perusahaan dan "*Bus XYZ Reservation System"* yang hanya dapat diakses oleh karyawan internal untuk melakukan *booking* layanan, penyimpanan dan pengelolaan data sesuai pesanan serta cek pembayaran yang sudah diinput.

Teknologi informasi dalam penerapannya perlu diperhatikan mengingat risiko yang dapat terjadi kapanpun diluar dari manfaat yang ada, sehingga perlu dilakukan manajemen risiko sebagai bentuk pengawasan yang menyeluruh. Manajemen risiko merupakan proses penanganan dan identifikasi terhadap sebuah ancaman teknologi yang digunakan oleh perusahaan melalui manajer TI, dengan tujuan untuk meminimalisir tingkat risiko operasional, mencapai tujuan perusahaan dan menyetimbangkan pendapatan perusahaan dalam mencapai keuntungan [2]. Manajemen risiko dilakukan untuk mengurangi kemungkinan terjadinya risiko, menghindari risiko, mengalihkan risiko, dan mengurangi dampak risiko yang terjadi [3]. Berdasarkan wawancara dengan beberapa karyawan, penelitian mengenai analisis manajemen risiko dan performa perusahaan pada PT. XYZ belum pernah dilakukan. Penelitian yang pernah dilakukan masih terkait rancang bangun dan perancangan strategis sistem informasi. Melihat hal tersebut, membuat perusahan belum memiliki dokumen standar berisi catatan risiko yang terjadi berdasarkan performa perusahaan, beserta dengan rekomendasi penanganan risiko untuk mengatur risiko yang ada. Proses analisis manajemen risiko dan performa perusahaan dapat dilakukan secara bersamaan dengan memanfaatkan *framework* COBIT (*Control Objective for Information and Related Technology*). COBIT merupakan *framework* tata kelola dan manajemen TI yang bisa digunakan untuk seluruh organisasi untuk mencapai tujuan [4] [5].

*Framework* COBIT mengalami penyempurnaan seiring berjalannya waktu oleh ISACA dan saat ini versi terbaru adalah COBIT 2019. COBIT 2019 berisi kerangka gabungan antara manajemen organisasi dan tata kelola dengan menghadirkan model analitik untuk dapat diterima secara menyeluruh, tujuannya untuk menaikkan nilai serta kepercayaan pada sistem informasi [6]. COBIT 2019 berkontribusi untuk menjamin keefektifan tata kelola perusahaan atas informasi teknologi serta mengoptimalkan tingkat risiko dan pemanfaatan sumber daya [7]. Penelitian ini menggunakan COBIT 2019 karena dianggap sebagai versi terbaru yang sudah disempurnakan dan bisa diterima secara luas dengan mencangkup berbagai aspek tata kelola serta manajemen yang dibutuhkan sebuah organisasi yang didalamnya terdapat analisis manajemen risiko. Pada penelitian ini, penulis akan melakukan analisis performa menggunakan 11 faktor desain COBIT 2019 untuk melihat keadaan perusahaan secara menyeluruh, kemudian akan berfokus pada domain yang mengandung unsur manajemen risiko yaitu domain EDM03, APO12, APO13, dan DSS05 dengan melihat nilai tingkat kapabilitas yang diharapkan. Hal tersebut dikarenakan PT. XYZ belum pernah dilakukan penelitian mengenai analisis manajemen risiko TI.

Tujuan penelitian untuk membantu PT. XYZ dalam mengetahui tingkat kapabilitas perusahaan saat ini menggunakan COBIT 2019 dengan pertimbangan fokus ke beberapa domain yang termasuk dalam manajemen risiko TI yaitu domain EDM03, APO12, APO13, dan DSS05. Hasil penelitian berupa faktor desain perusahaan, tingkat kapabilitas perusahaan dan rekomendasi perbaikan terkait manajemen risiko TI pada PT. XYZ.

 ISSN:2302-8149
e-ISSN:2540-9719

## 2 Tinjauan Literatur

Penulis menggunakan beberapa jurnal penelitian sebagai tinjauan literatur penelitian ini. Penelitian pertama [8] penulis menggunakan metode pengumpulan data kombinasi (*mixed method*) pada Perguruan Tinggi XYZ untuk dilakukan pengukuran tes tingkat kapabilitas pada COBIT 2019. Peneliti berfokus pada domain APO12. Hasil penelitian berupa perhitungan nilai rata-rata sub domain APO12.01-APO12.06 sebesar 28%. Jika mengacu pada teori tes tingkat kapabilitas maka termasuk ke dalam kategori level 2 (*Managed*). Kemudian dilakukan analisis GAP pada setiap sub domain menunjukan nilai indeks yang didapat ada pada rentang 2-3, dengan indeks yang diharapkan yaitu 4. Mengartikan setiap subdomain terdapat rentang GAP 1-2, sehingga belum ada domain yang mampu mencapai target. Karena hal tersebut, perlu diberikan beberapa rekomendasi dengan harapan dapat dimanfaatkan untuk meningkatkan proses pemeliharaan, perencanaan, pengendalian hingga pemonitoran Perguruan Tinggi XYZ.

Penelitian kedua [9] penulis menggunakan metode pengumpulan data secara kuantitatif dengan penentuan respondennya menggunakan RACI *Chart* untuk *Department of ICT* PT Semen Indonesia (Persero) TBK dengan tujuan untuk menentukan nilai kapabilitas beserta kesenjangan nilainya. Peneliti berfokus dengan domain EDM03 dan APO12 dari COBIT 2019. Hasil penelitian tingkat kapabilitas domain EDM03 ada di level 3 dan domain APO12 ada di level 2. Hal tersebut dikarenakan pada masing-masing domain belum secara penuh mencapai *Fully Achieved*, melainkan baru mencapai *Largely Achieved* sebesar 50%-85%. Kemudian berdasarkan hasil penilaian tingkat kapabilitas nilai GAP domain EDM03 adalah 1 disebabkan saat ini domain berada di level 3 dengan level yang ingin dicapai perusahaan ada pada level 4, dimana seluruh proses yang berjalan dapat terdefinisi dengan baik dan kinerja terukur secara kuantitatif. Nilai GAP domain APO12 adalah 1, dikarenakan saat ini domain berada di level 2 dengan level yang ingin dicapai perusahaan yaitu level 3, dimana seluruh proses sudah diorganisir dengan baik menggunakan aset perusahaan. Karena hal tersebut, perusahaan perlu diberikan beberapa rekomendasi yang dapat digunakan untuk mengelola dan menerapkan manajemen risiko TI dengan lebih baik.

Penelitian ketiga [10] penulis menggunakan metode pengumpulan data primer secara kuantitatif dengan penentuan respondennya menggunakan RACI *Chart* pada PT.XYZ. Penelitian dilakukan untuk menentukan tingkat kapabilitas perusahaan saat ini dengan penilaian yang dilakukan secara bertahap dan akan berhenti jika aktivitas penerapan mencapai <85% pada domain EDM03 dan APO12 dari COBIT 2019. Hasil penelitian pada domain EDM03 dan APO12 masing-masing menunjukan penerapan aktivitas kapabilitas level 2 dengan persentase sebesar 44,44% untuk domain EDM03 dan 33,33% untuk domain APO12. Hal tersebut mengartikan tingkat kemampuan perusahaan berada di 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. Kemudian berdasarkan hasil penilaian tingkat kapabilitas nilai GAP pada domain EDM03 dan APO12 masing-masing adalah 1. Hal ini disebabkan karena kedua domain belum mencapai penilaian tingkat kapabilitas level 2, hingga saat ini kedua domain berada di level 1. Karena hal tersebut, perusahaan memerlukan beberapa rekomendasi untuk dapat digunakan dalam mengelola dan menerapkan manajemen risiko TI dengan lebih baik.

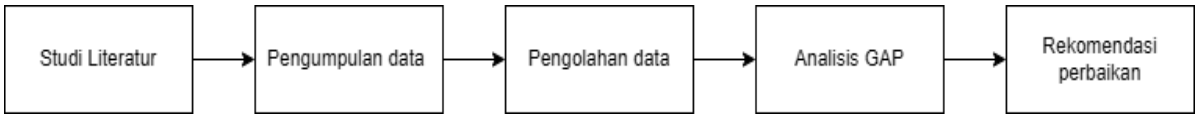
Berdasarkan penelitian sebelumnya yang digunakan penulis sebagai bahan tinjauan literatur, disimpulkan bahwa ketiga penelitian mengenai manajemen risiko tersebut menggunakan *Framework* COBIT 2019 untuk mencari nilai tingkat kapabilitas. Penelitian pertama berfokus hanya pada satu domain yaitu APO12, penelitian kedua dan ketiga memiliki fokus yang sama yaitu pada domain EDM03 dan APO12. Dari hasil analisis tersebut, didapatkan dua hal yang membedakan penelitian ini dengan penelitian-penelitian sebelumnya yaitu untuk pengukuran tingkat kapabilitas akan difokuskan hanya pada domain yang mengandung unsur manajemen risiko TI yaitu EDM03 (*Ensured Risk Optimization*) dan APO12 (*Managed Risk*), dengan melakukan tambahan domain APO13 (*Managed Security*) dan DSS05 (*Managed Security Services*) untuk menilai keamanan TI. Penambahan domain manajemen risiko yang diteliti berangkat dari saran yang diberikan pada penelitian ketiga, yang mengatakan bahwa dalam melakukan penelitian manajemen risiko pada sebuah perusahaan dapat ditambahkan meneliti domain APO13 dan DSS05 [10] untuk meningkatkan pengukuran manajemen risiko pada bidang TI. Selain meneliti pengukuran tingkat kapabilitas pada domain-domain tersebut, penulis juga melakukan analisis performa perusahaan terlebih dahulu menggunakan 11 faktor desain.

 ISSN:2302-8149
e-ISSN:2540-9719

Pertimbangan penulis adalah untuk melihat performa dari tiap-tiap domain di perusahaan yang sudah berjalan sekaligus membuat penulis mengetahui nilai tingkat kapabilitas yang diharapkan pada domain EDM03, APO12, APO13, dan DSS05. Pertimbangan faktor analisis performa tersebut belum pernah diimplementasikan pada penelitian-penelitian sebelumnya.

## 3 Metode Penelitian

Metode penelitian yang digunakan yaitu *Design Science Research* (DSR) yang merupakan pendekatan penelitian terkait perancangan realitas baru. Dengan metodologi pengumpulan data menggunakan pendekatan kualitatif untuk memperoleh gambaran yang lengkap dari sebuah fenomena yang terjadi dan diamati berdasarkan sudut pandang subjek tanpa harus membuktikan apapun [11]. Sumber data utama yang digunakan dalam metode ini berdasarkan hasil wawancara dan kuisioner. Tahap penelitian yang dilakukan ditunjukan dengan Gambar 1 sebagai berikut:




**Gambar 1. Tahap penelitian**

### 3.1 Studi Literatur

Studi literatur dilaksanakan untuk memperoleh teori yang mendukung penelitian serta referensi penelitian terdahulu dari jurnal penelitian maupun *ebook* yang berkaitan dengan penelitian ini. Tujuannya untuk memperoleh informasi yang mendukung latar belakang penelitian, serta rekomendasi dan saran dari penelitian sebelumnya.

### 3.2 Pengumpulan Data

Pengumpulan data dilakukan untuk memenuhi proses analisis performa dan pengukuran tingkat kapabilitas perusahaan. Proses analisis performa PT. XYZ dilakukan menggunakan 11 faktor desain COBIT 2019 dengan wawancara terstruktur ke beberapa narasumber baik di dalam maupun di luar bidang TI. Hal tersebut dipertimbangan penulis agar mendapatkan hasil data wawancara yang lebih luas dari berbagai sudut pandang. Pertanyaan yang diberikan berasal dari *toolkit* 11 faktor desain COBIT 2019. Hasil dari 11 faktor desain berupa nilai dari setiap domain COBIT 2019 yang akan menunjukan kualitas performa perusahaan yang sedang berjalan dan tingkat kapabilitas yang diharapkan perusahaan, terutama pada domain EDM03, APO12, APO13, dan DSS05. Penjelasan dari 11 faktor desain pada COBIT 2019 [12] [13] sebagai berikut :

a. Faktor desain 1 (*Enterprise Strategy*) terdiri dari beberapa jenis strategi untuk perusahaan menyesuaikan dengan bidang bisnisnya, yaitu strategi untuk fokus pada pertumbuhan perusahaan (*Growth*), produk dan layanan yang inovatif (*Innovation*), meminimalisir biaya pengeluaran jangka pendek (Cost Leadership), serta menyediakan pelayanan yang berorientasi pada klien (*Client Service*).
b. Faktor desain 2 (*Enterprise Goals*) terdiri dari 13 tujuan umum perusahaan yang mendukung *enterprise strategy* untuk perusahaan dapat memprioritaskan sasaran perusahaan sesuai dengan strategi perusahaan yang pilih.
c. Faktor desain 3 (*IT Risk Profile*) terdiri dari profil risiko perusahaan dengan 19 kategori skenario risiko untuk mengidentifikasi skenario apa saja yang dapat mempengaruhi perusahaan, menilai dampaknya, dan kemungkinan terjadinya risiko.
d. Faktor desain 4 (*I&T Related Issues*) terdiri dari 20 daftar masalah umum terkait TI yang dapat diidentifikasikan untuk menjadi input perusahaan dalam menentukan prioritas desain tata kelola.
e. Faktor desain 5 (*Threat Landscape*) terdiri dari 2 kategori ancaman yaitu ancaman normal dan tinggi yang biasa dihadapi dalam sebuah perusahaan

 ISSN:2302-8149
e-ISSN:2540-9719

f. Faktor desain 6 (*Compliance Requirement*) terdiri dari 3 jenis kategori tuntutan atau kebutuhan yaitu rendah, normal, dan tinggi yang harus dipenuhi oleh perusahaan
g. Faktor desain 7 (*Role of IT*) terdiri dari posisi TI pada sebuah perusahaan yang dinilai menggunakan kategori *strategic*, *support*, atau *factory*
h. Faktor desain 8 (*Sourcing Model of IT*) terdiri dari pengelolaan sumber daya TI yang diimplementasikan perusahaan berdasarkan beberapa model yaitu *outsourcing*, *cloud*, *insourced*, maupun *hybrid*.
i. Faktor desain 9 (*IT Implementation Methods*) terdiri dari beberapa metode yang digunakan perusahaan dalam mengimplementasikan TI seperti *Agile*, *DevOps*, dan *Traditional*
j. Faktor desain 10 (*Technology Adoption Strategy*) terdiri dari kategori strategi yang diimplementasikan oleh perusahaan untuk mengadopsi teknologi baru seperti *first mover*, *follower*, dan *slow adopter*.
k. Faktor desain 11 (*Enterprise Size*) terdiri dari ukuran dari perusahaan dari segi jumlah karyawan tetap yang dipekerjakan.

Proses pengukuran tingkat kapabilitas merupakan langkah selanjutnya yang lebih mengerucut dari analisis performa untuk mengetahui kualitas dan kemampuan dari manajemen risiko TI pada PT. XYZ. Pengumpulan data untuk pengukuran tingkat kapabilitas domain DM03, APO12, APO13, dan DSS05 dilakukan melalui wawancara dan kuesioner. Kuesioner dibuat bersumber dari aktivitas pada masing-masing domain yang diukur berdasarkan pada tingkat aktivitas yang ada pada COBIT 2019. Pengukuran tingkat kapabilitas tersebut menggunakan model *Capability and Maturity Model Integration* yang terdiri dari level 0 sampai 5, berikut adalah penjelasan dari setiap levelnya [8]:

a. Level 0 merupakan tingkatan yang prosesnya tidak memiliki dasar kemampuan sama sekali, tidak lengkap dalam mencerminkan pendekatan yang terpadu untuk mencapai tujuan dari tata kelola serta manajemen, dan tidak mencapai dari proses praktek apapun.
b. Level 1 merupakan tingkatan yang prosesnya kurang lebih mencapai tujuan dengan melewati implementasi sekumpulan aktivitas yang tidak lengkap dan tidak terlalu terorganisir.
c. Level 2 merupakan tingkatan yang prosesnya sudah mencapai tujuan dengan melewati implementasi sekumpulan aktivitas dasar yang lengkap dan terorganisir
d. Level 3 merupakan tingkatan yang prosesnya sudah mencapai tujuan dengan menggunakan cara organisasi yang lebih terorganisir, dimana proses yang ada terdefinisikan dengan baik.
e. Level 4 merupakan tingkatan yang prosesnya sudah mencapai tujuan, terdefinisikan dengan baik, dan dilakukan pengukuran kuantitatif terhadap kinerjanya.
f. Level 5 merupakan tingkatan yang prosesnya sudah mencapai tujuan, terdefinisi dengan baik, dilakukan pengukuran kuantitatif terhadap kinerjanya untuk meningkatkan performa, dan dilakukan usaha perbaikan yang berkelanjutan.

### 3.3 Pengolahan Data

Data-data yang berhasil didapatkan dari wawancara dan kuesioner diolah menggunakan *framework* COBIT 2019. Data tersebut akan diolah menggunakan *toolkit* 11 faktor desain untuk mengetahui bagaimana keadaan sesungguhnya dari performa perusahaan yang sedang berjalan serta mengetahui tingkat kapabilitas domain yang diharapkan terhadap domain EDM03, APO12, APO13, dan DSS05.

Setelah diketahui tingkat kapabilitas yang diharapkan pada domain dengan manajemen risiko TI yaitu EDM03, APO12, APO13, dan DSS05, melalui tahapan selanjutnya yaitu pengukuran tingkat kapabilitas menggunakan model *Capability and*

 ISSN:2302-8149
e-ISSN:2540-9719

*Maturity Model Integration*. Data yang diperoleh akan diolah untuk menghitung nilai kapabilitas risiko saat ini pada PT. XYZ menggunakan rumus (1):

$$Tingkat\ Kapabilitas = \frac{\sum aktivitas\ yang\ sudah\ dilakukan}{Total\ aktivitas} \text{X100\%} \quad (1)$$

Pengukuran tingkat kapabilitas memiliki standar penilaian sebagai berikut [14]:

1. *Not Achieved (N)*
   Tidak ada pencapaian maupun bukti pencapaian proses tersebut dengan tingkat kapabilitas mencapai 0% - 15%
2. *Partial Achieved (P)*
   Diperoleh sejumlah pencapaian maupun bukti pencapaian proses yang tersedia, namun terdapat aspek-aspek yang tidak bisa diperkirakan dengan tingkat kapabilitas mencapai 15% - 50%
3. *Largely Achieved (L)*
   Diperoleh pencapaian maupun bukti pencapaian, namun terdapat kekurangan pada proses yang dinilai dengan tingkat kapabilitas mencapai 50% - 85%
4. *Fully Achieved (F)*
   Diperoleh pencapaian maupun bukti pencapaian secara lengkap dan tidak memiliki kekurangan untuk proses yang dinilai dengan tingkat kapabilitas mencapai 85% - 100%

### 3.4 Analisis GAP

Tahapan selanjutnya dari pengukuran tingkat kapabilitas penerapan tata kelola TI yaitu untuk menunjukkan pencapaian kinerja TI pada PT. XYZ dengan proses perhitungan GAP atau nilai kesenjangan. Pada analisis GAP dilakukan perbandingan antara nilai tingkat kapabilitas dengan nilai yang diharapkan. Selisih yang didapatkan nantinya akan menjadi nilai atau hasil dari sebuah kesenjangan atau GAP. Nila GAP didapatkan dari rumus (2):

$$GAP = Expected\ Capability\ (EC) - Current\ Cpability\ (CC) \quad (2)$$

EC adalah tingkat kapabilitas yang diharapkan perusahaan dan CC adalah tingkat kapabilitas yang berlangsung sekarang dengan didasakan pada pengukuran tingkat kapabilitas perusahaan. Hasil dari pengukuran analisis GAP akan menjadi tolak ukur rekomendasi yang akan diberikan untuk PT. XYZ sebagai perbaikan pada perusahaannya.

### 3.5 Rekomendasi Perbaikan

Rekomendasi perbaikan berisi kumpulan rekomendasi yang diberikan atau diusulkan penulis untuk memperbaiki tata kelola TI sekaligus sebagai bentuk manajemen risiko PT. XYZ dengan tujuan perusahaan dapat memperoleh tingkat kapabilitas yang diharapkan ke depannya. Rekomendasi yang disampaikan berdasarkan dari pengukuran analisis performa dan tingkat kapabilitas yang terjadi saat penelitian dilakukan.

## 4 Hasil dan Pembahasan

Hasil dan pembahasan merupakan kumpulan dari hasil analisis data yang menunjukkan nilai dari faktor desain dan pengukuran tingkat kapabilitas pada PT. XYZ menggunakan *framework* COBIT 2019 ditunjukan sebagai berikut:

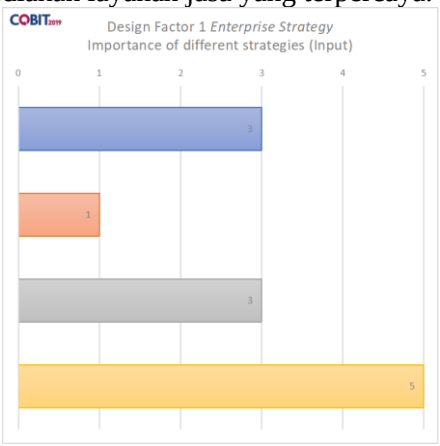
 ISSN:2302-8149
e-ISSN:2540-9719

### 4.1 Analisis Performa

Analisis performa PT. XYZ dilakukan dengan faktor desain menggunakan 11 desain *toolkit* COBIT 2018 [15], berikut adalah hasil yang diperoleh:

1. Faktor desain 1: *Enterprise Strategy*

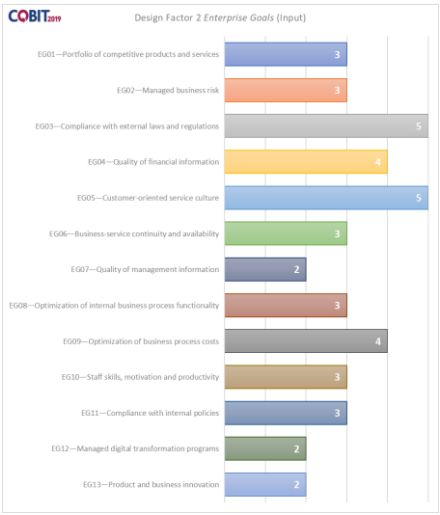
Pada Gambar 2 menampilkan strategi perusahaan ada pada *Client Service/ Stability* dengan nilai tingkat kepentingan 5. Hal tersebut sesuai dengan PT. XYZ yang bergerak pada bidang transportasi dan pariwisata sehingga fokus utama adalah menyediakan layanan jasa yang terpercaya.




**Gambar 2. *Enterprise strategy***

2. Faktor desain 2 : *Enterprise Goals*

Pada Gambar 3 menampilkan tujuan atau fokus perusahaan ada pada EG05 *Customer-oriented service culter* dengan nilai tingkat kepentingan 5, di mana PT. XYZ sangat mementingkan kepuasan pelanggan sebagai sumber pendapat utama perusahaan.

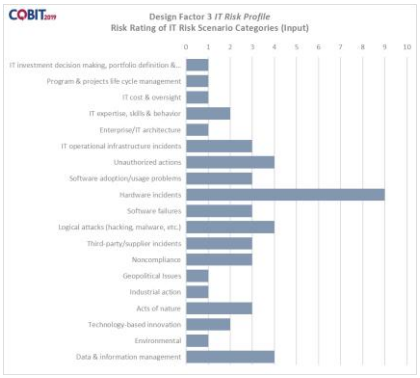



**Gambar 3. *Enterprise strategy***

3. Faktor desain 3 : *IT Risk Profile*

Pada Gambar 4 menampilkan bentuk risiko TI paling tinggi yang dimiliki PT. XYZ bernilai 9 pada *Hardware incidents* dengan *likehood* 4 dan *impact* 3, karena disebabkan perangkat keras pada perusahaan yang tidak diperbaharui secara berkala. Menyebabkan proses oprasional terkendala karena *loading* perangkat terlalu lama maupun perangkat yang tiba-tiba *restart* atau mati sendiri.

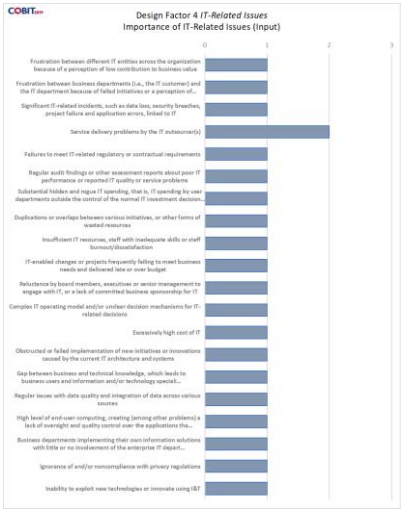
 ISSN:2302-8149
e-ISSN:2540-9719




**Gambar 4. *IT risk profile***

4. Faktor desain 4 : *I&T Related Issues*

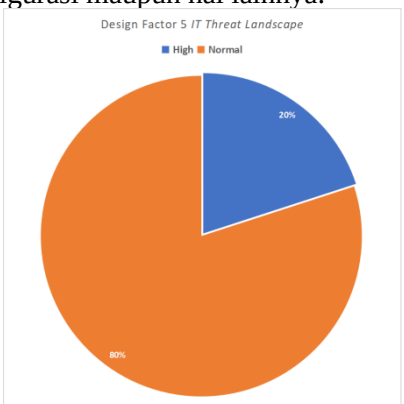
Pada Gambar 5 *IT-related issues* sering terjadi di perusahaan adalah masalah penyediaan layanan TI oleh penyedia jasa TI dengan nilai 5, secara spesifik dari segi penyediaan perangkat keras yang memadai dan terawat untuk mendukung oprasional perusahaan.




**Gambar 5. *I&T related issues***

5. Faktor desain 5 : *Threat Landscape*

Pada Gambar 6 tingkat ancaman pada PT. XYZ masih tergolong normal yaitu 80% mengartikan perusahaan masih mampu mengatasi dan mengelola ancaman yang terjadi. Risiko tersebut dapat berupa terjadinya gangguan koneksi internet hingga *hardware* yang tidak berfungsi seperti seharusnya dikarenakan ada kesalahan konfigurasi maupun hal lainnya.

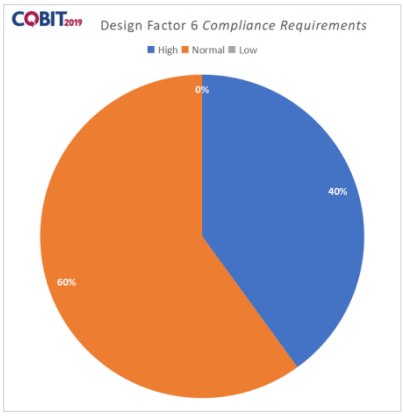



**Gambar 6. *Threat landscape***

6. Faktor desain 6 : *Compliance Requirements*

 ISSN:2302-8149
e-ISSN:2540-9719

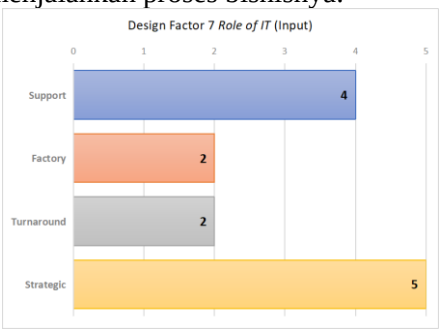
Pada Gambar 7 persentase PT. XYZ untuk nilai nominal adalah 60% karena sudah melengkapi peraturan beserta persyaratan di industrinya seperti peraturan perusahaan, akte pendirian bangunan, NPWP, dan IMB (Izin Mendirikan Bangunan). Persentase nilai *high* adalah 40%, dikarenakan PT. XYZ sudah melengkapi persyaratan penting atau risiko tinggi yaitu KIR (Uji Kendaraan Bermotor), STNK, SIUP (Surat Izin Usaha Perdagangan), dan KPS (Kartu Pengawasan).




**Gambar 7. *Compliance requirement***

7. Faktor desain 7 : *Role of IT*

Pada Gambar 8 untuk *support* bernilai 4 karena PT. XYZ sudah menerapkan TI dalam mendukung strategi bisnisnya yaitu untuk mengatur *booking* pesanan dan keuangannya. *Factory* bernilai 2 dikarenakan jika TI perusahaan terdapat kegagalan tidak akan secara langsung memberi dampak besar hingga mempengaruhi proses bisnis PT. XYZ. *Turnaround* bernilai 2 dikarenakan peran TI di PT. XYZ membantu dalam inovasi bisnis perusahaan. *Strategic* bernilai 5 dikarenakan pengimplementasian TI berdampak besar yaitu mempermudah PT. XYZ dalam menjalankan proses bisnisnya.

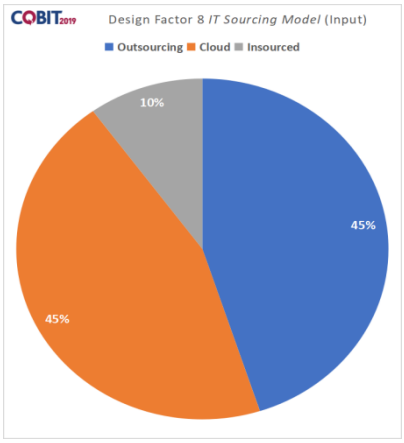



**Gambar 8. *Compliance requirement***

8. Faktor desain 8 : *IT Sourcing Model*

Pada Gambar 9 sebagian besar SI/TI PT. XYZ menggunakan layanan dari pihak ketiga, sehingga *outsourcing* bernilai 65%. Sedangkan pada *cloud* bernilai 25% disebabkan perusahaan memanfaatkan layanan Google Drive untuk layanan penyimpanan berkas dan Google Mail untuk surat menyurat. *Insourced* bernilai 10% karena PT. XYZ memiliki tenaga IT tetapi masih digunakan sebagai *support.*

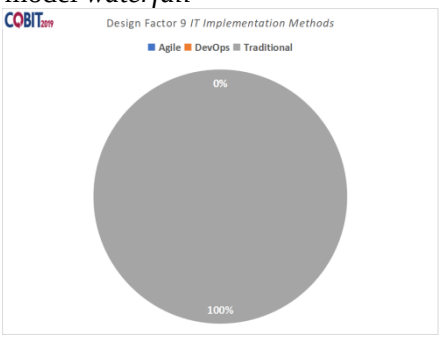
 ISSN:2302-8149
e-ISSN:2540-9719




**Gambar 9. *IT sourcing model***

9. Faktor desain 9: *IT Implementation Methods*

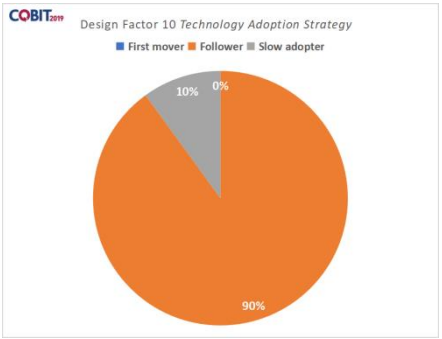
Pada Gambar 10 pengembangan SI/TI pada PT. XYZ masih sepenuhnya menggunakan model *waterfall*




**Gambar 10. *IT implementation methods***

10. Faktor desain 10: *Technology Adoption Strategy*

Pada Gambar 11 menghasilkan data bahwa perusahaan 80% masih sebagai *follower* dan *slow adopter* bernilai 20% untuk mengimplementasikan TI. Sehingga menjelaskan jika PT. XYZ tidak tergesa-gesa dalam mengaplikasikan teknologi baru.



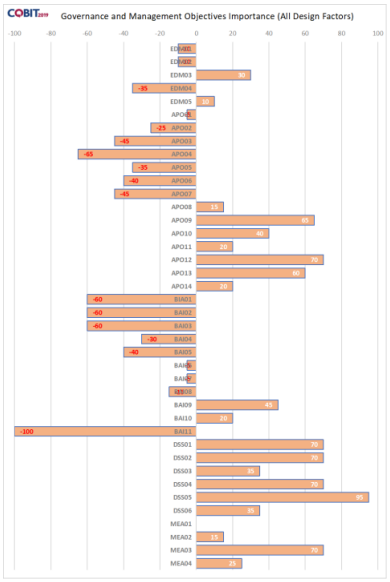

**Gambar 11. *Technology adoption strategy***

11. Faktor desain 11: *Enterprise Size*

Besar kecilnya perusahaan dapat dilihat dari jumlah karyawan tetap yang bekerja untuk sebuah perusahaan. PT. XYZ memiliki beberapa cabang perusahaan yang tersebar di Jawa Tengah, dengan perusahaan yang menjadi objek penelitian memiliki jumlah karyawan tetap sebanyak 80-90 orang. Sehingga PT. XYZ termasuk ke dalam kategori perusahaan kecil menengah.

Berdasarkan dari faktor desain yang telah dilaksanakan dengan *toolkit* desain COBIT 2019 diperoleh hasil sebagai berikut:

 ISSN:2302-8149
e-ISSN:2540-9719




**Gambar 12. Hasil faktor desain**

Pada Gambar 11 menunjukan seluruh informasi yang telah dikumpulkan dan disatukan dalam *all design factor* COBIT 2019 yang mengandung 40 proses, di mana setiap prosesnya memiliki nilai yang berbeda-beda. Area kanan bernilai positif, menunjukkan proses-proses yang penting untuk PT. XYZ. Area kiri bernilai negatif, menunjukkan proses-proses yang belum atau bukan prioritas untuk PT. XYZ. Berikut adalah hasil nilai dan level dari domain EDM03, APO12, APO13, dan DSS05 yang telah dilakukan:

1. Domain EDM03 bernilai 30 (berada pada rentang nilai 25%-50%) mengartikan tingkat kapabilitas yang diharapkan domain tersebut ada di level 2
2. Domain APO12 bernilai 70 (berada pada rentang nilai 50%-85%) mengartikan tingkat kapabilitas yang diharapkan domain tersebut ada di level 3
3. Domain APO13 bernilai 60 (berada pada rentang nilai 50%-85%) mengartikan tingkat kapabilitas yang diharapkan domain tersebut ada di level 3
4. Domain DSS05 bernilai 95 (berada pada rentang nilai 85%-100%) mengartikan tingkat kapabilitas yang diharapkan domain tersebut ada di level 4
5. Tingkat Kapabilitas

Pengukuran tingkat kapabilitas manajemen risiko TI PT. XYZ dilaksanakan hanya terhadap domain EDM03, APO12, APO13, dan DSS05 [6]. Berikut hasil dari pengukuran tingkat kapabilitas :

**Tabel 1. Pengukuran tingkat kapabilitas EDM03**

| No. | Domain | Jumlah Aktifitas | Aktivitas yang dijalankan | | Nilai Kapabilitas |
|---|---|---|---|---|---|
| | | | Ya | Tidak | |
| 1 | EDM03.01 | 4 | 2 | 2 | **78% (L)** |
| 2 | EDM03.02 | 4 | 4 | 0 | |
| 3 | EDM03.03 | 1 | 1 | 0 | |
| **Total** | | **9** | **7** | **2** | |

Tabel 1 merupakan perhitungan dari domain EDM03 (*Ensured Risk Optimization*). EDM03 bertujuan untuk menjamin jika risiko perusahaan terkair TI tidak melebihi batas toleransi risiko yang dimiliki perusahaan. Dari Tabel 1 diperoleh perhitungan bahwa PT. XYZ

 ISSN:2302-8149
e-ISSN:2540-9719

menjalankan aktivitas tidak lebih dari 7/9 aktivitas. Termasuk ke dalam tingkat kapabilitas level 2 dengan perolehan nilai kapabilitas sebesar 78% dan skala pemeringkatannya *large (L)*. Hal ini menunjukkan bahwa domain EDM03 belum mencapai tingkat kapabilitas level 2. Sehingga ditarik kesimpulan EDM03 masih berada di level 1.

**Tabel 2. Pengukuran tingkat kapabilitas APO12**

| No. | Domain | Jumlah Aktifitas | Aktivitas yang dijalankan | | Nilai Kapabilitas |
|---|---|---|---|---|---|
| | | | Ya | Tidak | |
| 1 | APO12.01 | 2 | 0 | 2 | **33%** |
| 2 | APO12.03 | 3 | 2 | 1 | **(P)** |
| 3 | APO12.05 | 1 | 0 | 1 | |
| **Total** | | **6** | **2** | **4** | |

Tabel 2 merupakan perhitungan dari domain APO12 (*Managed Risk*). Tujuan dari APO12 yaitu menggabungkan manajemen risiko perusahaan TI dengan manajemen risiko perusahaan secara keseluruhan. Dari Tabel 2 diperoleh perhitungan APO12 pada PT. XYZ menjalankan aktivitas tidak lebih dari 2/6 aktivitas. Termasuk ke dalam tingkat kapabilitas level 2 dengan perolehan nilai kapabilitas sebesar 33% dan skala pemeringkatan *Partial (P)*. Hal tersebut menunjukkan bahwa domain APO12 belum mencapai tingkat kapabilitas level 2. Sehingga ditarik kesimpulan APO12 masih berada di level 1.

**Tabel 3. Pengukuran tingkat kapabilitas APO13**

| No. | Domain | Jumlah Aktifitas | Aktivitas yang dijalankan | | Nilai Kapabilitas |
|---|---|---|---|---|---|
| | | | Ya | Tidak | |
| 1 | APO13.01 | 7 | 3 | 4 | **43%** |
| **Total** | | **7** | **3** | **4** | **(P)** |

Tabel 3 merupakan perhitungan dari domain APO13 (*Managed Security*). Tujuan dari APO13 adalah unutk menjaga terjadinya serta dampak dari insiden keamanan TI dalam tingkat risiko perusahaan. Dari Tabel 3 diperoleh perhitungan APO13 pada PT. XYZ menjalankan aktivitas tidak lebih dari 3/7 aktivitas. Termasuk ke dalam tingkat kapabilitas level 2 dengan perolehan nilai kapabilitas sebesar 43% dan skala pemeringkatan *Partial (P)*. Hal tersebut menunjukkan bahwa domain APO13 belum mencapai tingkat kapabilitas level 2. Sehingga ditarik kesimpulan APO13 masih berada di level 1.

**Tabel 4. Pengukuran tingkat kapabilitas DSS05**

| No. | Domain | Jumlah Aktifitas | Aktivitas yang dijalankan | | Nilai Kapabilitas |
|---|---|---|---|---|---|
| | | | Ya | Tidak | |
| 1 | DSS05.01 | 2 | 2 | 0 | **58%** |
| 2 | DSS05.02 | 4 | 3 | 1 | **(L)** |
| 3 | DSS05.03 | 9 | 7 | 2 | |
| 4 | DSS05.04 | 1 | 1 | 0 | |
| 5 | DSS05.05 | 4 | 2 | 2 | |
| 6 | DSS05.06 | 2 | 0 | 2 | |
| 7 | DSS05.07 | 4 | 0 | 4 | |
| **Total** | | **26** | **15** | **11** | |

Tabel 4 merupakan perhitungan dari domain DSS05 (*Managed Security Services*). Tujuan dari DSS05 adalah untuk meminimalisir dampak dari kerentanan dan insiden keamanan oprasional TI. Dari Tabel 4 diperoleh perhitungan DSS05 pada PT. XYZ menjalankan aktivitas tidak lebih dari 15/26 aktivitas. Termasuk ke dalam tingkat kapabilitas

 ISSN:2302-8149
e-ISSN:2540-9719

level 2. Hal tersebut menunjukkan bahwa domain DSS05 belum mencapai pada tingkat kapabilitas level 2. Sehingga ditarik kesimpulan DSS05 masih berada di level 1.

### 4.2 Analisis GAP

Berangkat dari hasil pengukuran tingkat kapabilitas yang telah dilakukan, dihasilkan GAP dari tingkat kapabilitas domain manajemen risiko sebagai berikut:

**Tabel 5. Analisis GAP**

| Domain | *Expected Capability (EC)* | *Current Capability (CC)* | GAP |
|---|---|---|---|
| EDM03 | 2 | 1 | 1 |
| APO12 | 3 | 1 | 2 |
| APO13 | 3 | 1 | 2 |
| DSS05 | 4 | 1 | 3 |

Tabel 5 dapat dilihat bahwa domain EDM03 mempunyai nilai GAP sebesar 1, domain APO12 dan APO13 memiliki nilai GAP sebesar 2, serta domain DSS05 memiliki nilai GAP sebesar 3. Hal ini menunjukkan bahwa PT. XYZ masih memerlukan cukup banyak perbaikan dalam pengelolaan manajemen risiko TI untuk dapat mencapai target dari tingkat kapabilitas yang diharapkan.

### 4.3 Rekomendasi

Berdasarkan hasil dari analisis GAP domain EDM03, APO12, APO13, dan DSS05 menunjukkan bahwa diperlukan beberapa rekomendasi yang diharapkan dapat membentuk perbaikan manajemen risiko PT. XYZ. Rekomendasi yang diberikan berdasarkan nilai tingkat kapabilitas yang sedang terjadi dengan mengacu pada kerangka kerja COBIT 2019.

Rekomendasi domain EDM03 dengan perusahaan perlu untuk menentukan tingkat risiko TI yang ada dan melakukan sosialisasi kepada para *stakeholder*, tujuannya agar masing-masing *stakeholder* bisa lebih memahami mengenai risiko TI yang dapat terjadi beserta alur penangannya. Selain itu, perusahaan juga perlu melakukan evaluasi dari aktivitas menajamen risiko yang terjadi untuk mengetahui kapasitas perusahaan. Harapannya dengan hal tersebut dapat membantu perusahaan dalam mengidentifikasi risiko lebih baik dan detail.

Rekomendasi domain APO12 dengan perusahaan perlu untuk melakukan pencatatan kejadian risiko TI secara signifikan agar perusahaan bisa melakukan survei, analisis risiko, hingga menerapkan analisis kejadian serta faktor risikonya secara teratur dengan tujuan agar dapat mengidentifikasikan masalah risiko yang baru dari catatan kejadian tersebut.

Rekomendasi domain APO13 dengan perusahaan perlu untuk membangun *Information Security Management System* (ISMS), dengan tujuan memelihara informasi dari segala wujud ancaman dari risiko yang dapat terjadi. ISMS merupakan sistem manajemen yang sudah mencakup prosedur, kebijakan, praktik, dan teknologi yang diperlukan dalam mengendalikan keamanan informasi perusahaan.

Rekomendasi domain DSS05 dengan perusahaan perlu untuk mengimplementasikan makanisme penyaringan jaringan seperti *firewall* serta pendeteksi penyusupan pada *software* yang digunakan. Selain itu, perusahaan juga harus secara berkala mengevaluasi dan meninjau informasi mengenai kemungkinan ancaman baru seperti meninjau sarana keamanan produk dan layanan vendor atau pilihan ketiga.

 ISSN:2302-8149
e-ISSN:2540-9719

## 5 Kesimpulan

Kesimpulan dari hasil penelitian ini mengenai analisis manajemen risiko pada PT. XYZ berdasarkan performa perusahaan menggunakan *framework* COBIT 2019 yang diawali dengan melakukan faktor desain untuk melihat performa perusahaan. Hasil faktor desain yang diambil hanya berfokus pada domain yang mengandung unsur manajemen risiko yaitu EDM03, APO12, APO13, dan DSS05. Hasil tersebut menunjukkan bahwa domain EDM03, APO12, APO13, dan DSS05 memiliki target tingkat kapabilitas yang berbeda-beda yaitu pada level 2, level 3, level 3, dan level 4. Berdasarkan hasil tersebut didapatkan nilai GAP yaitu domain EDM03 bernilai GAP 1, APO12 bernilai GAP 2, APO13 bernilai GAP 2, dan DSS05 bernilai GAP 3. Dengan adanya kesenjangan nilai diantara tingkat kapabilitas yang diharapkan dengan tingkat kapabilitas yang terjadi sekarang di perusahaan maka perlu adanya rekomendasi manajemen risiko TI. Beberapa rekomendasi yang dapat diberikan seperti perbaikan seperti menentukan tingkat risiko TI dan mensosialisasikannya kepada para *stakeholder*, mencatat kejadian risiko TI, membangun *Information Security Management System* (ISMS), menerapkan mekanisme penyaringan jaringan, dan secara teratur melakukan evaluasi informasi mengenai potensi ancaman baru dengan meninjau keamanan produk serta layanan vendor atau pihak ketiga.

## Referensi

[1] World Health Orgaization, "Statement on the fifteenth meeting of the IHR (2005) Emergency Committee on the COVID-19 pandemic," *5 May 2023. Available: https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-%282005%29-emergency-committee-regarding-the-coronavirus-disease-%28covid-19%29-pandemic*

[2] I. Ravikumar Ramachandran, *CISA, CISM, CGEIT, CRISC, CDPSE, OCA-Multi Cloud Architect, CISSP-ISSAP, SSCP, CAP, PMP, CIA, CRMA, CFE, FCMA, CIMA-Dip.MA, CFA, CEH, ECSA, CHFI, MS (Fin), MBA (IT), COBIT-5 Implementer, Certified COBIT Assessor, ITIL 4 -Managing P, "Can IT Governance Be Dispensed With?," 20 October, 2021. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-34/can-it-governance-be-dispensed-with#:~:text=The title of this article,of the IT governance process*

[3] A. Ahmed, B. Kayis, dan S. Amornsawadwatana, *"A review of techniques for risk management in projects," Benchmarking, vol. 14, no. 1, hal. 22–36, 2007, doi: 10.1108/14635770710730919.*

[4] *M. Hasan,et al.*, Metode Penelitian Kualitatif, *1st ed., Tahta Media Group. 2023.*

[5] S. A. Chandra, R. Fauzi, dan I. Santosa, "Analisis dan Perancangan Proses Manajemen Kepatuhan Ti Menggunakan Kerangka Kerja Cobit 2019 Di PT Inti (persero)," *eProceedings Eng.*, vol. 7, no. 2, hal. 9635–9642, 2020.

[6] S. D. Haes,et al., "Information System Audit and Control Association"., *COBIT 2019 Framework Governance and Management Objectives.*

[7] D. F. Tanjung, A. Oktaviana, dan A. P. Widodo, "Analisis Manajemen Risiko Startup pada Masa Pandemi COVID-19 Menggunakan COBIT® 2019," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 3, hal. 635, 2021, doi: 10.25126/jtiik.2021834914.

[8] R. Anugrah, E. Utami, dan A. H. Muhammad, "Analisis Manajemen Risiko TI pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO12," *J. Ilm. Univ. Batanghari Jambi*, vol. 22, no. 2, hal. 991, 2022, doi: 10.33087/jiubj.v22i2.2175.

[9] J. S. A. Rajjani, B. T. Hanggara, dan Y. T. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan …," *... Teknol. Inf. dan Ilmu ...*, vol. 5, no. 5, hal. 1734–1744, 2019, [Daring]. Tersedia pada: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/8982/4092

 *ISSN:2302-8149*
*e-ISSN:2540-9719*

[10] L. F. Wirawan dan J. Tambotoh, "Evaluasi Kinerja Tata Kelola Teknologi Informasi pada PT. XYZ Menggunakan COBIT 2019," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 11, no. 3, hal. 775, 2022, doi: 10.35889/jutisi.v11i3.992.

[11] A. Christopher, *"Employing COBIT 2019 for Enterprise Governance Strategy,"* *ISACA*, 2019. https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy#16

[12] P. N. Anastasia, L. H. Atrinawati, P. Studi, S. Informasi, dan I. T. Kalimantan, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Hotel Xyz perkembangan bisnis maupun tamu hotel . Dampak positif tersebut seperti jangkauan yang TI . Jika layanan TI dalam perusahaan tidak dikelola dengan baik , maka akan," *J. Sist. Inf.*, vol. 12, no. 2, 2020.

[13] D. Darmawan dan A. F. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," *J. Comput. Inf. Syst. Ampera*, vol. 3, no. 1, hal. 1–17, 2022, doi: 10.51519/journalcisa.v3i1.139.

[14] M. Silvianthie, S. Suprapto, dan A. R. Perdanakusuma, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. IKI Karunia Indonesia menggunakan COBIT 2019," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 12, hal. 5726–5735, 2022, [Daring]. Tersedia pada: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/11983

[15] M. Lestari, Y. Nataliani, dan I. R. Widiasari, "Analisis Kinerja Sistem Informasi Akademik Menggunakan Framework Cobit 2019 (Studi Kasus: Sia-Sat Uksw)," *JUSIM (Jurnal Sist. Inf. Musirawas)*, vol. 7, no. 1, hal. 1–12, 2022, doi: 10.32767/jusim.v7i1.1424.

[16] N. M. Parera, J. J. C. Tambotoh, "Pengukuran Kapabilitas Tata Kelola Teknologi Informasi pada DISKOMINFO Salatiga menggunakan COBIT2019," *J. SISTEMASI*, vol. 13, no. 1, hal. 324-334, 2024, doi: https://doi.org/10.32520/stmsi.v13i1.3669