Jurnal Informasi dan Teknologi

https://jidt.org/jidt

2023 Vol. 5 No. 2 Hal: 30-38 e-ISSN: 2714-9730

Analisis Manajemen Risiko IT Menggunakan COBIT 5 Pada Domain APO12

Rievaldy Ardhyka[1]✉, Afifah Fidaiyah[2], Ruci Meiyanti[3]

[1,2,3] Universitas Mercu Buana

riealdy10@gmail.com

Abstrak

Terdapat risiko saat penggunaan TI yang dapat mengakibatkan proses bisnis menjadi kurang optimal. Hal ini menyebabkan kerugian finansial dan berbagai kejadian lain yang dapat merugikan perusahaan, tidak terkecuali PT. XYZ. Untuk mengatasi hal tersebut, setiap organisasi atau perusahaan harus memiliki manajemen risiko di bidangnya. Manajemen risiko yang tepat dalam teknologi informasi diperlukan untuk mengurangi risiko seperti adanya kendala pada aplikasi atau infrastruktur, penyalahgunaan akses aplikasi, data, dan infrastruktur, kehilangan atau rusaknya data dan informasi, serta yang lainnya. Berdasarkan masalah tersebut, penelitian ini melakukan analisis manajemen risiko TI di PT. XYZ menggunakan *framework* COBIT 5 menggunakan domain APO (*Align, Plan, Organize*)12. Hasilnya menunjukkan risiko yang mungkin berbahaya serta menawarkan penyelesaian akan mengurangi kemungkinan kerugian. Selain itu, hasil evaluasi tingkat kemampuan manajemen TI proses APO12 menunjukkan bahwa kondisi saat ini (*As Is*) dalam manajemen risiko berada di level 4 (*Predictable Process*). Sementara itu, tingkat kemampuan kondisi yang diharapkan (*To Be*) dalam mengelola risiko TI adalah pada level 5 (*Optimizing Process*).

Kata Kunci: Manajemen Risiko, COBIT 5, APO12, Tingkat Kapabilitas.

1. Pendahuluan

Saat ini perkembangan teknologi informasi sudah sangat pesat. Teknologi informasi merupakan teknologi digunakan untuk mengolah data, meliputi pengolahan, akuisisi, mengumpulkan, menyimpan, dan mengolah data menghasilkan dengan berbagai cara informasi berharga, yaitu informasi relevan, akurat dan tepat waktu, yaitu untuk pribadi, kehidupan bisnis, organisasi dan pemerintah. Kemajuan teknologi informasi dan telekomunikasi begitu pesat, sehingga memungkinkan diterapkannya cara-cara baru yang lebih efisien untuk produksi, distribusi dan konsumsi barang dan jasa [1]. Dampak dan peran TI dalam kehidupan manusia sangat banyak, salah satunya dimanfaatkan oleh perusahaan atau organisasi untuk menopang sistem perusahaan dengan menggunakan teknologi informasi. Karena teknologi informasi memiliki peranan penting bagi sebuah organisasi dikarenakan peranan strategis itu mampu untuk meningkatkan kualitas pelayanan dan memberi dukungan pada proses bisnis dalam mencapai tujuan organisasi. Namun dibalik banyaknya dampak baik yang dihasilkan oleh teknologi informasi, pasti akan ada risiko-risiko yang muncul. Risiko akan selalu menghadang setiap manusia maupun berbagai perusahaan, termasuk perusahaan bisnis. Mengingat adanya ketidakpastian mengenai terjadinya risiko, individu maupun institusi, maka mereka harus berusaha menetapkan langkah-langkah antisipatif untuk menghadapi risiko itu, guna mengurangi, meniadakan, atas masalah yang dapat meraup keuntungan dari terjadinya suatu risiko. Karena itu, setiap manusia diharapkan menjadi manajer risiko [2]. Khususnya risiko teknologi informasi yang akan mengakibatkan kerugian bagi organisasi. Maka dari itu untuk meminimalisir risiko perlu adanya manajemen risiko, manajemen risiko adalah sistem dimana organisasi dikelola, diarahkan dan dikendalikan (*lead, direct, direct*) untuk meningkatkan efisiensi organisasi untuk kepentingan pemegang saham, pemangku kepentingan dan pertumbuhan ekonomi. Peningkatan kinerja ini terjadi dalam kerangka hukum dan standar etika yang berlaku [3]. Manajemen risiko diterapkan untuk mengidentifikasi dan mengendalikan risiko serta kemungkinan peristiwa, untuk Untuk menurunkan efek dan menentukan manajemen risiko yang tepat, maka dapat meningkatkan peluang keberhasilan.

Fungsi krusial IT pula digunakan PT. XYZ dalam menjalankan mekanisme bisnisnya. Bila dalam pemanfaatan yang terkait dengan Teknologi Informasi mekanisme bisnis yang memperoleh gangguan bakal memicu risiko dalam menjalankan mekanisme bisnis PT. XYZ mampu menahan mekanisme bisnis yang sedang berlangsung. Oleh karenanya, dibutuhkan Analisis Manajemen Risiko Teknologi Informasi demi menurunkan, menghindari, serta mengelola risiko TI. Analisis manajemen risiko TI mampu dicapai melalui penerapan kerangka kerja COBIT

Diterima: 10-06-23 | Revisi: 11-06-23 | Diterbitkan: 13-06-23 | doi: 10.37034/jidt.v5i1.325

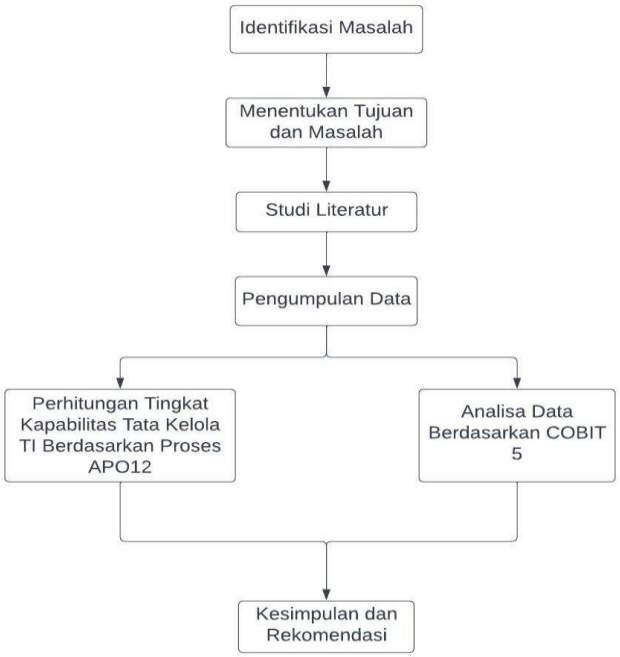
5. Analisis manajemen risiko diaplikasikan dalam penelitian ini merupakan domain TI COBIT 5 yaitu APO (Align, Plan, and Organize)12. APO12 sanggup diterapkan untuk menerapkan manajemen risiko teknologi informasi PT. XYZ dengan enam subdomain yang berkontribusi pada manajemen risiko yang terkait dengan teknologi informasi. Dalam penelitian ini, analisis proses dilakukan menggunakan domain APO12, yaitu proses untuk menemukan, menilai, dan mengelola risiko TI akan memungkinkan untuk mengidentifikasi tindakan terhadap risiko TI dengan cepat dan tepat untuk menghindari akibat mempertaruhkan. Kemudian dengan pengelolaan risiko yang tepat, PT. XYZ yang akan datang dapat menggunakan temuan penelitian sebagai pedoman untuk melakukan pengelolaan risiko. Selain itu, terdapat saran tentang cara mengatasi risiko yang dihasilkan oleh analisis ini.

Penelitian tentang penggunaan Cobit 5 untuk analisis manajemen risiko IT [4], tujuan penelitian ini adalah untuk menentukan ancaman TI saat ini di PT Global Infotech Solutions dan untuk mengetahui seberapa efektif COBIT 5 digunakan oleh perusahaan untuk mengelola dan meminimalkan risiko TI. Hasil menunjukkan bahwa perusahaan memiliki tingkat kapabilitas level 1 sebagai akibat dari kurangnya kontrol risiko TI dan kurangnya dokumentasi khusus tentang situasi TI yang tepat. Penelitian sebelumnya melakukan penilaian tingkat kapabilitas dengan proses APO12 [5], dalam penelitian ini dilakukan untuk mengetahui *Capability level* dengan domain APO12 (*Align, Plan, Organize*) dalam manajemen risiko. Selain itu, ada beberapa rekomendasi risiko, seperti bahwa SOP harus ada untuk perawatan komputer dan sistem untuk mengoptimalkan pengoperasian TI. Selain itu, dokumen yang jelas harus dimiliki oleh yayasan untuk identifikasi risiko dan evaluasi manajemen risiko untuk memastikan bahwa yayasan dapat menangani masalah risiko dengan baik.

Penelitian serupa yang mengenai proses tingkat kapabilitas [6], penelitian ini dilakukan untuk mengetahui proses *capability level* TSI, serta pengendalian risiko seperti peninjauan proses komunikasi risiko agar tidak tertunda untuk menangani risiko, menambahkan kriteria efektivitas pengendalian risiko untuk mengetahui seberapa baik pengendalian risiko bekerja untuk mengurangi tingkat risiko. Penelitian ini bertujuan untuk mengetahui ancaman risiko IT yang berpotensi berbahaya dan memberikan saran untuk mengurangi risiko kerugian dengan penggunaan COBIT 5 khususnya domain APO12 di PT. XYZ. Serta juga melakukan analisis tingkat kapabilitas untuk mengetahui tingkat kematangan tata kelola TI proses APO12 kondisi saat ini (*As Is*) dan kondisi yang diharapkan (*To Be*).

2. Metode Penelitian

Metode penelitian merupakan gambaran dari proses penelitian yang dilakukan seperti perencanaan, pengumpulan dan pengolahan data. Tahapan ini akan menjelaskan beberapa tahapan untuk menyelesaikan permasalahan yang ada. Metode penelitain yang digunakan yaitu menggunakan metode kualitatif, yaitu termasuk memahami data tentang fenomena risiko TI sebelum peneliti terjun ke lapangan untuk mengumpulkan informasi. Informasi yang didapatkan melalui metode observasi dan wawancara. Alur penelitian ini dapat diperhatikan pada Gambar 1.



Gambar 1. Alur Metode Penelitian

2.1. Identifikasi Masalah.

Identifikasi merupakan langkah awal yang dilakukan untuk melihat apakah ada masalah atau kejadian yang dapat diselidiki dan diteliti. Dalam penelitian ini, masalah analisis manajemen risiko TI di perusahaan.

2.2. Menentukan Tujuan dan Masalah.

Pada tahapan ini, masalah serta tujuan atau sasaran penelitian ditentukan dari permasalahan yang ada di dalam perusahaan. Masalah yang diangkat dalam penelitian ini mengenai apa saja risiko-risiko TI yang muncul pada perusahaan dan mempunyai tujuan untuk menggambarkan risiko dan saran untuk mengurangi kemungkinan kerugian. Serta mengetahui tingkat kapabilitas tata kelola TI proses APO12 kondisi saat ini (*As Is*) dan kondisi yang diharapkan (*To Be*) dalam mengelola risiko TI.

2.3. Studi Literatur.

Pada tahap ini, melakukan pencarian literatur jurnal atau materi tentang COBIT 5 dan manajemen risiko TI untuk menemukan referensi tentang masalah yang terjadi serta menjadi acuan pada penelitian ini.

2.4. Pengumpulan Data.

Metode yang digunakan untuk mengumpulkan data primer dan sekunder, penelitian ini dilakukan melalui wawancara dengan pihak berwenang dan pengawasan proses teknologi informasi di PT. XYZ.

2.5. Perhitungan Tingkat Kapabilitas.

Perhitungan tingkat kapabilitas Tata Kelola Teknologi Informasi berlandaskan mekanisme APO12 pada COBIT 5.

2.6. Analisis Data Berdasarkan COBIT 5.

Hasil risiko IT menentukan analisis data yang ditemukan dalam panduan COBIT 5, dengan menggunakan domain APO12 yang dikenal sebagai Manajemen Risiko, dengan enam subdomain. Pada APO12 ialah APO12.01 hingga APO12.06. untuk mengetahui ancaman risiko IT yang berpotensi berbahaya dan memberikan saran untuk mengurangi risiko kerugian dengan penggunaan COBIT 5 khususnya domain APO12.

3. Hasil dan Pembahasan

Proses yang dihasilkan dari analisis manajemen risiko TI di PT. XYZ, yang menggunakan langkah-langkah proses domain APO12 yang telah disebutkan sebelumnya, dan hasilnya termasuk dalam tahap hasil dan tingkat kapabilitas tata kelola TI proses domain APO12. Hasil penelitian tentang manajemen risiko TI di domain APO12 di *framework* COBIT 5 dan tingkat kapabilitas tata kelola TI proses domain APO12 tepatnya, sebagai berikut:

3.1. APO12.01 *Collect Data (Mengumpulkan Data)*

Proses mengumpulkan data ini diantaranya menemui dan mengkompilasi data informasi tentang kejadian risiko yang telah terjadi mewakili dan dapat mewakili risiko untuk Teknologi Informasi. Kompilasi data informasi risiko terkait teknologi informasi berhubungan dengan masalah, kejadian saat ini, dan wawancara tentang masalah IT. Hasilnya menunjukkan ancaman risiko TI sebagai berikut:

1. Ketidaksesuaian pemilihan atau penerapan teknologi (biaya, kinerja, fitur, kompatibilitas) dengan kebutuhan bisnis dan tujuan strategis Perusahaan.
2. Eksploitasi kerentanan keamanan informasi dalam hal aplikasi, infrastruktur, dan manusia melalui serangan *Cyber* (*Malware, DDOS attack, deface attack*, dll.) dan melalui serangan rekayasa sosial.
3. Kegagalan untuk mencapai *SLA* (*Service Level Agreement*) layanan seperti layanan aplikasi, konektivitas, e-mail, atau ERP yang mengganggu operasi bisnis Perusahaan.
4. Pemasok tidak dapat mencapai target *Service Level Agreement* (*SLA*).
5. Kehilangan atau kerusakan data dan informasi.
6. Penyalahgunaan akses ke aplikasi, data, dan infrastruktur.
7. Ada bugs di aplikasi atau infrastruktur.
8. Kegagalan pemrosesan pembayaran atas transaksi penjualan.
9. Kehilangan data di *File Server* lokal karena penghapusan yang tidak disengaja oleh pengguna atau paparan *malware/ransomware*.

3.2. APO12.02 *Analyze Risk (Menganalisis Risiko)*

Menyajikan pandangan atau diinformasikan akurat dapat meningkatkan relevansi dan aktualitas risiko TI. Analisis risiko akan mempertimbangkan semua faktor risiko dengan meninjau efek risiko dan peluang risiko. Berdasarkan tahapan ini, tingkat risiko diukur berdasarkan efek risiko dan peluang risiko. Nilai dampak risiko dikategorikan menjadi ringan, sedang, dan berat, sementara itu nilai peluang risiko dikategorikan menjadi kecil, sedang, dan tinggi. Memahami dan menilai hasil dari kedua faktor ini, Anda dapat menentukan hasil *input* untuk evaluasi risiko.

Table 1. Tabel Analisis Resiko yang Ditemukan

Risiko	Pengendalian	Peluang	Dampak
Ketidaksesuaian pemilihan atau penerapan teknologi.	Membuat perancangan Penyelesaian Proyek - Strategi Transformasi Digital.	Sedang	Berat
Kerentanan keamanan informasi melalui serangan *Cyber* dalam hal aplikasi, infrastruktur, dan manusia.	Mempunyai personal keamanan yang kuat.	Tinggi	Berat
Kegagalan untuk mencapai *SLA* layanan.	Melakukan *training*/sertifikasi/seminar/*benchmark* untuk pegawai secara berkala.	Tinggi	Berat
Pemasok tidak dapat mencapai target *Service Level Agreement* (*SLA*).	Memastikan proses evaluasi supplier berjalan secara objektif sehingga terpilih supplier (perusahaan dan tenaga kerja) yang berkualitas.	Sedang	Ringan
Kehilangan atau kerusakan data dan informasi.	Melakukan backup rutin agar dapat dipulihkan.	Kecil	Berat
Penyalahgunaan akses ke aplikasi, data, dan infrastruktur.	Memperjelas wewenang mengenai tanggung jawab terhadap akses ke aplikasi, data, dan infrastruktur.	Sedang	Berat
Ada *bugs* di aplikasi atau infrastruktur.	Memberikan pemberitahuan untuk mengupdate aplikasi atau infrastruktur.	Tinggi	Berat
Kegagalan pemrosesan pembayaran atas transaksi penjualan.	Memantau kinerja penyedia jaringan secara teratur.	Sedang	Sedang

Risiko	Pengendalian	Peluang	Dampak
Kehilangan data di *File Server* lokal karena penghapusan yang tidak disengaja oleh pengguna atau paparan *malware/ransomware*.	Melakukan *backup* rutin untuk memungkinkan pemulihan.	Kecil	Berat

3.3. APO12.03 *Maintain A Risk Profile* (Memelihara Profil Risiko)

Menjaga inventarisasi risiko yang diketahui serta atribut risiko, termasuk frekuensi yang diantisipasi, dampak yang mungkin, dan respons, serta sumber daya, kemampuan, dan tindakan yang terkait dengan pengendalian kegiatan yang sedang dilakukan:

1. Mencatat aplikasi, infrastruktur, personel pendukung, fasilitas, vendor, pemasok, dan *outsourcing*, serta dokumen yang bergantung pada prosedur yang digunakan untuk mengelola sumber daya infrastruktur TI dan layanan.
2. Mendefinisikan sumber daya infrastruktur TI dan layanan penting untuk menjaga dan memelihara operasi proses bisnis.
3. Menganalisis dependensi dan menemukan hubungan yang tidak kuat.
4. Setiap profil risiko secara teratur dikumpulkan dan digabungkan ke dalam profil risiko gabungan.

Table 2. Tabel Hasil Tahap Pemeliharaan Profil Risiko

Risiko	Tingkat Risiko
Ketidaksesuaian pemilihan atau penerapan teknologi.	Tinggi
Kerentanan keamanan informasi melalui serangan *Cyber* dalam hal aplikasi, infrastruktur, dan manusia.	Tinggi
Kegagalan untuk mencapai *SLA* layanan.	Tinggi
Pemasok tidak dapat mencapai target *Service Level Agreement* (*SLA*).	Sedang
Kehilangan atau kerusakan data dan informasi.	Kecil
Penyalahgunaan akses ke aplikasi, data, dan infrastruktur.	Sedang
Ada *bugs* di aplikasi atau infrastruktur.	Tinggi
Kegagalan pemrosesan pembayaran atas transaksi penjualan.	Sedang
Kehilangan data di *File Server* lokal karena penghapusan yang tidak disengaja oleh pengguna atau paparan *malware/ransomware*.	Kecil

3.4. APO12.04 *Articulate Risk* (Mengkomunikasin Risiko)

Memberi tahu semua pemangku kepentingan dengan cepat tentang keadaan TI saat ini. Salah satu pekerjaan yang telah diselesaikan adalah:

1. Melaporkan seluruh pemangku kepentingan yang terpengaruh tentang hasil analisis risiko dalam format dan bentuk yang berguna untuk membantu keputusan bisnis. Laporan ini harus mencakup kemungkinan dan jumlah keuntungan atau kerugian, serta tingkat kepercayaan yang memungkinkan pengembalian mempertaruhkan diimbangi oleh manajemen.
2. Membuat ketetapan berdasarkan pemahaman yang baik tentang situasi terburuk serta kemungkinan terburuk, serta melakukan pemeriksaan dan pertimbangan menyeluruh terhadap hukum, peraturan, dan reputasi.
3. Melaporkan pemangku kepentingan tentang profil risiko terbaru, yang mencakup informasi tentang bagaimana mekanisme manajemen risiko, kontrol, perbedaan, ketidaksesuaian, redudansi, kemajuan, dan pengaruh profil risiko.

Table 3. Tabel Artikulasi Risiko

Risiko	Peluang	Rekomendasi
Ketidaksesuaian pemilihan atau penerapan teknologi.	Tinggi	Melakukan studi atau analisis kelayakan sebelum mengajukan/melaksanakan inisiatif atau program kerja.
Kerentanan keamanan informasi melalui serangan *Cyber* dalam hal aplikasi, infrastruktur, dan manusia.	Tinggi	Sosialisasi kepada pengguna layanan untuk meningkatkan *awareness* terkait keamanan informasi. Pemenuhan personel terutama yang terkait *Security*. Mengikuti *training*/sertifikasi/seminar/*benchm*ark untuk personel secara berkala. *Managed Security Service*s untuk *Security Operation Center*.
Kegagalan untuk mencapai *SLA* layanan.	Tinggi	Monitoring pro aktif secara berkala menggunakan monitoring tools. Mengikuti *training*/sertifikasi/seminar/*benchm*ark untuk personel secara berkala. Melakukan proses *backup* dan pengujian *restore* secara berkala. Pemeriksaan internal terkait konfigurasi sesuai dengan standar atau *best practice*.
Pemasok tidak dapat mencapai target *Service Level Agreement* (*SLA*).	Sedang	Memastikan proses evaluasi supplier berjalan secara objektif sehingga terpilih supplier (perusahaan dan tenaga kerja) yang berkualitas. Pastikan bahwa dalam Kontrak pemasok menjamin SLA-nya di atas SLA. Menggunakan minimal 2 (dua) pemasok untuk layanan konektivitas kritis.
Kehilangan atau kerusakan data dan informasi.	Kecil	Melakukan *maintenance* secara berkala. Rutin melakukan *backup* data data agar dapat di *restore*
Penyalahgunaan akses ke aplikasi, data, dan infrastruktur.	Sedang	Verifikasi hak akses ke aplikasi dan pengguna kunci pengguna data. Perbarui matriks akses pengguna secara teratur. Memastikan penerapan standar yang terkait dengan keamanan kata sandi (kompleksitas, kedaluwarsa). Menjangkau pengguna layanan untuk meningkatkan kesadaran terkait keamanan akun dan kata sandi.
Ada *bugs* di aplikasi atau infrastruktur.	Tinggi	Pastikan skenario pengujian aplikasi mencakup semua kasus penggunaan. Memastikan bahwa patch kritis/keamanan yang berlaku pembaruan diterapkan secara teratur.
Kegagalan pemrosesan pembayaran atas transaksi penjualan.	Sedang	Pemantauan kinerja penyedia payment gateway secara berkala. Memantau kinerja penyedia jaringan secara teratur. Memastikan proses manajemen perubahan berjalan dengan baik.

Risiko	Peluang	Rekomendasi
Kehilangan data di *File Server* lokal karena penghapusan yang tidak disengaja oleh pengguna atau paparan *malware/ransomware.*	Kecil	Menggunakan penyimpanan awan atau *Cloud File Server*. Rutin melakukan *backup* data data agar dapat di *restore*

3.5 APO12.05 Mendefinisikan Portfolio Tindakan Manajemen Risiko

Pastikan bahwa langkah-langkah yang diambil untuk menciptakan peluang dan strategi mengurangi risiko portofolio ke tingkat yang dapat diterima untuk dikelola. Salah satu pekerjaan yang telah diselesaikan adalah:

1. Menjaga inventarisasi aktivitas pengendalian yang ada untuk mengelola risiko dan membiarkan risiko diambil sesuai dengan toleransi mempertaruhkan. Mengkategorikan tindakan pengendalian dan mengacu pada laporan risiko TI spesifik dan agregasi risiko TI.
2. Tentukan apakah setiap bagian dari perusahaan memantau risiko dan menerima tanggung jawab untuk beroperasi sesuai dengan toleransi dan portofolio setiap orang.
3. Tentukan serangkaian proposal proyek yang seimbang yang dimaksudkan untuk mengurangi risiko proyek dan memungkinkan perusahaan strategis, pertimbangkan *cost/benefit*, efek pada profil risiko terkini, serta regulasi.

Jenis-jenis cara mengelola atau menangani risiko adalah:

1. Menghindari Risiko (*Risk Avoidance*)
2. Pembagian Risiko atau Memecah Risiko (*Risk Sharing/Risk Transfer*)
3. Mitigasi Risiko (*Mitigation*)
4. Menerima Risiko (*Risk Acceptance*)

Table 4. Tabel Tindakan Terhadap Risiko

Risiko	Pengendalian	Peluang	Tindakan
Ketidaksesuaian pemilihan atau penerapan teknologi.	Membuat perancangan Penyelesaian Proyek - Strategi Transformasi Digital.	Sedang	Mitigasi
Kerentanan keamanan informasi melalui serangan *Cyber* dalam hal aplikasi, infrastruktur, dan manusia.	Mempunyai personal keamanan yang kuat.	Tinggi	Mitigasi
Kegagalan untuk mencapai *SLA* layanan.	Melakukan *training*/sertifikasi/seminar/*benchmark* untuk pegawai secara berkala.	Tinggi	Mitigasi
Pemasok tidak dapat mencapai target *Service Level Agreement* (*SLA*).	Memastikan proses evaluasi supplier berjalan secara objektif sehingga terpilih supplier (perusahaan dan tenaga kerja) yang berkualitas.	Sedang	Menghindari
Kehilangan atau kerusakan data dan informasi.	Melakukan *backup* rutin agar dapat dipulihkan.	Kecil	Menghindari
Penyalahgunaan akses ke aplikasi, data, dan infrastruktur.	Memperjelas wewenang mengenai tanggung jawab terhadap akses ke aplikasi, data, dan infrastruktur.	Sedang	Mitigasi
Ada *bugs* di aplikasi atau infrastruktur.	Memberikan pemberitahuan untuk mengupdate aplikasi atau infrastruktur.	Tinggi	Mitigasi
Kegagalan pemrosesan pembayaran atas transaksi penjualan.	Memantau kinerja penyedia jaringan secara teratur.	Sedang	Menghindari
Kehilangan data di *File Server* lokal karena	Melakukan *backup* rutin agar dapat dipulihkan.	Kecil	Menghidari

Risiko	Pengendalian	Peluang	Tindakan
penghapusan yang tidak disengaja oleh pengguna atau paparan *malware/ransomware*.			

3.6. APO12.06 Menanggapi Risiko

Menanggapi risiko secara cepat dan efektif untuk mengurangi kerugian akibat kejadian TI. Proses ini dapat dianggap sebagai langkah untuk mengurangi risiko, dan tindakan terkait dengannya juga dapat dilakukan untuk mengurangi risiko. Hasil penilaian risiko ini menghasilkan profil risiko yang terdiri dari berbagai saran yang dapat digunakan untuk memitigasi risiko untuk kebutuhan sistem informasi. Kegiatan yang dilakukan adalah sebagai berikut:

1. Laporkan kategori insiden dan kerugian terkait TI dengan batas toleransi risiko ke pemangku kepentingan dan sebagai update profil risiko.
2. Tentukan dampak risiko serta identifikasi sumber risiko.
3. Mengkomunikasikan tentang sumber risiko, perbaikan proses, dan kebutuhan untuk tindakan terhadap risiko tambahan, dan rencana tindakan yang tepat untuk mengurangi efek risiko.
4. Mengkategorikan insiden, membandingkan eksposur aktual dengan ambang batas toleransi risiko, melaporkan dampak bisnis kepada pengambil keputusan, dan memperbarui profil risiko.

3.7. Tingkat Kapabilitas

Pada penelitian ini juga menghitung tingkat kapabilitas Tata Kelola TI berdasarkan proses APO12 pada COBIT 5. Tingkat kapabilitas digunakan sebagai dasar untuk mengukur implementasi Tata kelola TI (*As Is*) dan kondisi yang akan datang (*To Be*) untuk menunjukkan pencapaian kinerja TI di PT. XYZ. Tingkat keseluruhan penilaian ini dibagi menjadi enam tingkat berdasarkan deskripsi tingkat dalam kapabilitas proses yaitu:

1. Level 0 *Incomplete Process* (Prosesnya tidak diimplementasikan atau gagal mencapai proses yang telah ditargetkan).
2. Level 1 *Performed Process* (Proses yang diimplementasikan mencapai tujuan prosesnya).
3. Level 2 *Managed Process* (Proses yang dilakukan sebelumnya dijelaskan sekarang diimplementasikan dengan cara yang dikelola sesuar dengan target).
4. Level 3 *Established Process* (Proses terkelola kemudian sekarang dilakukan dengan proses yang telah ditentukan, yang berarti mampu mencapai hasil prosesnya).
5. Level 4 *Predictable Process* (Proses beroperasi di dalam batas yang ditentukan untuk mencapai hasil prosesnya).
6. Level 5 *Optimizing Process* (Memenuhi tujuan bisnis saat ini dan yang diproyeksikan yang relevan).

Penilaian atribut tingkat kapabilitas menggunakan skala penilaian sebagai berikut:

1. F (*Fully*/ Tercapai Sepenuhnya)
   Tingkat kemampuan yang dicapai adalah 85% atau lebih tinggi. Dalam pemeringkatan ini, pencapaian penuh atas atribut proses tidak ada kelemahan.
2. L (*Largely*/ Secara Garis Besar Tercapai)
   Tingkat kemampuan yang dicapai antara 50% sampai dengan 85%. Pada pemeringkatan ini, merupakan capaian yang signifikan terhadap proses tersebut, walaupun masih memungkinkan terjadinya suatu kelemahan.
3. P (*Partially*/ Tercapai Sebagian)
   Tingkat kemampuan yang dicapai antara 15% sampai dengan 50%. Pada pemeringkatan ini terdapat beberapa pencapaian atribut dalam proses.
4. N (*Not*/ Tidak Tercapai)
   Tingkat kemampuan yang dicapai kurang dari 15%. Pada pemeringkatan ini tidak ada atribut yang dicapai selama proses.

Dalam penelitian ini digunakan kerangka kerja tingkat kapabilitas untuk mengukur implementasi Tata kelola TI kondisi saat ini (*As Is*) dan kondisi yang akan datang (*To Be*) untuk menunjukkan pencapaian kinerja TI di PT. XYZ. Berikut ini adalah nilai rata-rata dari domain APO12 yaitu dari APO12.01 - APO12.06 yang telah dicapai oleh PT. XYZ.

Table 5. Tabel Hasil Kapabilitas

No	Sub-Domain	Nilai Kapabilitas		*Capability Level*	
		As Is	*To Be*	*As Is*	*To Be*
1	APO12.01	4	5	4	5
2	APO12.02	4	5	4	5
3	APO12.03	4	5	4	5
4	APO12.04	4	5	4	5
5	APO12.05	4	5	4	5
6	APO12.06	4	5	4	5
Rata-Rata		4	5	4	5

Sumber: Data Olahan

Berdasarkan hasil tabel diatas menjelaskan bahwa proses APO12 memiliki nilai kapabilitas saat ini (*As Is*) adalah 4, sehingga capability level berada pada level 4, yaitu Predictable Process. Dapat diartikan bahwa proses yang dapat diprediksi, proses ini merupakan proses yang dijalankan dalam batasan yang ditentukan untuk mencapai hasil akhir yang diharapkan. Sedangkan nilai kapabilitas kondisi yang diinginkan (*To Be*) dari proses APO12 adalah 5, yang berarti PT. XYZ mengharapkan dimasa yang akan datang capability level berada pada level 5, yaitu Optimizing Process. Dapat diartikan bahwa Proses yang telah diprediksi dan dijelaskan sebelumnya terus diperbaiki yang berguna untuk memenuhi tujuan bisnis yang relevan saat ini.

4. Kesimpulan

Berdasarkan penelitian yang membahas analisis manajemen risiko TI di PT. XYZ dengan menggunakan langkah-langkah analisis manajemen risiko domain Cobit 5, yaitu APO12 dan penilaian tingkat kematangan prosedur manajemen teknologi informasi APO12, dapat disimpulkan bahwa:

1. Hasil analisis didapatkan bahwa 4 ancaman risiko TI masuk kedalam level *high* berupa ketidaksesuaian pemilihan atau penerapan teknologi, kerentanan keamanan informasi melalui serangan Cyber dalam hal aplikasi, infrastruktur, dan manusia, kegagalan untuk mencapai SLA layanan, dan ada *bugs* di aplikasi atau infrastruktur.
2. Hasil perhitungan tingkat kapabilitas proses APO12 (*Manage Risk*) didapatkan bahwa tingkat kapabilitas kondisi saat ini (*As Is*) PT. XYZ dalam mengelola risiko berada di level 4 (*Predictable Process*) dengan nilai 4. Sedangkan tingkat kemampuan kondisi yang diharapkan (*To Be*) dalam mengelola risiko TI adalah pada level 5 (*Optimizing Process*) dengan nilai 5.
3. Hasil analisis manajemen risiko TI dengan domain Cobit 5 yaitu APO12 ditemukan bahwa 6 ancaman risiko TI masuk kedalam level *high* sehingga perlu dilakukan tindakan rekomendasi yang dapat dilihat pada Tabel 3 Artikulasi Risiko. Oleh karena itu PT. XYZ harus bisa segera melakukannya pelaksanaan rekomendasi atas temuan risiko telah disebut sebagai reaksi untuk mengurangi atau menghilangkan risiko serta sebagai cara untuk meningkatkan risiko yang bermanfaat untuk meningkatkan kemampuan pemahaman dan evaluasi hasil yang lebih dalam tentang risiko untuk mengidentifikasi hasil *input* evaluasi risiko.

Daftar Rujukan

[1] W. Wardiana, “Perkembangan Teknologi Informasi di Indonesia”.

[2] L. P. Indra Siswanti, Conie Nopinda Br Sitepu, Novita Butarbutar, Edwin Basmar, Rahmita Saleh, Sudirman Sudirman, Mahyuddin Mahyuddin, Luthfi Parinduri, *Manajemen Risiko Perusahaan*. Yayasan Kita Menulis, 2020.

[3] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000,” *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[4] P. P. Thenu, A. F. Wijaya, and C. Rudianto, “Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech),” *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 2020, doi: 10.33557/binakomputer.v2i1.799.

[5] N. Butarbutar and A. R. Tanaamah, “Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma),” *J. Inf. Syst. Informatics*, vol. 3, no. 3, pp. 352–362, 2021, doi: 10.51519/journalisi.v3i3.155.

[6] M. A. G. Wattimena and A. R. Tanaamah, “Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus: TSI/Teknologi dan Sistem Informasi Perpustakaan UKSW),” *J. Inf. Syst. Informatics*, vol. 3, no. 3, pp. 483–498, 2021, doi: 10.51519/journalisi.v3i3.183.