JURNAL ACCOUNTING INFORMATION SYSTEM
AIMS
Jurnal Accounting Information System (AIMS)
Volume 6 No. 2 | September 2023 : 180-201
DOI: 10.32627
https://jurnal.masoemuniversity.ac.id/index.php/aims
p-ISSN: 2615-7381
e-ISSN: 2621-7279

# Audit Manajemen Risiko Sistem Informasi pada Website Digo.id dengan Framework COBIT 5 dan ISO 31000

**Putra Pamungkas Sukmana[1], Titan Parama Yoga [2], Chairul Habibi[3]**
[1,2,3]Sistem Informasi, Universitas Informatika dan Bisnis Indonesia, Indonesia
putrapps19@gmail.com

**Info Artikel**
***Sejarah artikel :***
Diterima September 2023
Direvisi September 2023
Disetujui September 2023
Diterbitkan September 2023

***ABSTRACT***
*This research was conducted to know, analyze, and audit on information system risk management on Digo.id website. The framework used in this audit research is COBIT 5 and ISO 31000, using qualitative descriptive research methods, these methods are used to obtain results that can be a clear picture of how Risk Management is implemented by the company. The results showed that the Existing Capability is at level 1, while the Capability Target is at level 3 so the final result of this audit is that the company still has 2 Capability GAPs to achieve the Capability Target.*

***Keywords*** **:** *APO12; COBIT 5; EDM03; Information System Risk Management Audit; ISO 31000.*

**ABSTRAK**
Penelitian ini dilakukan untuk mengetahui, menganalisis, dan mengaudit pada manajemen risiko sistem informasi di situs web Digo.id. Kerangka kerja yang digunakan pada penelitian audit ini adalah COBIT 5 dan ISO 31000, dengan menggunakan metode penelitian deskriptif kualitatif, metode ini digunakan untuk mendapatkan hasil yang bisa menjadi gambaran jelas bagaimana Manajemen Risiko yang dilaksanakan oleh perusahaan. Hasil penelitian menunjukan bahwa *Capability Existing*-nya adalah ada di level 1, sedangkan untuk *Capability Targetnya* berada di level 3 dengan begitu hasil akhir dari dilaksanakan audit ini adalah perusahaan masih memiliki 2 *Capability GAP* untuk mencapai *Capability Target*.

**Kata Kunci :** APO12; Audit Manajemen Risiko Sistem Informasi; COBIT 5; EDM03; ISO 31000.

## PENDAHULUAN

Perkembangan dunia digital saat ini sangat pesat, semuanya berbasis teknologi dengan *level* yang tinggi, dengan perkembangan dunia digital ini orang orang yang mengakses tentu tidak sedikit setiap waktunya. Akses dunia digital yang massif bisa memicu sebuah sistem khususnya sistem informasi lebih banyak menghadapi risiko risiko yang ada. Era digitalisasi yang terus berkembang membuat pengetahuan teknologi semakin meluas baik ke sisi positif maupun negatif, baik secara *software* maupun *hardware*, baik secara perlindungan ataupun penyerangan. Dengan begitu sebuah sistem informasi perlu dipersiapkan sematang mungkin dan organisasi perlu mempersiapkan segala kemungkinan yang bisa terjadi dan berisiko bagi sistem yang ada, Ketika sistem sudah menghadapi risiko yang sangat berat maka ini akan sangat bermasalah bagi perusahaan tersebut.

Risiko pada Sistem bisa berupa ancaman dari luar atau *error* yang terjadi karena hal lain didalam sistem, risiko yang sering muncul ketika sistem tersebut digunakan yaitu seperti adanya virus yang menyerang informasi pada sistem,

p-ISSN: 2615-7381
e-ISSN: 2621-7279

peretas yang mencuri data hingga merusak sistem, bisa juga risiko seperti kerusakan sistem pendukung lainnya bisa itu jaringan listrik atau yang lainnya. Ini sangat perlu diantisipasi dan di kelola secara benar benar, guna meminimalisir kerusakan dan kerugian yang fatal bagi perusahaan tersebut baik secara *software* maupun *hardware*.

Perusahaan yang memiliki Sistem Informasi pastinya perlu melindungi setiap data, informasi dan sistem itu sendiri. Selain melindungi perlu juga diberikan kesiapan pada sistem menghadapi ancaman yang ada, risiko yang bisa terjadi pada sistem harus dihindari sebisa mungkin dengan selalu dilakukannya improvisasi atau pengembangan yang lebih baik, Analisa sistem informasi sering dilakukan perusahaan untuk menghindari segala ancaman dan dengan analisa tersebut selalu diharapkan mendapatkan jalan terbaik untuk menyelesaikan atau hanya mengembangkan dari perlindungannya.

Analisa sistem bisa dilakukan oleh intern perusahaan atau oleh pihak luar yang membantu menganalisa, Analisa ini bisa berupa Analisa jaringan, Analisa keamanan, Analisa risiko, ataupun Analisa hal lain pada sistem tersebut. Dengan banyaknya problema dan ancaman yang bisa terjadi, perusahaan pasti sangat menghawatirkan ancaman ancaman yang ada, untuk mengetahui ancaman tersebut, dilakukannya audit risiko adalah salah satu cara untuk bisa mengetahui setiap ancaman dan dampak yang bisa terjadi pada sistem informasi, dengan dilakukannya audit risiko pada perusahaan maka ini bisa mengutungkan bagi mereka karena audit risiko ini menjadi metodologi penelitian pemeriksaan yang dipakai untuk memberikan kepastian dan jaminan bahwa risiko yang mungkin terjadi pada sistem sudah dikelola. Audit risiko pada sistem informasi dilakukan agar bisa mendapatkan evaluasi fakta ini bermanfaat untuk memutuskan apakah sistem tersebut terlindungi dan terpelihara sesuai dengan keinginan organisasi, guna mencapai efektifitas dan efisiensi penggunaan sumber dayanya.

Audit TI banyak sekali *framework*-nya, *framework* tersebut digunakan sebagai standarisasi atau panduan untuk menjalankan praktik dari audit itu sendiri, salah satu *framework* yang sering digunakan dalam melakukan audit yaitu COBIT, secara umum COBIT mencakup tentang perencanaan dan organisasi, pengadaan dan implementasi, pengantaran dan dukungan , juga tentang pengawasan dan evaluasi. COBIT 5 adalah sebuah kerangka kerja (*framework*) yang menggambarkan praktik manajemen TI *global* yang terbaik untuk membantu organisasi mencapai tujuannya melalui penggunaan teknologi informasi.[2]

Digo.id merupakan salah satu *website* berita yang ada di Indonesia, *website* ini hadir sejak agustus 2022, portal berita ini memiliki tujuan menyuguhkan berbagai informasi yang disajikan dengan materi yang disukai anak muda, tanpa menafikan orang dewasa. Dengan komitmen Digo.id memiliki perbedaan dengan portal berita lainnya, Digo.id mengedepankan atau menggali sisi potensi anak muda Indonesia atau lebih dikenal milenial. Berdasarkan hasil analisa penulis, Digo.id merupakan website yang memiliki potensi besar kedepannya dengan menyuguhkan berita berita yang bisa menjadi rujukan bagi anak muda Indonesia. Dengan potensi yang kuat tentunya Digo.id perlu memanajemen setiap risiko yang mungkin terjadi pada sistem informasinya agar privasi, data, dan sistem bisa terlindungi dengan baik. Dengan begitu dilakukannya manajemen risiko bisa

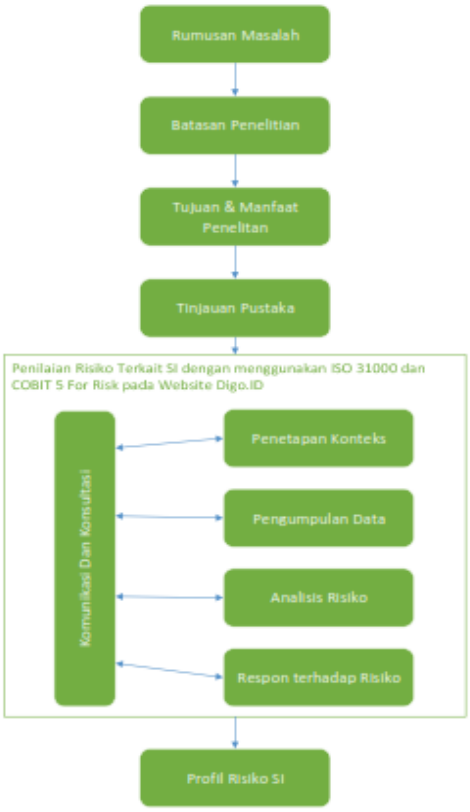
p-ISSN: 2615-7381
e-ISSN: 2621-7279

meminimalisir dan mengetahui apakah sistem informasi dari Digo.id ini sudah terlindungi dan terhindar dari ancaman ancaman yang bisa berisiko tinggi pada sistem, yang nantinya bila telah diketahui setiap ancamannya, risiko tersebut bisa di manajemen dengan baik.

Audit Manajemen Risiko yang akan dilakukan oleh peneliti akan menggunakan *framework COBIT 5 for Risk* dan *ISO 31000*. Biasanya proses audit manajemen risiko bisa dengan menggunakan satu *framework*, namun pada penelitian ini menggunakan dua *framewor*k karena *COBIT 5* digunakan sebagai Kerangka bantuan perusahaan dalam mencapai hasil nilai terbaik dalam Kelola dan manajemen Teknologi Informasinya, sedangkan *ISO 31000* merupakan metode yang digunakan dalam segala jenis organisasi yang tentunya meliputi identifikasi risiko dan pemeliharaan risiko yang bertujuan melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem danaset pendukung kinerja sistem di masa depan. Standar *ISO* digunakan dalam semasa hidup organisasi tersebut juga sebagai standar segala kegiatan sistem maupun proyeknya.

## METODE

Metode yang digunakan pada penelitian ini adalah metode pendekatan deskriptif kualitatif. Pendekatan penelitian ini digunakan untuk mendapatkan hasil yang bisa menjadi gambaran jelas bagaimana Manajemen Risiko yang dilaksanakan oleh perusahaan tersebut berdasarkan COBIT 5 dan *Standar ISO* 31000. Dalam pengumpulan data yang dilakukan dalam penelitian ini diambil dari wawancara juga observasi tentang tingkat manajemen risiko sistem informasi pada Digo.id.




**Gambar 1. Tahapan Penelitian**

p-ISSN: 2615-7381
e-ISSN: 2621-7279

Pada audit manajemen risiko ini menggunakan *framework* COBIT 5 dan Standar ISO 31000. Penggunaan kedua *framework* ini harus dengan dimulai dari penggabungan dengan menemukan titik temu dari kedua *framework.* Berikut adalah titik temu dari kedua *framework.*


**Gambar 2. Titik temu antara ISO 31000 dan COBIT 5 *For Risk* [20]**

Pada Gambar 2, sesuai dengan standar ISO 31000, proses manajemen risiko dibagi menjadi 6 (Enam) tahapan, yaitu Lingkup, Konteks, Kriteria; Asemen Risiko; Identifikasi Risiko; Analisis Risiko; Evaluasi Risiko; Perlakuan Risiko.Pada Gambar 2, COBIT 5 untuk risiko yang menggunakan proses APO12. APO 12 ini dibagi jadi 6 *management practice,* diurutkan berdasarkan proses pengerjaannya, yaitu *Collect Data* (APO12.01), *Analyze Risk* (APO12.02), *Maintain Risk Profile* (12.03), *Articulate Risk* (APO12.04), *Define Risk Management Action Portfolio* (APO12.05), *Respond to Risk* (APO12.06).

## HASIL DAN PEMBAHASAN

### Pemeriksaan Data Temuan Audit Manajemen Risiko pada Domain EDM03

Proses number EDM03 memiliki turunan untuk penetapan hasil sebagai berikut :

**Tabel 1. Tabel Outcome dari Proses EDM03**

| Outcome | Deskripsi |
|---|---|
| EDM03.01 | Risiko perusahaan terkait TI tidak melebihi tingkat risiko yang dapat diterima dan toleransi risiko, dampak risiko TI terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diantisipasi. |
| EDM03.02 | Pelaksana manajemen risiko bisa menjamin manajemen risiko, dipastikantidak melebihi pertumbuhan risiko organisasi. |
| EDM03.03 | Proses manajemen resiko menyusun bagaimana masalah resiko TI diidentifikasi, dilacak dan dilaporkan. Penilaian kapabilitas dilakukan terhadap aktifitas (*base practices*) yang dilakukan dan output (*work product*) yang dilakukandan output yang dihasilkan oleh organisasi dari setiap proses pada EDM03.03. |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

Presentasi *achievement/outcome* menentukan nilai dari *Achievement Total* PA 1.1 dan *Rating by Criteria* untuk EDM03, namun presentase *achievement/outcome* masing-masing *outcome* ditentukan berdasarkanpresentase *achievement/component*. Komponen dari masing-masing *outcome* yaitu sebagai berikut.

**Tabel 2. Komponen dari masing-masing outcome pada proses EDM03**

| Outcome | Component | Number | Description |
|---|---|---|---|
| EDM03.01 | Work Product Output | EDM03-WP1 | Panduan selera risiko |
| | | EDM03-WP2 | Tingkat toleransi risiko yang disetujui |
| | | EDM03-WP3 | Evaluasi kegiatan manajemen risiko |
| | Base Practice + Work Product Input | EDM03-BP1 | Mengevaluasi manajemen risiko. |
| EDM03.02 | Work Product Output | EDM03-WP1 | Panduan selera risiko |
| | | EDM03-WP2 | Tingkat toleransi risiko yang disetujui |
| | | EDM03-WP3 | Evaluasi kegiatan manajemen risiko |
| | | EDM03-WP4 | Kebijakan manajemen risiko |
| | | EDM03-WP5 | Tujuan utama yang harus dipantau untukmanajemen risiko |
| | | EDM03-WP6 | Menyetujui proses untuk mengukur manajemen risiko |
| | | EDM03-WP7 | Remedial actions to address risk management deviations |
| | | EDM03-WP8 | Masalah manajemen risiko untuk dewan |
| | Base Practice + Work Product Input | EDM03-BP1 | Mengevaluasi manajemen risiko |
| | | EDM03-BP2 | Manajemen risiko langsung. |
| | | EDM03-BP3 | Memantau manajemen risiko |
| EDM03.03 | Work Product Output | EDM03-WP4 | Kebijakan manajemen risiko |
| | | EDM03-WP5 | Tujuan utama yang harus dipantau untuk manajemen risiko |
| | | EDM03-WP6 | Menyetujui proses untuk mengukur manajemen risiko |
| | | EDM03-WP7 | Tindakan perbaikan untuk mengatasi penyimpangan manajemen risiko |
| | | EDM03-WP8 | Masalah manajemen risiko untuk dewan |
| | Base Practice + Work Product Input | EDM03-BP2 | Direct risk management. |
| | | EDM03-BP3 | Monitor risk management. |

Proses *component* diperoleh dari total semua jawaban "Y" dibagi total jumlah pertanyaan dari setiap *component*-nya, seperti tabel berikut.

Tabel diatas merupakan tabulasi penilaian audit pada proses *number* EDM03, hasil dari *achievement component* pertama didapatkan dari hasil rekapitulasi dari hasil dilaksanakannya wawancara kepada CEO perusahaan.

Dari EDM03-WP1, EDM03-WP2, dan EDM03-WP3 dijumlahkan jawabannya menjadi 100%. Selanjutnya perhitungan number EDM03-BP1

p-ISSN: 2615-7381
e-ISSN: 2621-7279

menghasilkan perhitungan sebanyak 100%. Selanjutnya diakumulasikan dari seluruh bagian *outcome* EDM03.01 yang dibagi 2 dengan begitu menghasilkan *Achievement Outcome* EDM03.01 sebesar 100%

Perhitungan yang kedua dari EDM03.02 yaitu untuk EDM03-WP1 hingga EDM03-WP8 memiliki *achievement component* sebesar 63% dan EDM-BP1sampai EDM-BP1 yang memiliki *achievement component* sebesar 75% dengan begitu kedua bagian diakumulasikan dan menghasilkan *Achievement Outcome* sebesar 69%

Dan untuk perhitungan terakhir, EDM03.03 memiliki perhitungan dari WPnya sebesar 40% sedangkan untuk dari BPnya sebesar 70%, dengan begitu akumulasi dari kedua bagian yang sudah dihitung menghasilkan *Achievement Outcome* sebesar 55%

Dari semua *Achievement Outcome* yang telah dihitung, *Total Achievement* P.A 1.1 dari EDM03 dijumlahkan terlebih dahulu dan dibagi 3 seperti berikut :

$$\frac{100\% + 69\% + 55\%}{3} = 75\%$$

Dengan begitu *Achievement Outcome* yang didapat dari EDM03 P.A 1.1 ini yaitu 75%.

**Pemeriksaan Data Temuan Audit Manajemen Risiko pada Domain APO12**

Setelah dilaksanakannya pemeriksaan data temuan pada domain EDM03, selanjutnya dilakukan juga pemeriksaan data temuan pada APO12nya, Proses number EDM03 memiliki turunan untuk penetapan hasil sebagai berikut :

**Tabel 3. Tabel Outcome dari Proses EDM03**

| Outcome | Deskripsi |
|---|---|
| APO12.01 | Risiko terkait TI diidentifikasi, dianalisis, dikelola, dan dilaporkan. |
| APO12.02 | Profil risiko yang terkini juga lengkap telah tersedia. |
| APO12.03 | Semua tindakan pengelolaan risiko yang signifikan dikelola dan berada di bawahkendali. |
| APO12.04 | Tindakan pengelolaan risiko diimplementasikan dengan efektif. |

Presentasi *achievement/outcome* menentukan nilai dari *Achievement Total* PA 1.1 dan *Rating by Criteria* untuk APO12, namun presentase *achievement/outcome* masing-masing *outcome* ditentukan berdasarkan presentase *achievement/component*. Komponen dari masing-masing *outcome* yaitu sebagai berikut.

**Tabel 4. Komponen dari masing-masing *outcome* pada proses APO12**

| Outcome | Component | Number | Description |
|---|---|---|---|
| | Work Product Output | APO12-WP1 | Data mengenai lingkungan operasional terkait risiko |
| | | APO12-WP2 | Data mengenai peristiwa risiko dan faktor kontribusi |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Outcome | Component | Number | Description |
|---|---|---|---|
| | | APO12-WP3 | Isu risiko yang muncul dan faktor-faktor terkait |
| | | APO12-WP4 | Lingkup upaya analisis risiko |
| | | APO12-WP5 | Skenario risiko TI |
| | | APO12-WP6 | Hasil analisis risiko |
| APO12.01 | Base Practice +Work Product Input | APO12-BP1 | Collect Data. Identifikasi dan kumpulkan data yang relevan untuk memungkinkan identifikasi,analisis, dan pelaporan risiko terkait TI yang efektif. |
| | | APO12-BP2 | Menganalisis risiko. Kembangkan informasi yang berguna untuk mendukung keputusan risiko yangmempertimbangkan relevansi bisnis darifaktor risiko. |
| APO12.02 | Work Product Output | APO12-WP7 | Skenario risiko yang didokumentasikanberdasarkan unit bisnis dan fungsi |
| | | APO12-WP8 | Profil risiko yang teragregasi, termasukstatus dari tindakan pengelolaan risiko |
| | Base Practice + Work Product Input | APO12-BP3 | Menjaga profil risiko. Menjaga inventaris risiko yang diketahui beserta atribut risiko (termasuk frekuensiyang diharapkan, dampak potensial, danrespons) dan sumber daya terkait, kapabilitas, dan aktivitas kontrol saat ini. |
| APO12.03 | Work Product Output | APO12-WP9 | Laporan analisis risiko dan profil risikountuk pemangku kepentingan |
| | | APO12-WP10 | Meninjau hasil evaluasi risiko pihak ketiga |
| | | APO12-WP11 | Peluang penerimaan risiko yang lebih besar |
| | | APO12-WP12 | Usulan proyek untuk mengurangi risiko |
| | | APO12-WP13 | Rencana tanggap insiden terkait risiko |
| | | APO12-WP14 | Komunikasi dampak risiko |
| | | APO12-WP15 | Penyebab akar terkait risiko |
| | Base Practice + Work Product Input | APO12-BP4 | Mengartikulasikan risiko. Menyediakan informasi mengenai kondisiterkini dari paparan dan peluang terkait TI |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Outcome | Component | Number | Description |
|---|---|---|---|
| | | APO12-BP5 | Menentukan portofolio tindakan pengelolaanrisiko. |
| | | APO12-BP6 | Menanggapi risiko secara tepat waktu denganlangkah-langkah yang efektif untuk membatasi besarnya kerugian dari peristiwa terkait TI. |
| APO12.04 | Work Product Output | APO12-WP4 | Lingkup upaya analisis risiko |
| | | APO12-WP5 | Skenario risiko TI |
| | | APO12-WP6 | Hasil analisis risiko |
| | | APO12-WP9 | Laporan analisis risiko dan profil risiko untuk pemangku kepentingan |
| | | APO12-WP10 | Meninjau hasil evaluasi risiko pihakketiga |
| | | APO12-WP11 | Peluang penerimaan risiko yang lebih besar |
| | | APO12-WP12 | Usulan proyek untuk mengurangi risiko |
| | Base Practice + Work Product Input | APO12-BP2 | Menganalisis risiko. Kembangkan informasi yang berguna untuk mendukung keputusan risiko yang mempertimbangkan relevansi bisnis dari faktor risiko. |
| | | APO12-BP4 | Mengartikulasikan risiko. Menyediakan informasi mengenai kondisiterkini dari paparan dan peluang terkait TI |
| | | APO12-BP5 | Menentukan portofolio tindakan pengelolaan risiko. |

Proses *component* diperoleh dari total semua jawaban "Y" dibagi total jumlah pertanyaan dari setiap *component*-nya, seperti table berikut.

**Tabel 5. Tabulasi penilaian audit terhadap proses number APO12**

| Outcome | Number | Description | Achievement Component | Achievement Outcome | Total Achievement PA 1.1 (APO12) |
|---|---|---|---|---|---|
| | APO12-WP1 | Data mengenai lingkungan operasional terkait risiko | | | |
| | APO12-WP2 | Data mengenai peristiwa risikodan faktor kontribusi | | | |
| | APO12-WP3 | Isu risiko yang muncul dan faktor-faktor terkait | | | |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Outcome | Number | Description | Achievement Component | Achievement Outcome | Total Achievement PA 1.1 (APO12) |
|---|---|---|---|---|---|
| APO12.01 | APO12-WP4 | Lingkup upaya analisis risiko | 83% | 56% | |
| | APO12-WP5 | Skenario risiko TI | | | |
| | APO12-WP6 | Hasil analisis risiko | | | |
| | APO12-BP1 | Collect Data. Identifikasi dan kumpulkan datayang relevan untuk memungkinkan identifikasi, analisis, dan pelaporan risiko terkait TI yang efektif. | 29% | | |
| | APO12-BP2 | Menganalisis risiko. Kembangkan informasi yang berguna untuk mendukung keputusan risiko yang mempertimbangkan relevansi bisnis dari faktor risiko. | | | |
| APO12.02 | APO12-WP7 | Skenario risiko yang didokumentasikan berdasarkan unit bisnis dan fungsi | 100% | 64% | |
| | APO12-WP8 | Profil risiko yang teragregasi, termasuk status dari tindakan pengelolaan risiko | | | |
| | APO12-BP3 | Menjaga profil risiko. Menjaga inventaris risiko yangdiketahui beserta atribut risiko(termasuk frekuensi yang diharapkan, dampak potensial, dan respons) dan sumber daya terkait, kapabilitas, dan aktivitas kontrol saat ini. | 29% | | |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Outcome | Number | Description | Achievement Component | Achievement Outcome | Total Achievement PA 1.1 (APO12) |
|---|---|---|---|---|---|
| APO12.03 | APO12-WP9 | Laporan analisis risiko dan profil risiko untuk pemangku kepentingan | 71% | 61% | 60% |
| | APO12-WP10 | Meninjau hasil evaluasi risiko pihak ketiga | | | |
| | APO12-WP11 | Peluang penerimaan risiko yanglebih besar | | | |
| | APO12-WP12 | Usulan proyek untuk mengurangi risiko | | | |
| | APO12-WP13 | Rencana tanggap insiden terkaitrisiko | | | |
| | APO12-WP14 | Komunikasi dampak risiko | | | |
| | APO12-WP15 | Penyebab akar terkait risiko | | | |
| | APO12-BP4 | Mengartikulasikan risiko. Menyediakan informasi mengenai kondisi terkini dari paparan dan peluang terkait TI | 50% | | |
| | APO12-BP5 | Menentukan portofolio tindakan pengelolaan risiko. | | | |
| | APO12-BP6 | Menanggapi risiko secara tepat waktu dengan langkah-langkah yangefektif untuk membatasi besarnya kerugian dari peristiwa terkait TI. | | | |
| | APO12-WP4 | Lingkup upaya analisis risiko | 86% | 60% | |
| | APO12-WP5 | Skenario risiko TI | | | |
| | APO12-WP6 | Hasil analisis risiko | | | |
| | APO12-WP9 | Laporan analisis risiko dan profilrisiko untuk pemangku kepentingan | | | |
| | APO12-WP10 | Meninjau hasil evaluasi risiko pihak ketiga | | | |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Outcome | Number | Description | Achievement Component | Achievement Outcome | Total Achievement PA 1.1 (APO12) |
|---|---|---|---|---|---|
| APO12.04 | APO12-WP11 | Peluang penerimaan risiko yanglebih besar | 33% | | |
| | APO12-WP12 | Usulan proyek untuk mengurangi risiko | | | |
| | APO12-BP2 | Menganalisis risiko. Kembangkan informasi yang berguna untuk mendukung keputusan risiko yang mempertimbangkan relevansibisnis dari faktor risiko. | | | |
| | APO12-BP4 | Mengartikulasikan risiko. Menyediakan informasi mengenai kondisi terkini dari paparan dan peluang terkait TI | | | |
| | APO12-BP5 | Menentukan portofolio tindakan pengelolaan risiko. | | | |

Tabel diatas merupakan tabulasi penilaian audit pada proses *number* APO12, hasil dari *achievement component* pertama didapatkan dari hasil rekapitulasi dari hasil dilaksanakannya pemberian Kuisioner kepada CEO perusahaan yang lalu diteruskankepada karyawan perusahaan yang berkepentingan.

Dari APO12-WP1 hingga APO12-WP6 dijumlahkan jawabannya menjadi 83%. Selanjutnya perhitungan number APO12- BP1 dan APO12-BP2 menghasilkan perhitungan sebanyak 29%. Selanjutnya diakumulasikan dari seluruh bagian *outcome* APO12.01 yang dibagi 2 dengan begitu menghasilkan *Achievement Outcome* APO12.01 sebesar 56%

Perhitungan yang kedua dari APO12.02 yaitu untuk APO12-WP7 dan APO12-WP8 memiliki *achievement component* sebesar 100% dan APO12-BP3 memiliki *achievement component* sebesar 29% dengan begitu kedua bagian diakumulasikan danmenghasilkan *Achievement Outcome* sebesar 64%.

Setelah itu di perhitungan ketiga yaitu APO12.03 pada bagian 3 ini *Work product*-nya memiliki *achievement component* 71% dan perhitungan *Base Practice* + *Work Product Input* memiliki *achievement component* 50%,kalkulasi dari 2 bagian tersebut menghasilkan 61% *achievement outcome.*

Dan untuk perhitungan terakhir, APO12.04 memiliki perhitungan dari WPnya sebesar 86% sedangkan untuk dari BPnya sebesar 33%, dengan begitu akumulasi dari kedua bagian yang sudah dihitung menghasilkan *Achievement*

p-ISSN: 2615-7381
e-ISSN: 2621-7279

*Outcome* sebesar 60%

Dari semua *Achievement Outcome* yang telah dihitung, *Total Achievement* P.A 1.1 dari APO12 dijumlahkan terlebih dahulu dan dibagi 4 seperti berikut :

$$\frac{56\% + 64\% + 61\% + 60\%}{4} = 60\%$$

Dengan begitu *Achievement Outcome* yang didapat dari EDM03 P.A 1.1 ini yaitu 60%, Total *Achievement* PA 1.1 dari tiap domain yang digunakan, dimasukan kedalam format yang disesuaikan. Maka dihasilkanlah *rating* dari masing masing level yang telah di *planning* dari tiap domain, seperti berikut :

**Tabel 6. Rating untuk Domain EDM03**

| Process Name | Level 1 | Level 2 | | Level 3 | |
|---|---|---|---|---|---|
| **EDM03** | **PA 1.1** | **PA 2.1** | **PA 2.2** | **PA 3.1** | **PA 3.2** |
| **Rating by Criteria** | 75% | 50% | 75% | 20% | 8% |
| **Rating** | L | P | L | P | N |
| **Capability Level Achieved** | 1 | Stop! | Stop! | Stop! | Stop! |
| **Capability Existing** | 1 | | | | |

Tabel tersebut menunjukan rating untuk Domain EDM03. Pada *process name*-nya dapat dilihat untuk level 1 menghasilkan *Rating by Criteria* 75% dimana itu menjadikan *rating* yang didapat L, yang berarti L adalah *LargelyAchieved.*

Setelah mendapatkan hasil level 1 masih tidak mencapai *Rating* F (*Fully Achieved*) maka dengan itu perusahaan tidak bisa berlanjut pada Level 2, walaupun telah dilaksanakan wawancara untuk level 2 dan 3 namun hasil pada level 1 masih belum mencukupi.

Selanjutnya untuk *Rating* APO12 yang telah dilaksanakan dengan pengumpulan data berupa kuisioner, kuisioner ini disebar ke 10 orang dan dilakukan penarikan kesimpulan dari 10 orang yang menjawab kuisioner tersebut, jika dari 10 orang itu 75% atau lebih menjawab iya maka akan diambil kesimpulan bahwa jawabannya iya. Berikut adalah *rating* untuk domain APO12

**Tabel 7. Rating untuk Domain APO12**

| Process Name | Level 1 | Level 2 | | Level 3 | |
|---|---|---|---|---|---|
| **APO12** | **PA 1.1** | **PA 2.1** | **PA 2.2** | **PA 3.1** | **PA 3.2** |
| **Rating by Criteria** | 60% | 38% | 31% | 10% | 0% |
| **Rating** | L | P | L | P | N |
| **Capability Level Achieved** | 1 | Stop! | Stop! | Stop! | Stop! |
| **Capability Existing** | 1 | | | | |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

Pada domain APO12, dapat dilihat pada tabel diatas bahwa *Rating by criteria* untuk level 1 yang didapat hanya 60%, yang berarti hanya mendapat *Largely Achieved.*

Dalam tabel tersebut, level APO12 yang dicapai hanya sampai level 1, dimana perusahaan belum bisa memenuhi *Process* yang ada pada level 1, dan dapat dilihat ketika level 1 belum memenuhi, level selanjutnya pun walau memiliki *Rating,* Tetap ada dibawah dari target yang diharuskan untuk berlanjut ke level selanjutnya.

Maksud dari huruf yang diberikan pada rating tersebut adalah sebagai berikut :

a. N (Not Achieved / Tidak Tercapai)
   Kategori ini terjadi apabila range yang didapatkan dari rating bycriteria berkisaran antara 0-15%
b. P (*Partialy Achieved* / Sebagian Tercapai)
   Kategori ini terjadi apabila *range* yang didapatkan dari *rating by criteria* berkisaran antara 15-50%
c. L (*Large Achieved* / Sebagian Besar Tercapai)
   Kategori ini terjadi apabila *range* yang didapatkan dari *rating by criteria* berkisaran antara 50-85%
d. F (*Fully Achieved* / Sepenuhnya tercapai)
   Kategori ini terjadi apabila *range* yang didapatkan dari *rating by criteria* berkisaran antara 85-100%

**Evaluasi Manajemen Risiko**

Tahapan evaluasi manajemen risiko ini terdiri dari beberapa bagian, yang dimana nantinya di tahapan ini akan ada hasil akhir berupa rekomendari untuk perusahaan yang didalamnya menjelaskan terkait profil manajemen dari perusahaan.

**Penilaian Hasil Existing**

Perolehan *rating* dari masing-masing domain telah didapatkan, tahap selanjutnya yaitu penilaian hasil *existing*, diantaranya :

1. Kondisi *Existing* EDM03 PA.1.1
   a. Belum Adanya Kebijakan manajemen risiko
   b. Belum ada persetujuan proses untuk mengukur manajemen risiko
   c. Belum ada Penyampaian budaya sadar risiko TI dan memberdayakan perusahaan untuk secara proaktif mengidentifikasi risiko, peluang, dan potensi dampak bisnis TI.
   d. Belum ada Implementasi langsung dari mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkan ke tingkat manajemen yang sesuai, didukung oleh prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana)
   e. Belum ada tinjauan pemangku kepentingan utama atas kemajuan perusahaan menuju tujuan yang teridentifikasi.
   f. Belum ada Laporkan setiap masalah manajemen risiko kepada dewan atau

p-ISSN: 2615-7381
e-ISSN: 2621-7279

komite eksekutif.

g. Belum ada yang Mempromosikan budaya sadar risiko TI danmemberdayakan perusahaan untuk secara proaktif mengidentifikasi risiko, peluang, dan potensi dampak bisnis TI.
h. Belum ada Implementasi langsung dari mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkan ke tingkat manajemen yang sesuai, didukung oleh prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).
i. Belum ada Laporkan setiap masalah manajemen risiko kepada dewan atau komite eksekutif.

2. Kondisi *Existing* EDM03 PA 2.1 dan PA 2.2
   a. Tidak ada Identifikasi tujuan untuk kinerja proses. Tujuan kinerja, dicakup bersama dengan asumsi dan kendala, didefinisikan dan dikomunikasikan.
   b. Catatan kinerja proses tidak memberikan detail tentang hasil atau hasil akhirnya.
   c. Tidak ada perencanaan dan pemantau kinerja proses untuk memenuhi tujuan yang diidentifikasi. Ukuran dasar kinerjaproses yang terkait dengan tujuan bisnis ditetapkan dan dipantau. Mereka termasuk tonggak penting, kegiatan yang diperlukan, perkiraan dan jadwal.
   d. Belum ada Rencana proses yang harusnya mencakup perincian rencana komunikasi proses serta pengalaman kinerja proses, persyaratan keterampilan.
   e. Belum ada penentuan tanggung jawab dan wewenang untuk melakukan proses. Tanggung jawab utama dan wewenang untuk melakukan aktivitas utama dari proses didefinisikan, ditugaskan dan dikomunikasikan. Kebutuhan untuk pengalaman kinerja proses, pengetahuan dan keterampilan didefinisikan.
   f. Belum ada identifikasi dan pembuat sumber daya yang tersedia untuk melakukan proses sesuai dengan rencana. Sumber dayadan informasi yang diperlukan untuk melakukan aktivitas utama dari proses diidentifikasi, disediakan, dialokasikan, dan digunakan.
   g. Belum ada pengelola antarmuka antara pihak-pihak yang terlibat. Individu dan kelompok yang terlibat dalam proses diidentifikasi, tanggung jawab ditentukan dan mekanisme komunikasi yang efektif.
   h. Belum ada penetapan persyaratan untuk dokumentasi dan kontrol produk kerja. Ini harus mencakup identifikasi ketergantungan, persetujuan dan ketertelusuran persyaratan
   i. Belum ada Tinjauan dan penyesuaian produk kerja untuk memenuhi persyaratan yang ditentukan. Produk kerja dapat ditinjau terhadap persyaratan sesuai dengan pengaturan yang direncanakan dan setiap masalah yang timbul diselesaikan.
3. Kondisi *Existing* EDM03 PA 3.1 dan 3.2
   a. Belum ada Kebijakan dan standar yang memberikan rincian tujuan organisasi untuk proses, standar kinerja minimum, prosedur standar, dan persyaratan pelaporan dan pemantauan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

b. Belum ada penentuan proses standar yang mendukung penerapan proses yang ditentukan. Proses standar didefinisikan yang mengidentifikasi elemen proses fundamental dan memberikan panduan dan prosedur untuk mendukung implementasi dan panduan tentang bagaimana hal itu dapat disesuaikan bila diperlukan.
c. Belum ada Kebijakan dan standar yang menyediakan pemetaan proses dengan rincian proses standar dan urutan serta interaksi yang diharapkan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
d. Belum ada urutan dan interaksi antar proses sehingga bekerjasebagai sistem proses yang terintegrasi. Urutan proses standardan interaksi dengan proses lain ditentukan dan dipertahankan ketika proses diterapkan di berbagai bagian organisasi.
e. Belum ada identifikasi peran dan kompetensi untuk melakukan proses standar.
f. Belum ada Kebijakan dan standar yang mengidentifikasi infrastruktur minimum yang dibutuhkan dan lingkungan kerja untuk melakukan proses tersebut. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
g. Belum ada Identifikasi infrastruktur dan lingkungan kerja, yang diperlukan untuk melakukan proses standar. Infrastruktur (fasilitas, alat, metode, dll.) dan lingkungan kerja untuk melakukan proses standar diidentifikasi.
h. Belum ada penentuan metode yang sesuai untuk memantau keefektifan dan kesesuaian proses standar, termasuk memastikan bahwa kriteria dan data yang sesuai diperlukan untuk memantau keefektifan dan kesesuaian proses telah ditetapkan, dan menetapkan kebutuhan untuk melakukan audit internal dan tinjauan manajemen.
i. Belum ada Kebijakan dan standar yang menentukan standar yang harus diikuti di semua implementasi proses. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
j. Belum ada penerapan proses yang ditentukan yang memenuhikonteks. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, itu didasarkan pada proses standar, disesuaikan sebagaimana mestinya, dengan kesesuaian dengan persyaratan proses yang ditentukan diverifikasi.
k. Belum ada penetapan dan komunikasi peran, tanggung jawab, dan wewenang untuk melakukan proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, wewenang dan peran untuk melakukan aktivitas proses ditetapkan dan dikomunikasikan.
l. Belum ada Dokumentasi proses harus memberikan rincian kompetensi dan persyaratan pelatihan.
m. Belum ada plan proses yang mencakup perincian rencanakomunikasi proses, rencana pelatihan, dan rencana sumber daya untuk setiap contoh proses.
n. Tidak ada pemastian kompetensi yang diperlukan untuk melakukan proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, kompetensi yang sesuai untuk personel yang ditugaskan

diidentifikasi dan pelatihan yang sesuai tersedia bagi mereka yang menerapkan proses yang ditentukan.

o. Belum melakukan perencanaan proses yang mencakup perincian rencana sumber daya untuk setiap contoh proses
p. Belum Menyediakan sumber daya dan informasi yang mendukung kinerja proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, sumber daya manusia dan informasi yang diperlukan untuk melakukan proses tersebut tersedia, dialokasikan, dan digunakan
q. Belum ada perencanaan proses yang mencakup perincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses.
r. Tidak Menyediakan infrastruktur proses yang memadai untuk mendukung kinerja proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, dukungan organisasi, infrastruktur, dan lingkungan kerja yang diperlukan tersedia, dialokasikan, dan digunakan.
s. Belum ada Catatan kualitas dan GWP 9.0, Catatan kinerja proses harus memberikan bukti alat tinjauan yang dilakukan untuk setiap contoh proses.
t. Belum mengumpulkan dan menganalisis data tentang kinerja proses untuk menunjukkan kesesuaian dan efektivitasnya. Data yang diperlukan untuk memantau keefektifan dan kesesuaian proses di seluruh organisasi ditentukan, dikumpulkan, dan dianalisis sebagai dasar untuk perbaikan berkelanjutan.

4. Kondisi *Existing* APO12 PA 1.1
   a. Belum Adanya Penyimpan data *risk event* yang dapat atau telah menyaebabkan dampak terhadap manfaat IT, program IT dan project deliverya, serta IT operation dan service deliverya. Menangkap data yang revelan dari isu terkait, insiden, masalah dan investigasi.
   b. Belum adanya Penentuan faktor yang memepengaruhi risiko- risiko telah didata pada risk event.
   c. Belum adanya Penentuan Kondisi spesifik yang ada atau tidak ketika terjadi risk event dan bagaimana kondisi dipengaruhi frekuensi event dan kerugian besar.
   *d.* Belum adanya Perlakuan analisis secara berkala terkait event dan risk factor untuk mengidentifikasi isu risiko yang baru dan mengumpulkan pemahaman internal yang terasosiasi dan *risk factor external.*
   e. Belum adanya Pembangunan dan Pembaharuan skenario risikoTI secara berkala, termasuk juga kombinasi skenario yang bersifat cascading dan/atau koinsidentil dari tipe ancaman dan mengembangkan ekspektasi untuk aktivitas kontrol spesifik, kapabilitas untuk mendeteksi dan pengukuran respon lainnya.
   f. Belum adanya Estimasi frekuensi dan besarnya kehilangan atau keuntungan yang berkaitan dengan skenario risiko TI. Memperhitungkan seluruh faktor risiko, evaluasi kontroloperasional dan estimasi level risiko residual.
   g. Belum adanya Pembandingan risiko residual dengan tingkat risk tolerance yang dapat diterima dan mengidentifikasi gejala yang mungkin membutuhkan risk response

h. Belum adanya Analisis cost-benefit dari potensi pilihan risk response seperti avoid, reduce/mitigate, transfer/share dan accept dan exploit/seize. Mengajukan risk response yang optimal.
i. Belum adanya Penspesifikasian kebutuhan tingkat tinggi untuk proyaek atau program yang akan mengimplementasikan risk response yang terpilih. Mengidentifikasi kebutuhan dan ekspektasi terhadap control yang sesuai untuk respon mitigasi risiko
j. Belum adanya Validasi hasil analisis risiko sebelum digunakan pada pengambilan keputusan, konfirmasi bahwa analisis selaras dengan kebutuhan perusahaan dan verifikasi bahwa estimasi telah terukur dan dipelajari dengan tepat terhadap bias.
k. Belum adanya Penentuan dan persetujuan dimana layanan TI dan sumber daya infrastrktur TI penting untuk mempertahankan pengoprasian proses bisnis. Analisis ketergantungan dan mengidentifikasi link yang lemah.
l. Belum adanya Pengumpulan scenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.
m. Belum adanya Aktifitas secara teratur menangkap semua profil informasi risiko dan mengkonsolidasikan ke dalam agregat profil risiko.
n. Belum adanya Penangkapan informasi pada peristiwa risiko TI yang telah terjadi, untuk dimasukkan ke dalam profil risiko TI perusahaan.
o. Belum adanya Penangkapan informasi mengenai status rencana aksi risiko, untuk dimasukkan ke dalam profil risiko TI perusahaan.
p. Belum adanya Pelaporan profil risiko saat ini ke semua stakeholder, termasuk efektivitas manajemen proses risiko, efektivitas control, gaps, inkonsistensi, redundansi, perbaikan status, dan dampaknya pada profil risiko.
q. Belum adanya Review hasil dari objektif penilaian pihak ketiga, audit internal dan review penjaminan kualitas, dan memetakan ke dalam profil risiko. Review identifikasi gaps dan eksposuruntuk menentukan kebutuhan analisis risiko tambahan.
r. Secara periodic, untuk daerah dengan risiko relative dan kapasitas paritas risiko, identifikasi berkaitan dengan peluang TI yang memungkinkan penerimaan risiko yang lebih besar dan meningkatkan pertumbuhan dan kembali
s. Belum adanya Penentuan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi di dalam setiap individunya dan tingakat toleransi portofolio
t. Belum adanya Pengkategorian insiden dan membandingkannya dengan eksposur yang terjadi terhadap batasan toleransi risiko. Komunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan, dan memperbarui risk profile
u. Belum adanya Penerapan tanggapan yang tepat untuk meminimalisir dampak saat insiden risiko terjadi.

5. Kondisi *Existing* APO12 PA 2.1 dan 2.2
   a. Tidak ada Catatan kinerja proses, yang memberikan rincian hasil.
   b. Belum ada Planning dan monitor performa yang memenuhi tujuan yang diidentifikasi. Ukuran dasar kinerja proses yang terkait dengan tujuan bisnis

ditetapkan dan dipantau. Mereka termasuk tonggak penting, kegiatan yang diperlukan, perkiraan dan jadwal.

c. Belum ada Quality Record, yang memberikan perincian tindakan yang diambil ketika kinerja tidak tercapai.
d. Belum ada Adjust the performance of the process. Tindakan yang diambil ketika kinerja yang direncanakan tidak tercapai. Tindakan termasuk identifikasi masalah kinerja proses dan penyesuaian rencana dan jadwal yang sesuai.
e. Belum ada penentuan tanggung jawab dan wewenang dalam melakukan proses. Tanggung jawab utama dan wewenang untuk melakukan aktivitas utama dari proses didefinisikan, ditugaskan dan dikomunikasikan. Kebutuhan untuk pengalaman kinerja proses, pengetahuan dan keterampilan didefinisikan.
f. Belum ada identifikasi dan sumber daya yang tersedia untuk melakukan proses sesuai dengan rencana. Sumber daya dan informasi yang diperlukan untuk melakukan aktivitas utama dari proses diidentifikasi, disediakan, dialokasikan, dan digunakan.
g. Belum ada Proses Dokumentasi, yang memberikan perincian individu dan kelompok yang terlibat (pemasok, pelanggan, danRACI).
h. Belum ada Rencana proses ,yang memberikan rincian rencana komunikasi proses.
i. Tidak ada pengelola antarmuka antara pihak-pihak yang terlibat. Individu dan kelompok yang terlibat dalam proses diidentifikasi, tanggung jawab ditentukan dan mekanisme komunikasi yang efektif tersedia.
j. Belum ada Perencanaan mutu, yang memberikan rincian produk kerja, kriteria mutu, persyaratan dokumentasi dan pengendalian perubahan.
k. Tidak ada Penetapan persyaratan untuk dokumentasi dan kontrol produk kerja. Ini harus mencakup identifikasi ketergantungan, persetujuan dan ketertelusuran persyaratan
l. Tidak ada Penetapan mutu, harus memberikan rincian produk kerja, kriteria mutu, persyaratan dokumentasi dan pengendalian perubahan.
m. Belum ada identifikasi, dokumentasi dan kontrol produk kerja. Produk kerja tunduk pada kontrol perubahan, pembuatan versi, dan manajemen konfigurasi yang sesuai.
n. Belum ada Catatan mutu, harus memberikan jejak audit atas tinjauan yang dilakukan.
o. Belum ada Tinjauan dan penyesuaian produk kerja, untuk memenuhi persyaratan yang ditentukan. Produk kerja dapat ditinjau terhadap persyaratan sesuai dengan pengaturan yang direncanakan dan setiap masalah yang timbul diselesaikan.

6. Kondisi *Existing* APO12 PA 3.1 dan 3.2
   a. Tidak ada Kebijakan dan standar yang memberikan rincian tujuan organisasi untuk proses, standar kinerja minimum, prosedur standar, dan persyaratan pelaporan dan pemantauan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

b. Belum menentukan proses standar yang akan mendukung penerapan proses yang ditentukan. Proses standar didefinisikan yang mengidentifikasi elemen proses fundamental dan memberikan panduan dan prosedur untuk mendukung implementasi dan panduan tentang bagaimana hal itu dapat disesuaikan bila diperlukan.
c. Belum ada Kebijakan dan standar yang menyediakan pemetaanproses dengan rincian proses standar dan urutan serta interaksi yang diharapkan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
d. Belum ada penentuan urutan dan interaksi antar proses sehingga bekerja sebagai sistem proses yang terintegrasi. Urutan proses standar dan interaksi dengan proses lain ditentukan dan dipertahankan ketika proses diterapkan di berbagai bagian organisasi.
e. Tidak adanya Kebijakan dan standar yang memberikan rincian peran dan kompetensi untuk melakukan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
f. Belum ada identifikasi peran dan kompetensi untuk melakukan proses standar.
g. Belum ada Kebijakan dan standar yang memberikan rincian tujuan organisasi untuk proses, standar kinerja minimum, prosedur standar, dan persyaratan pelaporan dan pemantauan. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
h. Tidak ada Catatan kualitas dan GWP 9.0 Catatan kinerja proses harus memberikan bukti tinjauan yang dilakukan.
i. Belum ada identifikasi peran dan kompetensi untuk melakukan proses standar.
j. Belum ada Kebijakan dan standar yang menentukan standar yang harus diikuti di semua implementasi proses. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
k. Tidak ada penerapan proses yang ditentukan yang memenuhi konteks. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, itu didasarkan pada proses standar, disesuaikan sebagaimana mestinya, dengan kesesuaian dengan persyaratan proses yang ditentukan diverifikasi.
l. Belum ada Kebijakan dan standar harus memberikan perincian, tanggung jawab, dan wewenang untuk melakukan aktivitas proses. Persyaratan bukti pada tingkat ini bukan hanya kebijakan dan standar yang ada, tetapi diterapkan di seluruh organisasi.
m. Tidak ada penentapan dan komunikasi peran, tanggung jawab, dan wewenang untuk melakukan proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, wewenang dan peran untuk melakukan aktivitas proses ditetapkan dan dikomunikasikan.
n. Tidak ada Dokumentasi proses yang memberikan rincian kompetensi dan

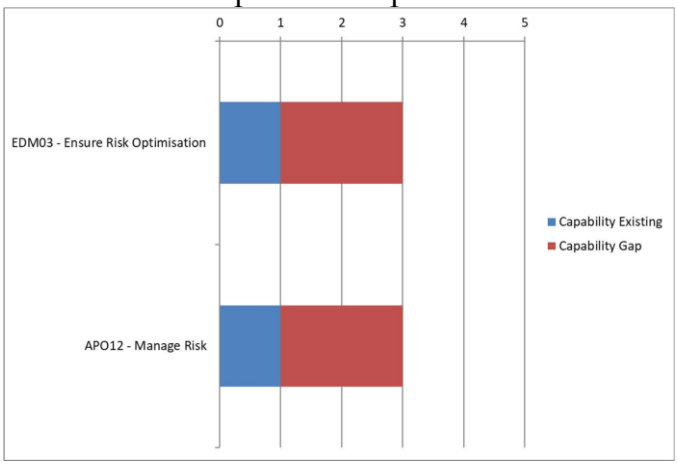
p-ISSN: 2615-7381
e-ISSN: 2621-7279

persyaratan pelatihan.

o. Belum ada Rencana proses yang mencakup perincian rencana komunikasi proses, rencana pelatihan, dan rencana sumber daya untuk setiap contoh proses.
p. Belum ada pemastian kompetensi yang diperlukan untuk melakukan proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, kompetensi yang sesuai untuk personel yang ditugaskan diidentifikasi dan pelatihan yang sesuai tersedia bagi mereka yang menerapkan proses yang ditentukan.
q. Tidak ada Rencana proses yang mencakup perincian rencana sumber daya untuk setiap contoh proses
r. Belum Menyediakan sumber daya dan informasi yang mendukung kinerja proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, sumber daya manusia dan informasi yang diperlukan untuk melakukan proses tersebut tersedia, dialokasikan, dan digunakan
s. Belum ada Rencana proses yang mencakup perincian infrastruktur proses dan lingkungan kerja untuk setiap contoh proses.
t. Belum ada penyediaan infrastruktur proses yang memadai untuk mendukung kinerja proses yang ditentukan. Ketika proses yang sama digunakan dalam area organisasi yang berbeda, dukungan organisasi, infrastruktur, dan lingkungan kerja yang diperlukan tersedia, dialokasikan, dan digunakan.
u. Belum ada Catatan kualitas dan GWP 9.0 Catatan kinerja proses yang memberikan bukti alat tinjauan yang dilakukan untuk setiap contoh proses.
v. Tidak ada pengumupulan dan analisis data tentang kinerja proses untuk menunjukkan kesesuaian dan efektivitasnya. Data yang diperlukan untuk memantau keefektifan dan kesesuaian proses di seluruh organisasi ditentukan, dikumpulkan, dan dianalisis sebagai dasar untuk perbaikan berkelanjutan.

## GAP

Gap adalah selisih dari *Capability Target* dan *Capability Existing*. Hasil capaian dari kedua domain ini dapat dilihat pada *Chart* dibawah




**Gambar 3.** ***Grafik Capability existing*** **dan** ***Capability gap***

Dijelaskan pada Grafik tersebut bahwa untuk level yang dicapai dari kedua domain berada pada level 1, namun sebelumnya *Capability Target*yang ditentukan adalah pada level 3, maka *Capability GAP* dari audit yang dilaksanakan adalah 2 level, yaitu level 2 dan level 3, karena perusahaan belum sanggup mencapai *Capability level* tersebut pada kedua domain.

## PENUTUP

Dengan dilaksanakannya Audit Manajemen Risiko Sistem Informasi pada DIGO.ID, didapatkan hasil kesimpulannya sebagai berikut : (1) Audit manajemen risiko pada perusahaan ini dilakukan dengan beberapa tahapan seperti membuat latar belakangnya, rumusan masalah, Batasan penelitian, tujuan dan manfaat penelitian, lalu dilanjut dengan pengumpulan data dengan beberapa metode, setelah itu baru dilaksanakan audit dan di evaluasi sebagai bentuk hasil berupa Profil Risiko. (2) Profil Risiko manajemen risiko pada perusahaan DIGO.ID setelah dilakukan audit menggunakan *framework* COBIT 5 dan ISO 31000 rupanya manajemen risiko perusahaan masih berada di *Capability Existing* Level 1 baik dari domain APO12 maupun EDM03, Jadi profil risiko perusahaan masih ada dibawah dari target yang ditetapkan.

Saran dan Rekomendasi yang didapat setelah dilakukannya audit manajemen risiko ini ada beberapa rekomendasi berupa hal apa saja yang perlu dipenuhi dan dijalani untuk mencapai *Capability Target,* untuk saran yang diberikan berupa *Capability Exsiting* pada perusahaan agarbisa terlihat apa saja yang belum terjalani, apa yang belum terpenuhi, dan apa yang belum tercapai. Berikut adalah sebagian Rekomendasi untuk manajemen risiko website DIGO.ID : (1) Melakukan Penegasan pada pembuatan Kebijakan manajemen risiko. (2) Berfokus menyempurnakan level 1 karena masih memiliki presentase yang rendah pada kedua domain. (3) Pengelolaan profil risiko dalam penanggapan dan perlakuan dalamtindakan terkait risiko yang ada. (4) Mengembangkan informasi berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis faktor risiko. (5) Menyediakan Sumber daya dan informasi yang diperlukan untukmelakukan proses diidentifikasi, disediakan, dialokasikan, dan digunakan.

## DAFTAR PUSTAKA

[1] O'Brien, J. A., & Marakas, G. M. (2018). Management Information Systems. New York, NY: McGraw-Hill Education.
[2] ISACA. (2012). COBIT 5 Framework: Introduction and Methodology.
[3] Kuswara, H., & Kusmana, D. (2017). Sistem Informasi Absensi Siswa Berbasis Web Dengan SMS Gateway Pada Sekolah Menengah Kejuruan Al – Munir Bekasi. Indonesian Journal on Networking and Security, 6(2), 17–22.
[4] Mirnasari, P. D., & Suardhika, I. M. S. (2018). Pengaruh Penggunaan Teknologi Informasi, Efektivitas Sistem Informasi Akuntansi, Dan Sistem Pengendalian Intern Terhadap Kinerja Karyawan. E-Jurnal Akuntansi, 23(1), 567–594.
[5] Messier Jr., W. F., Glover, & Prawitt, D. F. (2020). *Auditing & assuranceservices: A systematic approach (11th ed.). McGraw-Hill Education*.
[6] Jaya, I. B. K. A. (2018). Audit Manajemen Risiko Teknologi Informasi pada

Perguruan Tinggi Menggunakan Kerangka Kerja COBIT 5 (Doctoral dissertation, Institut Teknologi Sepuluh Nopember).

[7] Weber, Ron. (2012) . Information System Control and Audit. Prentice-Hall, Inc: New Jersey.

[8] Soelistya, I. D., & MM, C. (2021). Buku Ajar: Manajemen Sumber Daya Manusia (MSDM) Strategy. Nizamia *Learning Center*.

[9] Hasibuan, M.S.P. (2016). Manajemen Sumber Daya Manusia. Edisi Revisi. Jakarta: Penerbit PT Bumi Aksara..

[10] ISO. (2018). ISO 31000:2018 Risk management – Guidelines. Geneva, Switzerland: International Organization for Standardization.

[11] COSO (2017). Enterprise Risk Management – Integrating with Strategy and Performance. The Committee of Sponsoring Organizations of the Treadway Commission.

[12] Institute of Risk Management. (2021). Fundamentals of risk management. Institute of Risk Management.

[13] Hutahaean, J. (2014). Konsep Sistem Informasi. Yogyakarta: Deepublish.

[14] Fathansyah. (2018). Basis Data. Bandung: Penerbit Informatika Bandung.

[15] Kadir, A. (2014). Pengenalan Sistem Informasi. Edisi Revisi. Yogyakarta: Andi.

[16] Trimahardika, R., & Sutinah, E. (2017). Penggunaan Metode Rapid Application Development Dalam Perancangan Sistem Informasi Perpustakaan. JURNAL INFORMATIKA, 4(2), 249-260.

[17] Tukino. (2020). Rancang Bangun Sistem Informasi E-Marketing Pada Pt Pulau Cahaya Terang. Computer Based Information System Journal, 08(01), 25–33.

[18] Lumbangaol, H. M. (2020). Rancang Bangun Sistem Informasi Penjualan dan Penyewaan Properti Berbasis WEB Di Kota Batam. Jurnal Comasie, 01(03), 83–92.

[19] ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA.

[20] Aprianto, K., Endroyono, E., & Nugroho, S. M. S. (2021). AnalisisManajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000: 2018 di Kabupaten Magetan (E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000: 2018 in Magetan Regency). JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi), 23(2), 107-122.

[21] Putri, R. E. (2015, December). Model Penilaian Kapabilitas Proses Optimasi Resiko Ti Berdasarkan Cobit 5. In Seminar Nasional Informatika (SEMNASIF) (Vol. 1, No. 1).