IMPLEMENTASI DAN PENILAIAN *RISK ASSESSMENT* ATAS INFRASTRUKTUR TEKNOLOGI INFORMASI DI PT. XYZ MENGGUNAKAN *FRAMEWORK* COBIT 5

IMPLEMENTATION AND ASSESSMENT OF RISK ASSESSMENT ON INFORMATION TECHNOLOGY INFRASTRUCTURE AT PT. XYZ USING COBIT 5 FRAMEWORK

Panji Permana Syahid[1], Rd. Rohmat Saedudin[2], Basuki Rahmad[3]

[1, 2, 3] Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

panjipermana@student.telkomuniversity.ac.id[1], roja2128@gmail.com[2], basukirahmad@telkomuniversity.ac.id[3]

Abstrak

PT. XYZ merupakan perusahaan yang bergerak sebagai penyedia produk-produk elektronika industri dan prasarana serta infrastruktur yang luas. Dalam kegiatan operasionalnya, tentunya didukung Teknologi Informasi yang dapat meningkatkan nilai tambah dan daya saing perusahaan. PT. XYZ memiliki aset TI utama yang perlu dilindungi untuk menjaga fungsi hubungan dengan proses bisnis yang berjalan. Dalam perlindungan aset TI, perlu diketahui ancaman-ancaman yang mungkin terjadi dan menilai kontrol yang sudah ada untuk mengurangi dampak negatif dari risiko. PT. XYZ memiliki penerapan *risk assessment* dalam pengelolaan TI dan proses bisnis pada tiap divisi terkait. Akan tetapi, penerapan tersebut belum sepenuhnya menilai adanya ancaman pada aset TI dan menilai seberapa jauh kontrol yang sudah ada dapat mengurangi ancaman yang akan datang serta dampaknya. Maka dari itu, diperlukan implementasi dan penilaian *risk assessment* di PT. XYZ untuk menjaga fungsi TI dalam kegiatan operasionalnya.

implementasi dan penilaian *risk assessment* terhadap infrastruktur TI dilakukan menggunakan *framework* COBIT 5 *for risk* yang difokuskan untuk melakukan pengelolaan/kontrol terhadap risiko TI. Penerapan *risk assessment* dilakukan dengan mengacu pada *risk scenario* dan *control objective* pada COBIT 5 *for risk*. Penelitian ini dilakukan dengan mengidentifikasi *risk scenario* pada aset TI berdasarkan penilaian kontrol yang ada dengan *control objective* pada COBIT 5 *for risk*, selanjutnya menentukan *risk treatment* yang disesuaikan dengan keputusan perusahaan sebagai kontrol untuk menjaga kemungkinan ancaman dan dampak yang terjadi.

Hasil pada penelitian ini berupa rekomendasi implementasi dan penilaian *risk assessment* berupa *risk potential* dan *risk treatment*, sehingga diharapkan implementasi dan penilaian *risk assessment* yang mengacu pada COBIT 5 *for risk* dapat diterapkan pada PT. XYZ dalam melakukan kontrol sebagai pengelolaan pada aset TI.

Kata Kunci: **COBIT 5 *for risk, risk assessment, risk scenario, control objective, risk potential, risk treatment***

Abstract

PT. XYZ is a company engaged as a provider of industrial electronics products and infrastructure and extensive infrastructure. In its operational activities, of course, supported by Information Technology that can increase the added value and competitiveness of the company. PT. XYZ has major IT assets that need to be protected to maintain the functionality of relationships with running business processes. In the protection of IT assets, keep in mind possible threats and assess existing controls to reduce the negative impact of risk. PT. XYZ has the application of risk assessment in the management of IT and business processes in each related division. However, the application has not fully assessed the threat to IT assets and assesses how far existing controls can reduce future threats and their impacts. Therefore, it is necessary to design and assess risk assessment in PT. XYZ to maintain IT function in its operational activities.

The design and assessment of risk assessment on the IT infrastructure is carried out using the COBIT 5 for risk framework that is focused on managing / controlling IT risks. Implementation of risk assessment is done by referring to risk scenario and control objective in COBIT 5 for risk. This study was conducted by identifying risk scenarios on IT assets based on the assessment of existing controls with control objectives in COBIT 5 for risk, subsequently determining risk treatments tailored to corporate decisions as controls to safeguard possible threats and impacts.

The results of this study are recommendations on the implementation and assessment of risk assessment in the form of risk potential and risk treatment, so it is expected that the implementation and assessment of risk assessment referring to COBIT 5 for risk can be applied to PT. XYZ in control as management of IT assets.

Keywords: ***COBIT 5 for risk, risk assessment, risk scenario, control objective, risk potential, risk treatment***

1. Pendahuluan

Penelitian ini membahas permasalahan yang ada di PT. XYZ. Berdasarkan data dari hasil wawancara kepada manajer sistem informasi yang terdapat di lampiran c, kondisi *risk assessment* yang ada yaitu sudah melakukan identifikasi ancaman pada proses bisnis yang terjadi sebelumnya, *treatment* yang dilakukan sebagai antisipasi terhadap ancaman yang terjadi sebelumnya, belum adanya penilaian kontrol *existing*, belum adanya penilaian dampak terhadap ancaman yang mungkin terjadi. Dalam menilai risiko berdasarkan COBIT 5 *for risk* bahwa *risk assessment* meliputi identifikasi risiko (aset, ancaman, kontrol *existing*, konsekuensi), analisis risiko (penilaian konsekuensi, penilaian kemungkinan ancaman, penentuan nilai risiko), evaluasi risiko, penanggulangan risiko. Untuk skenario ancaman yang belum ditinjau terjadi, PT. XYZ belum memiliki penilaian kontrol *existing* [1], sehingga perusahaan akan mengalami dampak kerugian [2].

PT. XYZ merupakan Badan Usaha Milik Negara (BUMN) yang bergerak sebagai penyedia produk-produk elektronika untuk industri dan prasarana dengan jejaring bisnis serta infrastruktur yang luas dan terpadu. Berdasarkan visi dari PT. XYZ yaitu "Menjadi perusahaan elektronika kelas dunia" serta didukung oleh misi yang akan mencapai visi tersebut yaitu "Meningkatkan kesejahteraan *stakeholder* melalui inovasi produk elektronika industri dan prasarana". Oleh karena itu, tentunya PT. XYZ memiliki aset-aset TI yang kritis sebagaimana dilampirkan pada Tabel 1 yang menggambarkan jenis aset TI kritis yang dimiliki oleh PT. XYZ.

Tabel 1. Daftar dan Jumlah Aset TI Kritis PT. XYZ
(Sumber: PT. XYZ, 2016-2017)

Jenis Aset TI	Jumlah
Informasi	7
Aplikasi	8
Server/*Data Centre*	17

Berdasarkan Tabel 1 dapat dilihat bahwa PT. XYZ memiliki banyak aset TI utama. Mengingat bahwa TI merupakan aset penting dalam operasional yang dapat meningkatkan kinerja, produktivitas dan kapabilitas [3]. Kemampuan teknologi yang buruk akan membawa bencana tersebut ke perlindungan privasi [3]. Aset TI tersebut perlu diketahui nilai-nilai ancaman yang mungkin terjadi dan dikaitkan dengan penilaian kontrol *existing*, sehingga mengurangi kegagalan pencapaian tujuan dan misi perusahaan yang berdampak pada ketidakpercayaan publik atas pelayanan yang diberikan dan pada akhirnya akan mengakibatkan ketidakstabilan ekonomi secara sistematis.

2. Landasan Teori

Sumber yang digunakan sebagai referensi pada penelitian ini sebagai berikut:

2.1. COBIT 5 *for risk*

COBIT 5 *for risk* membahas tentang pertanyaan mendasar dan isu-isu tentang manajemen risiko TI. COBIT 5 *for risk* dibangun diatas kerangka COBIT 5 yang berfokus pada risiko dan memberikan panduan rinci dan praktis bagi para profesional risiko dan pihak lain yang berkepentingan di semua tingkat perusahaan [2]. COBIT 5 *for risk* merupakan *best practice* yang artinya merupakan suatu ide atau gagasan tentang suatu metode, proses, aktivitas yang efektif dan efisien dalam membantu mengurangi dan menyelesaikan suatu masalah pada perusahaan untuk pencapaian tujuan organisasi.

2.2. ISO/IEC 27005

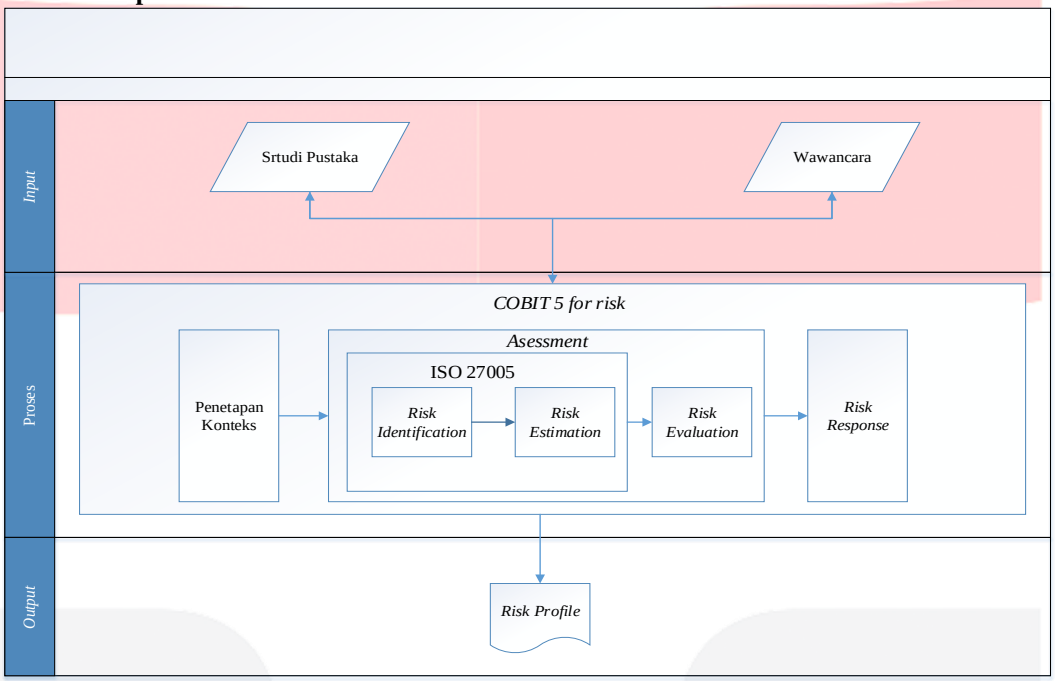
Menurut ISO/IEC 27005 berfokus pada analisis risiko, selanjutnya tahapan menuju pemilihan terhadap kontrol keamanan. ISO/IEC 27001 dan ISO/IEC 27002 lebih menjelaskan tentang perencanaan, pelaksanaan dan operasi terhadap kontrol keamanan. Proses manajemen risiko keamanan informasi terdiri dari *context establishment*, *risk assessment*, *risk treatment, risk acceptance, risk communication*, *risk monitoring and review* [4].

2.3. *Risk Assessment*

Risk assessment menentukan nilai pada aset informasi, mengidentifikasi ancaman-ancaman dan kerentanan yang dapat terjadi, mengidentifikasi kontrol dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang telah diperoleh dan menggolongkan pada kriteria evaluasi risiko yang diatur dalam *establishment context*. Tahapan pada *risk assessment* terdiri dari identifikasi risiko, analisis risiko, evaluasi risiko [4].

3. Metodologi Penelitian

3.1. Model Konseptual



Gambar 1. Model Konseptual

Pada Gambar 1 menunjukkan model konsep pada penelitian ini dengan menggunakan *input*, proses, *output*. *Input* dalam penelitian ini adalah berupa dokumen studi pustaka dan wawancara. Pada proses, dilakukan penetapan konteks sebagai ruang lingkup perusahaan, nilai aset, perhitungan nilai risiko. Penilaian terhadap risiko-risiko yaitu melakukan tahapan *assessment* (*risk identification*, *risk estimation*, *risk evaluation*), kemudian dilakukan *risk response* terhadap risiko yang telah di *assessment* yang dimana pilihan dari responnya yaitu *avoid*, *mitigate*, *transfer*, *accept*. *Output*/keluaran dari penelitian ini adalah *risk profile* berupa *risk potential*, *risk response* dan *risk treatment*

3.2. Sistematika Pemecahan Masalah

Tahapan pada sistematika pemecahan masalah antara lain:

a. Tahap identifikasi diawali dengan perumusan masalah yang berhubungan dengan permasalahan di PT. XYZ yang dilanjutkan dengan penentuan tujuan penelitian. Pada penentuan tujuan penelitian memiliki batasan masalah yang bertujuan untuk berfokus pada lingkup tertentu. Batasan masalah yaitu studi pustaka. Pada studi pustaka dimana panduan yang digunakan sebagai acuan dalam melakukan *risk assessment* yaitu COBIT 5 *for* risk, sebagai pendukungnya ISO 27005 dan *Risk IT*. Setelah itu, proses selanjutnya adalah pengamatan dokumen dan wawancara. Kemudian, dilakukan penetapan konteks sebagai ruang lingkup penelitian yaitu nilai aset, kriteria perhitungan nilai risiko. Setelah itu, dilakukannya proses identifikasi yang bertujuan untuk menentukan apa yang dapat terjadi yang menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana, dan mengapa kerugian dapat terjadi yang dimana tahapannya yaitu identifikasi aset, identifikasi ancaman dan identifikasi kontrol *existing*.
b. Pada tahap analisis dilakukan setelah melakukan tahapan identifikasi, karena tahap identifikasi merupakan tahapan awal dalam pemecahan masalah penelitian. Pada estimasi risiko ini terdapat dua metodologi dalam pelaksanaannya yaitu kualitatif dan kuantitatif. Kualitatif digunakan pertama untuk mendapatkan indikasi umum tingkat risiko. Kemudian dilanjutkan dengan kuantitatif yang berguna sebagai analisis yang spesifik. Pada tahap pertama, melakukan penilaian kerentanan dengan cara menilai *control effectiveness* terhadap kontrol *existing* dengan *control objective* pada COBIT 5 *for risk*. Aktivitas selanjutnya yaitu penilaian konsekuensi, penilaian *incident likelihood*, dan *level of risk estimation* (nilai/tingkat risiko). Pada bagian evaluasi dilakukan pemetaan nilai risiko yang disesuaikan dengan *risk appetite* (selera risiko) di perusahaan untuk penentuan *risk response* sebagai pengambilan keputusan terhadap nilai risiko. Jika telah disetujui, maka akan dilanjutkan ke tahap pelaporan dan jika tidak disetujui maka akan dilakukan kembali tahap identifikasi dan analisis.

c. Tahap pelaporan dilakukan setelah melakukan proses *assessment* risiko, yaitu menyusun dokumen rekomendasi perbaikan yang berisikan tentang profil risiko berupa *risk potential* yang berisikan nilai risiko, *risk response* yang dikaitkan dengan dokumen *risk appetite* (selera risiko) dari perusahaan dengan maksud risiko mana yang dapat diterima oleh perusahaan dan risiko mana yang tidak dapat diterima, kemudian menentukan strategi *risk treatment* yang dapat mengurangi kemungkinan terjadi suatu ancaman (*frequency*) atau dampak (*impact*) dari terjadinya ancaman yang menyebabkan kerugian bagi PT. XYZ.
d. Tahap ini merupakan tahap terakhir dalam penelitian. Tahap ini adalah tahap kesimpulan dan saran bagi implementasi dan penilaian *risk assessment* atas infrastruktur TI pada PT. XYZ menggunakan COBIT 5 *for risk*.

4. Pengolahan Data

4.1. Penetapan Konteks

Penetapan konteks merupakan ruang lingkup terhadap kajian risiko yang akan dilakukan pada *assessment* risiko. Infrastruktur TI yang akan dibahas berdasarkan data yaitu aset-aset TI kritis seperti *server*, *network* dan fasilitas ruang *server*. Dalam pelaksanaan penetapan konteks ini akan dilakukan pengelompokan aset dengan unit kerja sebagai penentuan nilai aset. Kemudian, penentuan kriteria perhitungan dalam melakukan *assessment* berupa analisis tingkat kemungkinan kejadian *existing* dan rekomendasi. Pada tahapan kriteria dampak yang dimana akan dilakukan penilaian dampak terhadap aset perusahaan. Dampak memiliki efek pada jangka pendek (operasional) dan jangka panjang (bisnis).

4.1.1. Perhitungan *Likelihood*

Rekomendasi penilaian ancaman pada infrastruktur teknologi informasi di PT. XYZ, menggunakan kriteria perhitungan menurut (ISO 27005, 2008) yang dikaitkan antara kemungkinan terjadinya suatu ancaman (*likelihood of threat*) dengan kondisi kontrol *existing* (*level of control effectiveness*) [4]. Kemudian, dapat dihasilkan nilai ancamannya (*likelihood value of incident scenario*) yang ditujukan pada Tabel 2, sebagai berikut:

Tabel 2. *Likelihood Value of Incident*
(Sumber: ISO 27005, 2008)

Likelihood of Threat	*Low* (L)			*Medium* (M)			*High* (H)		
Level of Control Effectiveness	H	M	L	H	M	L	H	M	L
Likelihood Value of an Incident Scenario	1	2	3	2	3	4	3	4	5

4.1.2. Perhitungan *Impact*

Kriteria penilaian dampak yang dilakukan berdasarkan ketentuan dari perusahaan pada dokumen yang diberikan oleh Manajer Sistem Informasi [5], sebagai berikut:

Tabel 3. Nilai Dampak
(Sumber: PT. XYZ, 2016)

Dampak	Penjelasan
1	Berpengaruh terhadap proses, tujuan, sasaran unit kerja (*minor*)
2	Berpengaruh terhadap proses, tujuan, sasaran unit kerja, dan relatif terdapat konsekuensi waktu yang masih dapat ditolerir (*moderate*)
3	Berpengaruh terhadap proses unit kerja lain dan terdapat konsekuensi waktu dan biaya/tambahan anggaran (*severe*)
4	Berpengaruh signifikan terhadap organisasi dan konsekuensi kerugian biaya (atau kehilangan peluang) yang tinggi (*major*)
5	Berpengaruh signifikan terhadap organisasi / organisasi tidak dapat beroperasi (dilihat dari *effect*) (*worst case*)

4.1.3. Kriteria Penilaian Kontrol *Existing*

Berikut merupakan kriteria dalam menentukan *rating* kontrol *existing* dan disesuaikan dengan *control objective* pada COBIT 5 *for risk*.

Tabel 4 Kriteria Penilaian Kontrol *Existing*

Rating	Keterangan
High	Kondisi kontrol *existing* memenuhi kriteria *control objective.*
Medium	Kondisi kontrol *existing* memenuhi sebagian kriteria *control objective*.
Low	Kondisi kontrol *existing* tidak memenuhi kriteria *control objective.*

4.1.4. Kriteria Penilaian *Control effectiveness*

Berikut kriteria penilaian tersebut berdasarkan pemetaan antara ancaman dengan kontrol *existing*. Dalam menentukan penilaian *control effectiveness* (keefektifan kontrol) merupakan pencapaian seberapa jauh penerapan kontrol *existing* dengan kriteria *control objective* pada COBIT 5 *for risk* dengan menggunakan perhitungan kontrol: $\frac{\text{kondisi } existing}{\text{kriteria COBIT 5 } for\ risk}$ x 100%. Sehingga dapat ditentukan persentase pencapaian kontrol *existing* sebagai berikut:

Tabel 5 Kriteria Penilaian *Control Effectiveness*

Rating	Keterangan
High	Kondisi kontrol *existing* dengan persentase ≥ 70%
Medium	Kondisi kontrol *existing* dengan persentase ≥ 40% < 70%
Low	Kondisi kontrol *existing* dengan persentase ≤ 30%

4.1.5. *Risk Response*

Dalam menentukan *risk response* terdapat 4 kriteria diantaranya *accept*, *mitigate*, *avoid*, *transfer*. Berikut kriteria respon suatu risiko yang digunakan pada penelitian ini:

- *Risk accept* dilakukan jika tingkat risiko mencapai nilai rendah/ sedang dengan aksi yaitu menerima risiko jika besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi.
- *Risk mitigate* dilakukan jika tingkat risiko mencapai nilai tinggi/ekstrem dengan aksi yaitu memutuskan untuk mengurangi dampak maupun kemungkinan terjadinya risiko.
- *Risk transfer* dilakukan jika tingkat risiko mencapai nilai tinggi/ekstrem terdapat pada aset TI yang berasal dari vendor/pihak ketiga, garansi, jaminan.
- *Risk avoid* dilakukan jika tingkat risiko mencapai nilai tinggi/ekstrem dan tergantung dari risiko yang terjadi pada suatu aset dengan aksi yang dilakukan adalah menghindari risiko yang muncul.

Pada Tabel 6 diketahui bahwa *risk appetite* (selera risiko) yang telah ditentukan oleh perusahaan, digunakan sebagai acuan dalam menentukan risiko yang dapat diterima terdapat pada warna hijau dan kuning (kecuali untuk warna kuning dengan nilai dampak 5) dan risiko yang tidak dapat diterima/yang perlu dilakukan pengendalian terdapat pada warna jingga dan merah. Berdasarkan dokumen yang diberikan oleh Manajer Sistem Informasi di PT. XYZ [6], sebagai berikut:

Tabel 6. *Risk Appetite* (Selera Risiko)
(Sumber: PT. XYZ, 2017)

5	5x1=5	5x2=10	5x3=15	5x4=20	5x5=25
4	4x1=4	4x2=8	4x3=12	4x4=16	4x5=20
3	3x1=3	3x2=6	3x3=9	3x4=12	3x5=15
2	2x1=2	2x2=4	2x3=6	2x4=8	2x5=10
1	1x1=1	1x2=2	1x3=3	1x4=4	1x5=5
Likelihood / *Impact*	1	2	3	4	5

Keterangan:

	Ekstrem
	Tinggi
	Sedang
	Rendah

4.2. Identifikasi Risiko

Tujuan dari identifikasi risiko adalah untuk menentukan apa yang bisa terjadi untuk menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, dimana dan mengapa kerugian mungkin terjadi.

4.2.1. Identifikasi Aset

Proses penilaian pada infrastruktur TI dilakukan dengan melakukan wawancara pada manajer sistem informasi dan divisi TI, dokumentasi infrastruktur yang dimiliki oleh PT. XYZ. Berikut daftar aset infrastruktur TI dengan hubungan proses bisnis yang dicantumkan pada Tabel 7 sebagai berikut:

Tabel 7. Data Aset Infrastruktur TI

Aset	Kategori
Server	*Main System Server*
	Development Server
	Supporting Server
	Application Server
Network	Fiber Optik
	Kabel data UTP CAT 6
	Kabel data STP CAT 6
	Wireless
Fasilitas	Catu daya Listrik
	Pengaturan Suhu dan Kelembaban
	Keamanan Fisik

4.2.2. Identifikasi Ancaman

Ancaman yang digunakan untuk melakukan implementasi dan penilaian *risk assessment* mengacu pada *risk scenario* menurut COBIT 5 *for risk* yang telah disesuaikan dengan jenis aset infrastruktur TI di perusahaan, sebagai berikut:

Tabel 8. Daftar Ancaman Aset Infrastruktur TI
(Sumber: ISACA, 2013)

Kategori Ancaman	Skenario Ancaman	ID
Keadaan infrastruktur teknologi	Teknologi TI yang digunakan sudah usang dan tidak dapat memenuhi kebutuhan bisnis baru (misal, jaringan, keamanan, penyimpanan)	A1
Kerusakan infrastruktur	Kerusakan *Data Centre* (sabotase)	A2
Infrastruktur (*hardware*)	Kesalahan konfigurasi pada komponen *hardware*	A3
	Kerusakan *server* kritis di ruang komputer (misal, karena kecelakaan)	A4
	Sengaja merusak *hardware* (misal perangkat keamanan)	A5
Kapasitas sistem	Sistem tidak dapat menangani transaksi saat *volume* pengguna meningkat	A6
	Sistem tidak dapat menangani beban sistem saat aplikasi baru diterapkan	A7
Malware	Gangguan *malware* pada *server* operasional	A8
	Infeksi *malware* pada komputer	A9
Staf Operasi (*human error*)	Kesalahan operator (misal saat *backup*, *upgrade* sistem, selama pemeliharaan sistem)	A10
Database integrity	*Database corrupt* (*client database*, *database* transaksi)	A11
Informasi (pelanggaran data: kerusakan, kebocoran, akses)	Hilang/kebocoran media *portable* yang mengandung data sensitif (CD, USB Drive, portable disk)	A12
	Hilang saat *backup* media	A13
	Pengungkapan informasi sensitif yang tidak disengaja, karena tidak mengikuti panduan penanganan informasi	A14
IT Expertise and Skills	Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru)	A15
Logical Attack	Pengguna asing masuk ke dalam sistem	A16
	Ada gangguan layanan akibat serangan DoS (*Denial of Service*)	A17
	Situs web aplikasi pada jaringan intranet rusak	A18
	Spionase (mata-mata)	A19
	Terdapat serangan virus	A20
Logical Trespassing	Pengguna menyalahgunakan peraturan akses *logic*	A21
	Pengguna mencuri data sensitif	A22
	Pengguna mengakses informasi diluar wewenang	A23
Pencurian infrastruktur	Pencurian dengan jumlah besar pada *server* pengembangan	A24
Bencana alam	Gempa Bumi	A25
	Badai	A26

Kategori Ancaman	Skenario Ancaman	ID
	Kebakaran	A27
	Banjir	A28
Lingkungan	Peralatan yang digunakan tidak ramah lingkungan (konsumsi daya dan *packaging*)	A29

4.2.3. Daftar Kontrol COBIT

Kontrol pada COBIT 5 *for risk* yang digunakan sesuai dengan kategori ancamannya masing-masing guna untuk melakukan penilaian terhadap kontrol *existing* di perusahaan, sehingga akan menghasilkan tingkat keefektifan kontrol (*control effectiveness*). Berikut daftar kontrol pada COBIT 5 *for risk* sebagai berikut:

Tabel 9. Daftar *Control Objective* COBIT 5 *for risk*
(Sumber: ISACA, 2013)

No.	Kategori Ancaman	Kriteria COBIT	ID
1.	Keadaan teknologi infrastruktur	Penilaian kemampuan dan kinerja saat ini	1-K1
		Perencanaan teknologi infrastruktur	1-K2
		Standar teknologi	1-K3
		Pemeliharaan infrastruktur	1-K4
2.	Kerusakan infrastruktur	Tindakan keamanan fisik	2-K1
		Akses fisik	2-K2
		Manajemen fasilitas fisik	2-K3
3.	Infrastruktur (*hardware*)	Perlindungan dan ketersediaan sumber daya infrastruktur	3-K1
		Tindakan keamanan fisik	3-K2
		Akses fisik	3-K3
4..	Kapasitas sistem	Kinerja dan perencanaan kapasitas	4-K1
5.	*Malware*	Keamanan, testing, pengawasan, dan monitoring	5-K1
		Software untuk pencegahan, deteksi, dan koreksi terhadap *malware*	5-K2
6.	Informasi	Pengaturan penyimpanan dan retensi	6-K1
		Disposal	6-K2
		Backup dan *restoration*	6-K3
7.	*Database integrity*	Data dan sistem *ownership*	7-K1
		Update standar dan prosedur	7-K2
8.	Staff operasi (*human error*)	Pelatihan personal	8-K1
		Pemulihan dan penggunaan kembali layanan TI	8-K2
		Identifikasi kebutuhan Pendidikan dan pelatihan	8-K3
		Pengiriman pelatihan dan Pendidikan	8-K4
		Prosedur dan instruksi operasi	8-K5
9.	*IT Expertise* dan *Skills*	Rekrut personal dan retensi	9-K1
		Pelatihan personal	9-K2
		Ketergantungan pada individu	9-K3
		Evaluasi Kinerja Pekerjaan Karyawan	9-K4
10.	*Logical attack*	Kebijakan manajemen TI	10-K1
		IT continuity plans	10-K2
		Keamanan, testing, pengawasan, dan monitoring	10-K3
		Software pencegahan, deteksi, koreksi terhadap *malware*	10-K4
		Persyaratan keamanan untuk pengelolaan data	10-K5
		Keamanan jaringan	10-K6
11.	*Logical trespassing*	Manajemen identitas	11-K1
		Manajemen *user* akun	11-K2
		Testing, keamanan, pengawasan dan monitoring	11-K3
12.	Pencurian infrastruktur	Kebijakan manajemen TI	12-K1
		Prosedur personal	12-K2
		Perlindungan dan ketersediaan sumber daya infrastruktur	12-K3
		Pemeliharaan model biaya	12-K4
		Tindakan keamanan fisik	12-K5
13.	Lingkungan	Rencana akuisisi infrastruktur teknologi	13-K1
		Pemilihan lokasi dan tata letak	13-K2
14.	Bencana alam	Pemulihan dan penggunaan kembali pelayanan TI	14-K1
		Pemilihan lokasi dan tata letak	14-K2
		Perlindungan terhadap faktor lingkungan	14-K3

5. Hasil dan Pembahasan

5.1. Penilaian Risiko

Penilaian risiko yang digunakan berupa *risk potential* yang dikaitkan antara *likelihood of threat* dengan *control effectiveness* yang telah disesuaikan dengan penilaian kontrol *existing*, sehingga menghasilkan nilai ancaman berupa

likelihood value of incident. Kemudian, untuk mengetahui nilai *risk potential* tersebut berdasarkan nilai pada *likelihood value of incident* dan nilai dampak sebagai pengaruh ancaman terhadap kegiatan operasional perusahaan. *Risk potential* dapat diketahui dengan menyesuaikan *risk appetite* perusahaan pada bab mengenai penetapan konteks sebelumnya. Maka, diperoleh hasil sebagai berikut:

a) Aset *server*

Tabel 10. Nilai Risiko Aset *Server*

No.	*Threat*	*Risk Potential* *Category Server*			
		Main System	*Develop-ment*	*Support-ing*	*Applica-tion*
1.	Teknologi TI yang digunakan sudah usang dan tidak dapat memenuhi kebutuhan bisnis baru (misal jaringan, keamanan, *storage*)	[3] Rendah	[2] Rendah	[6] Sedang	[3] Rendah
2.	Kerusakan *Data Centre* (sabotase)	[3] Rendah	[3] Rendah	[3] Rendah	[3] Rendah
3.	Kesalahan konfigurasi pada komponen *hardware*	[6] Sedang	[6] Sedang	[9] Sedang	[6] Sedang
4.	Kerusakan *server* yang kritis di ruang komputer (misal, karena kecelakaan)	[3] Rendah	[4] Rendah	[6] Sedang	[3] Rendah
5.	Sengaja merusak *hardware* (misal perangkat keamanan)	[3] Rendah	[2] Rendah	[8] Rendah	[3] Rendah
6.	Sistem tidak dapat menangani transaksi saat *volume* pengguna meningkat	[3] Rendah	[2] Rendah	[2] Rendah	[3] Rendah
7.	Sistem tidak dapat menangani beban saat aplikasi baru diterapkan	[3] Rendah	[2] Rendah	[4] Rendah	[6] Sedang
8.	Gangguan *malware* pada *server* operasional	[6] Sedang	[6] Sedang	[6] Sedang	[6] Sedang
9.	Infeksi *malware* pada komputer	[3] Rendah	[4] Rendah	[2] Rendah	[3] Rendah
10.	Kesalahan operator (misal pada *backup*, *upgrade* sistem, selama pemeliharaan sistem)	[12] Tinggi	[8] Sedang	[8] Sedang	[12] Tinggi
11.	*Database corrupt* (*client database*, *database* transaksi)	[6] Sedang	[4] Rendah	[6] Sedang	[6] Sedang
12.	Kehilangan/kebocoran media portabel yang mengandung data sensitif (CD, USB *Drive*, *portable disk*)	[9] Sedang	[6] Sedang	[6] Sedang	[9] Sedang
13.	Hilang data saat *backup* media	[4] Rendah	[2] Rendah	[4] Rendah	[4] Rendah
14.	Pengungkapan informasi sensitif yang tidak disengaja, karena tidak mengikuti panduan penanganan informasi	[6] Sedang	[2] Rendah	[4] Rendah	[6] Sedang
15.	Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru)	[12] Tinggi	[8] Sedang	[12] Tinggi	[12] Tinggi

b) Aset *Network* (LAN *interconnection*)

Tabel 11. Nilai Risiko Aset *Network*

No.	*Threat*	*Risk Potential*
1.	Teknologi TI yang digunakan sudah usang dan tidak dapat memenuhi kebutuhan bisnis baru (misalnya jaringan, keamanan, penyimpanan)	[6] Sedang
2.	Kesalahan konfigurasi pada komponen *hardware*	[9] Sedang
3.	Sengaja merusak *hardware* (misalnya pada perangkat keamanan)	[3] Rendah
4.	Pengguna asing masuk ke dalam sistem	[8] Sedang
5.	Terdapat gangguan layanan akibat serangan DoS (*Denial of Service*)	[6] Sedang
6.	Situs web aplikasi pada jaringan intranet rusak	[9] Sedang
7.	Spionase (mata-mata)	[8] Sedang
8.	Terdapat serangan virus	[9] Sedang
9.	Pengguna melanggar peraturan akses *logic*	[6] Sedang
10.	Pengguna mencuri data sensitif	[8] Sedang
11.	Pengguna mengakses informasi diluar wewenang	[9] Sedang

12.	Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru)	[9] Sedang

c) Aset fasilitas ruang *server*

Tabel 12. Nilai Risiko Aset Fasilitas Ruang *Server*

No.	*Threat*	*Risk Potential*
1.	Pencurian skala besar pada *server* pengembangan	[3] Rendah
2.	Gempa bumi	[20] Ekstrem
3.	Badai	[16] Tinggi
4.	Kebakaran	[15] Tinggi
5.	Banjir	[5] Sedang
6.	Peralatan yang digunakan tidak ramah lingkungan (misalnya konsumsi daya dan *packaging*)	[10] Sedang

5.2. *Risk Treatment*

Rekomendasi *Risk Treatment* terhadap hasil nilai risiko yang perlu di mitigasi. Penentuan *treatment* disesuaikan dengan *control objective* pada COBIT 5 *for risk* berdasarkan jenis ancamannya sebagai kontrol untuk mengurangi kemungkinan terjadinya ancaman dan dampak kejadian suatu ancaman. Maka, *treatment* yang diusulkan sebagai berikut:

1. Aset *Main System Server*

Tabel 13 *Risk Treatment* Aset *Main System Server*

No.	*Threat*	*Risk Potential*	*Risk Response*	*Treatment*
1.	Kesalahan operator (misal pada *backup*, *upgrade* sistem, selama pemeliharaan sistem)	[12] Tinggi	*Mitigate*	• Penerapan kebijakan mengenai *punishment* untuk meningkatkan tingkat kedisiplinan pegawai. • Memberikan pelatihan pada staf TI mengenai *system admin*, *network admin* dan *database admin*. • Penerapan prosedur dan intruksi sebagai panduan kegiatan operasional dan membahas langkah untuk *recovery* dan *resumption*, melakukan *update* prosedur terhadap teknologi atau sistem yang baru.
2.	Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru)	[12] Tinggi	*Mitigate*	• Melakukan rekruitasi staf TI pada unit *system admin*, *network admin*, dan *database admin* untuk mengurangi ketergantungan pada individu. • Identifikasi dan ketepatan pemberian pelatihan pada staf mengenai *system Admin*, *network admin* dan *database admin*. • Melakukan evaluasi oleh manajer TI terhadap kinerja staf TI minimal satu kali dalam dua minggu. Sehingga, dapat membantu dalam proses rekruitasi staf baru atau pemberian pelatihan pada staf TI.

2. Aset *Supporting Server*

Tabel 14. *Risk Treatment* Aset *Supporting Server*

No.	*Threat*	*Risk Potential*	*Risk Response*	*Treatment*
1.	Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru)	[12] Tinggi	*Mitigate*	• Identifikasi dan ketepatan pemberian pelatihan pada staf TI mengenai *system admin*, *network admin*, *database admin*

3. Aset Fasilitas Ruang *Server*

Tabel 15. *Risk Treatment* Aset *Fasilitas Ruang Server*

No.	*Threat*	*Risk Potential*	*Risk Response*	*Treatment*
1.	Gempa bumi	[20] Ekstrem	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtual atau fisik dengan lokasi penyimpanan di lokasi lain. Penanggulangan terhadap risiko dapat mengurangi efek pada dampak dan organisasi masih dapat berjalan seperti biasanya.
2.	Badai	[16] Tinggi	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtual atau fisik dengan lokasi penyimpanan di lokasi lain.
3.	Kebakaran	[15] Tinggi	*Mitigate*	• Perencanaan dan penerapan *disaster recovery* baik virtual atau fisik dengan lokasi penyimpanan di lokasi lain. • Pengecekan fungsi keamanan fisik (FAP, FM200, APAR) untuk mengurangi dampak kebakaran.

No.	*Threat*	*Risk Potential*	*Risk Response*	*Treatment*
4.	Banjir	[5] Sedang	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtual atau fisik dengan lokasi penyimpanan di lokasi lain
5.	Peralatan yang digunakan tidak ramah lingkungan (misalnya konsumsi daya dan *packaging*)	[10] Sedang	*Mitigate*	Pengecekan fungsi alat pendukung yang meliputi tegangan listrik, sistem monitoring (suhu, kelembaban), fungsi alat keamanan fisik (FAP, UPS, PAC, FM200).

4. Kesimpulan

Berdasarkan seluruh proses penilaian *risk assessment* atas infrastruktur teknologi informasi di PT. XYZ menggunakan COBIT 5 *for risk*, dapat disimpulkan bahwa:

a. Hasil dari penilaian risiko berupa *risk potential* pada aset infrastruktur teknologi informasi yaitu: Aset *main system server* dengan nilai risiko Tinggi=2, Sedang=5, Rendah=8; Aset *development server* dengan nilai risiko Sedang=5, Rendah=10; Aset s*upporting server* dengan nilai risiko Tinggi=1, Sedang=7, Rendah=7; Aset *application server* dengan nilai risiko Tinggi=2, Sedang=6, Rendah=7; Aset *network* (LAN *interconnection*) dengan nilai risiko Sedang=11, Rendah=1; Aset fasilitas ruang *server* dengan nilai risiko Ekstrem=1, Tinggi=2, Sedang=2, Rendah=1.

b. Hasil dari *risk assessment* diketahui bahwa nilai risiko terhadap ancaman yang perlu di mitigasi berdasarkan *risk appetite* (selera risiko) di PT. XYZ yaitu: Pada aset *main system server*, aset *application server* adalah Kesalahan operator (misal pada *backup*, *upgrade* sistem, selama pemeliharaan sistem), Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru; Aset *Supporting Server* adalah Kurangnya atau ketidakcocokan keahlian dalam penggunaan TI (misalnya, karena teknologi baru; Aset fasilitas ruang *server* adalah Gempa bumi, Badai, Banjir, Kebakaran, Peralatan yang digunakan tidak ramah lingkungan (misalnya konsumsi daya dan *packaging*).

c. Berdasarkan nilai risiko yang perlu di mitigasi terhadap masing-masing aset, maka akan dilakukan *treatment* sebagai kontrol yang dapat mengurangi tingkat kemungkinan ancaman terjadi dan dampaknya yaitu: Aset *main system server, application server* yaitu Penerapan kebijakan mengenai *punishment*, Memberikan pelatihan pada staf TI, Penerapan prosedur dan intruksi sebagai panduan mengenai *recovery* dan *resumption*, Melakukan rekruitasi staf TI untuk mengurangi ketergantungan pada individu, Melakukan evaluasi oleh manajer TI terhadap kinerja staf TI; Aset *supporting server* yaitu Identifikasi dan ketepatan pemberian pelatihan pada staf TI; Aset fasilitas ruang *server* yaitu Perencanaan dan penerapan *disaster recovery*, pengecekan fungsi keamanan fisik di ruang *server*, Pengecekan fungsi alat pendukung yang meliputi tegangan listrik, sistem monitoring (suhu, kelembaban).

Referensi

[1] XYZ, 20170602 RFR-001 IRO Sisfo Progress Mei, Bandung, 2016.

[2] ISACA, COBIT 5 For Risk, USA, 2013.

[3] M. Lubis, M. Kartiwi and S. Zulhuda, "A GUIDELINE TO ENFORCE PRIVACY AND DATA PROTECTION REGULATION IN INDONESIA," *Proceeding - Kuala Lumpur International Business, Economics and Law Conference*, 2013.

[4] ISO/IEC, Information Technology-Security Techniques-Information Security Risk Management - 27005, UK: British Standard, 2008.

[5] XYZ, RFR-910 Identifikasi Risiko_Operasional Unit Kerja, Bandung, 2016.

[6] XYZ, Laporan ManRISK unit pendukung_2, Bandung, 2017.

[7] XYZ, RFR-001 Identifikasi Risiko Operasional Sisfo draft 01, Bandung, 2016.

[8] ISACA, The Risk IT Framework, USA, 2009.

[9] G. Paulina, "Audit Tata Kelola Teknologi Informasi Berbasis Risiko dengan Menggunakan Framework Risk IT COBIT 4.1," 2013.