IMPLEMENTASI DAN PENILAIAN *RISK ASSESSMENT* ATAS APLIKASI DI PT. XYZ DENGAN MENGGUNAKAN *FRAMEWORK* COBIT 5

IMPLEMENTATION AND ASSESSMENT OF RISK ASSESSMENT ON APPLICATION AT PT.XYZ USING COBIT 5 FRAMEWORK

Ibnu Yazid Ikhwana[1], Rd. Rohmat Saedudin[2], Dr. Basuki Rahmad[3]

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

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

Abstrak

PT. XYZ Industri (Persero) merupakan perusahaan yang bergerak dalam bidang industri elektronik. Berdasarkan hasil wawancara dengan manajer sistem informasi di PT. XYZ, untuk penelitian ini akan dilakukan implementasi dan penilaian *risk assessment* pada aset aplikasi. Dalam aset aplikasi tersebut memiliki risiko yang dapat mempengaruhi operasional perusahaan. Kondisi pengelolaan risiko yang telah dilakukan oleh perusahaan yaitu berupa identifikasi risiko dengan ancaman yang sudah terjadi terhadap proses bisnis yang berjalan di perusahaan, dan *treatment* yang akan dilakukan terhadap setiap risiko tersebut, perusahaan belum sepenuhnya melakukan penilaian ancaman serta penilaian kontrol yang ada. Maka dari itu, dilakukan penelitian dengan melakukan perancangan *risk assessment* untuk risiko dengan ancaman-ancaman yang mungkin akan terjadi pada perusahaan serta penilaian atas kontrol yang ada berdasarkan kerangka kerja COBIT 5 *for risk* dan menggunakan metode *risk assessment* standar ISO/IEC 27005: *Risk Management.* Penerapan *risk assessment* yang dilakukan pada penelitian ini mengacu pada *risk scenario* dan *control objective* pada COBIT 5 *for risk*. Penelitian ini akan dilakukan identifikasi *risk scenario* pada aset TI dan penilaian kontrol yang ada berdasarkan *control objective* pada COBIT 5 *for risk*, lalu akan ditentukan *risk treatment* yang dapat dijadikan acuan oleh perusahaan untuk menjaga tingkat kemungkinan ancaman serta dampak yang dapat terjadi.

Hasil dari penelitian ini yaitu di dapatkannya *risk potential* dari setiap risiko yang ada, dimana risiko tersebut telah dilakukan penilaian dengan urutkan proses *assessment* menurut panduan BS ISO/IEC 27005 dan *treatment* yang akan dilakukan untuk setiap risiko tersebut.

Kata Kunci: COBIT 5, ISO/IEC 27005, *Risk Assessment, Control Objective, Risk Potential, Risk Treatment*

Abstract

PT. XYZ Industri (Persero) is a company engaged in the electronics industry. Based on the results of interviews with information systems managers at PT. XYZ, for this research will be performed and assessment of risk assessment on asset application. In the assets of such applications have risks that may affect the company's operations. Conditions of risk management that have been done by the company is in the form of risk identification with threats that have occurred to the business processes running in the company, and the treatment will be done on each risk, the company has not fully assess the threat and assessment of existing controls. Therefore, research is conducted by designing risk assessment for risks with possible threats to the company and assessment of existing controls based on the COBIT 5 for risk framework and using the risk assessment method of ISO / IEC 27005 standard: Risk Management. Implementation of risk assessment conducted in this study refers to risk scenario and control objective in COBIT 5 for risk. This research identifies risk scenarios on IT assets and assesses existing controls based on the control objectives in COBIT 5 for risk, and then determines the risk treatment that can be used as a reference by the company to maintain the level of possible threats and impacts that may occur.

The result of this research is to get the risk potential from each risk, where the risk has been assessed by sequencing the assessment process according to the guidance of BS ISO / IEC 27005 and treatment that will be done for each risk.

Keywords: COBIT 5, ISO/IEC 27005, *Risk Assessment, Control Objective, Risk Potential, Risk Treatment*

1. Pendahuluan

Berdasarkan hasil wawancara dengan manajer sistem informasi di PT. XYZ, diketahui bahwa perusahaan ini memiliki tiga aset TI utama perusahaan untuk menjalankan proses bisnisnya yaitu aset aplikasi, aset server, dan aset informasi. Dari setiap aset TI utama tersebut memiliki risiko yang dapat mempengaruhi operasional perusahaan. Kondisi pengelolaan risiko yang telah dilakukan oleh perusahaan yaitu berupa identifikasi risiko dengan ancaman yang sudah terjadi terhadap proses bisnis yang berjalan di perusahaan, dan *treatment* yang akan dilakukan terhadap setiap risiko tersebut, perusahaan belum sepenuhnya melakukan penilaian ancaman serta belum terdapat penilaian kontrol yang ada**.** Berikut merupakan tiga aset TI utama perusahaan:

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

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

PT XYZ merupakan Badan Usaha Milik Negara (BUMN) yang bergerak dalam bidang industri elektronik, visi dari PT. XYZ yaitu “Menjadi perusahaan elektronika kelas dunia”. Semakin berkembangnya teknologi di dunia pastinya juga akan mempengaruhi berkembangnya teknologi di Indonesia, untuk itulah perusahaan ini mempunyai misi yaitu “meningkatkan kesejahteraan pemangku kepentingan melalui inovasi produk elektronika industri dan prasarana”. Berdasarkan Tabel diatas, dapat dilihat bahwa PT. XYZ memiliki banyak aset TI utama dimana aset tersebut merupakan aset penting dalam operasional perusahaan. Maka dari itu, aset tersebut perlu diketahui nilai risiko dengan ancaman-ancaman yang mungkin akan terjadi dan dikaitkan dengan penilaian kontrol yang telah dilakukan, sehingga dapat mengurangi kegagalan pencapaian tujuan dan misi perusahaan.

2. Dasar Teori

2.1 COBIT 5 *for risk*

COBIT 5 (*Control Objectives for Information and Related Technology*) merupakan sebuah proses model yang dikembangkan untuk membantu perusahaan dalam melakukan pengelolaan sumber daya teknologi informasi (TI). Proses model ini difokuskan pada pengendalian terhadap masing-masing dari 34 proses teknologi informasi, meningkatkan tingkatan kemapanan proses dalam TI dan memenuhi ekspektasi bisnis dari TI.

2.2 ISO/IEC 27005

ISO/IEC 27005 dirancang sebagai panduan untuk Manajemen Risiko Keamanan Informasi dalam sebuah organisasi, khususnya untuk mendukung persyaratan ISMS (information System Managamenet Security) sesuai dengan ISO/IEC 27001 (BS ISO 27005, 2008). ISMS merupakan bagian yang terintegrasi dengan struktur organisasi dan proses manajemen secara keseluruhan, keamanan informasi terdapat pada desain proses, sistem informasi, dan kontrol (BS ISO 27001, 2005). Proses manajemen risiko keamanan informasi terdiri dari *context establishment, risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and review*.

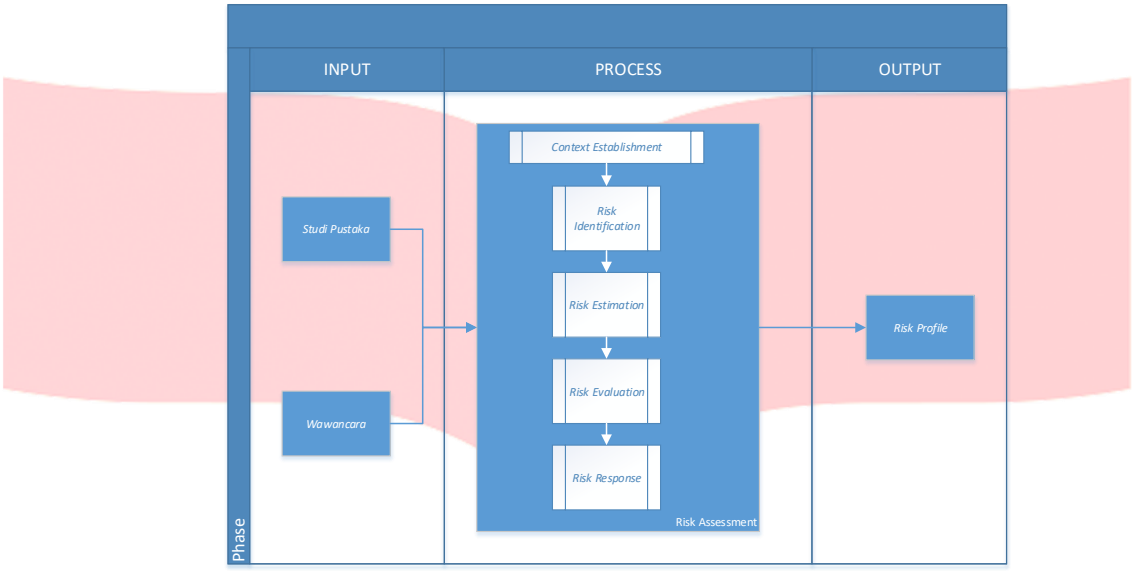
2.3 *Risk Assessment*

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.

3. Metode Penelitian

3.1 Metode Konseptual

Berikut ini adalah metode konseptual yang berdasarkan Gambar [3].



Gambar 1. Metode Konseptual

Tahapan pada sistematika pemecahan masalah antara lain:

a. Tahap identifikasi diawali dengan merumuskan masalah yang terdapat pada PT. XYZ dan dilanjutkan dengan menentukan tujuan dari penelitian. Penelitian dibatasi oleh batasan masalah agar penelitian fokus terhadap tujuan penelitian. Batasan masalah terdiiri dari studi litelatur dan studi pustaka. Pada studi litelatur yaitu data yang dibutuhkan sesuai dengan tujuan dan perumusan masalah diantaranya arsitektur infrastruktur eksisting, proses bisnis eksisting dan *framework* eksisting di PT. XYZ. Sedangkan pada studi pustaka dimana panduan yang digunakan sebagai acuan dalam melakukan *risk assessment* yaitu COBIT 5 *for risk*, dan ISO 27005. Setelah itu, proses selanjutnya adalah pengamatan dan dilanjutkan dengan wawancara. Kemudian, dilakukannya proses identifikasi bertujuan untuk menentukan apa yang dapat menyebabkan terjadinya potensi kerugian, dan untuk medapatkan wawasan tentang bagaimana, di mana, dan mengapa kerugian dapat terjadi, yang dimana tahapannya yaitu identifikasi aset, identifikasi ancaman, dan identifikasi kontrol..
b. Pada tahap analisis dilakukan setelah melakukan tahapan identifikasi, karena tahap identifikasi merupakan tahapan awal dalam pemecahan masalah penelitian. Tahap analisis yaitu mengestimasi risiko yang dilakukan dalam berbagai tingkat detail tergantung pada kekritisan aset, tingkat kerentanan dan insiden sebelumnya yang melibatkan organisasi. Pada estimasi risiko ini akan dibuat penilaian *risk potential* (potensi risiko), terdapat dua metodologi dalam pelaksanaannya yaitu kuantitatif dan kualitatif. Kualitatif digunakan pertama untuk mendapatkan indikasi umum tingkat risiko. Kemudian dilanjutkan dengan kuantitatif yang berguna sebagai analisis yang spesisifik. Aktivitas selanjutnya yaitu penilaian kerentanan yang didapat dengan melihat tingkat keefektifan kontrol, penilaian *incident likelihood*, dan *level of risk estimation*. Pada bagian *risk evaluation* dilakukan pengelompakan niliai risiko yang tidak sesuai dengan kriteria *risk appetite* (selera risiko) dari perusahaan.
c. Tahap pelaporan dilakukan setelah melakukan proses *assessment*. Kemudian akan mengasilkan laporan berupa dokumen rekomendasi yang berisikan tentang *risk profile*. *Risk Profile* tersebut berisi nilai dari risk potential (potensi terjadinya risiko), risk response terhadap risiko dari hasil penilaian yang telah dikaitkan dengan *risk appetite* (selera risiko) perusahaan, strategi *treatment* risiko yang direkomendasikan.
d. Tahap ini merupakan tahap terakhir dalam penelitian. Tahap ini adalah tahap kesimpulan dan saran bagi perancangan dan penilaian *risk assessment* atas aplikasi pada PT. XYZ.

4. Pengolahan Data

4.1 Penetapan Konteks

Penetapan konteks merupakan ruang lingkup terhadap kajian risiko untuk melakukan *risk assessment*. Penelitian ini akan dilakukan *assessment* pada aset TI di perusahaan khususnya aset aplikasi. Pada sub-bab penetapan konteks akan ditetapkan seluruh data yang akan dirancang untuk penilaiannya. Nilai-nilai yang ditetapkan seperti pada kriteria dampak dimana diberikan nilai minimum dan maksimum dari frekuensi serta dampaknya. Ditetapkan pula penilaian *likelihood of threat* (*low, medium, high*) dan krietria perhitungan risiko.

4.1.1 Perhitungan *Likelihood*

Rekomendasi penilaian ancaman pada aplikasi 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*). 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 "RFR-910 Identifikasi Risiko_Operasional Unit Kerja" yang diberikan oleh Manajer Sistem Informasi, 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*

High: Dikatakan tinggi apabila memenuhi *Control Objective.*
Medium: Dikatakan sedang apabila memenuhi sebagian dari *Control Objective.*
Low: Dikatakan rendah apabila memenuhi sebagian dari *Control Objective*.

4.1.4 Kriteria Penilaian Kontrol Berdasarkan Ancaman

Kriteria ditentukan berdasarkan pemetaan pada Lampiran B, yaitu pemetaan kontrol terhadap ancaman. Kriteria penilaian kontrol berdasarkan ancaman ditentukan dengan melihat persentase kondisi kontrol dari suatu ancaman, dikatakn high apabila persentase mencapai 70% – 100%, medium apabila persentase mencapai 40% – 70%, dan low apabila persentase 30% atau dibawahnya. Persentase kondisi kontrol tersebut didapatkan dengan rumus:

$$\frac{\text{Kondisi}}{\text{Kriteria}} \times 100\%$$

4.1.3 *Risk Response*

Dalam menentukan Risk Response, terdapat empat kriteria penentuan *response* terhadap risiko yaitu *accept*, *transfer*, *mitigate*, dan *avoid*. Pada penelitian ini, respon *accept* digunakan untuk risiko berwarna hijau atau kuning (kecuali untuk risiko dengan nilai lima), respon *transfer* digunakan untuk risiko yang dapat ditangani oleh vendor, respon mitigate digunakan untuk risiko berwarna oranye atau merah, dan respon *avoid* dapat digunakan tergantung dari kondisi ancaman (contoh: apabila terdapat ancaman yang menyebabkan perusahaan mengalami kekurangan *resources* atau biasa, maka dapat memperpanjang jadwal proyek). Keempat kriteria penentuan respon risiko tersebut dapat ditentukan dengan memasukkan nilai risiko kedalam *risk appetite*. Pada Tabel 4 diketahui bahwa *risk appetite* (selera risiko) yang telah ditentukan oleh perusahaan. *Risk Appetite* tersebut digunakan sebagai acuan dalam menentukan risiko yang dapat diterima dan risiko yang tidak dapat diterima/yang perlu dilakukan pengendalian. Berdasarkan dokumen "Laporan ManRisk Unit Pendukung" yang diberikan oleh Manajer Sistem Informasi di PT. XYZ sebagai berikut:

Tabel 4. Risk Appetite (Selera Risiko)
(Sumber: PT. XYZ, 2017)

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Likelihood / Dampak	1	2	3	4	5

Keterangan:

	Ekstrim
	Tinggi
	Sedang
	Rendah

4.2. Identifikasi Risiko

Tahapan awal dari identifikasi risiko yaitu terdiri dari identifikasi aset yang akan diberikan ulasan mengenai aset-aset aplikasi perusahaan, dilanjutkan dengan identifikasi ancaman, identifikasi kontrol eksisting yang akan disesuaikan dengan kontrol dari COBIT sehingga dapat dinilai keefektifan kontrolnya.

4.2.1. Identifikasi Aset

Proses penilaian pada aplikasi dilakukan dengan melakukan wawancara pada manajer sistem informasi dan divisi TI, dokumentasi aplikasi yang dimiliki oleh PT. XYZ. Berikut daftar aset aplikasi pada Tabel 5 sebagai berikut:

Tabel 5. Data Aset Aplikasi

No.	Nama Aplikasi
1.	Aplikasi ERP Agresso
2.	Aplikasi *Cash Flow*
3.	Aplikasi Pengadaan
4.	Aplikasi e-*Procurement*
5.	Aplikasi *Monitoring* Pengadaan
6.	Aplikasi SIM

4.2.2. Identifikasi Ancaman

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

Tabel 6. Daftar Ancaman Aset Aplikasi
(Sumber: ISACA, 2013)

Threat Category	*Threat Scenario*	ID
Software Implementation	1. Kesalahan operasional saat perangkat lunak baru dibuat	A1-1
	2. pengguna tidak siap untuk menggunakan dan memanfaatkan perangkat lunak aplikasi baru	A1-2
Software Integrity	1. Modifikasi perangkat lunak yang disengaja yang mengarah ke data yang salah atau tindakan curang	A2-1
	2. Modifikasi perangkat lunak yang tidak disengaja mengarah pada hasil yang tidak diharapkan	A2-2
	3. Kesalahan konfigurasi dan kesalahan pengelolaan yang tidak disengaja	A2-3
Software Performance	1. Perangkat lunak biasa mengalami malfungsi terhadap perangkat lunak aplikasi kritis	A3-1
	2. Masalah perangkat lunak intermiten dengan perangkat lunak sistem yang penting	A3-2
Malware	1. Infeksi malware pada komputer	A4-1
Logical Attack	1. Serangan virus	A5-1
	2. Pengguna yang tidak berwenang mencoba masuk ke sistem	A5-2
	3. Serangan dos (*denial-of-service*)	A5-3
	4. Spionase industri	A5-5
Staff Operations	1. Terjadi eror pada operator/Staf TI (selama *backup*, upgrade system, *maintenance* sistem)	A6-1
	2. Terjadi kesalahan pada input data	A6-2
IT expertise and skills	1. Ketidaksesuaian atau ketidakcocokan keterampilan terkait TI di dalam TI (mis., karena teknologi baru)	A7-1
	2. Kurangnya pemahaman bisnis oleh staf TI	A7-2
Information media	1. Kehilangan / pengungkapan media portabel yang berisi data sensitif (mis., CD, *drive* USB, *disk* portabel)	A8-1
	2. Pengungkapan informasi sensitif yang tidak disengaja karena tidak mengikuti panduan penanganan informasi.	A8-2

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 7. Daftar *Control Objective* COBIT 5 *for risk*

Threat Category	Kriteria COBIT	ID
Software Implementation	*Software Quality Assurance* (QA)	K1-1
	Knowledge Transfer to Operations and Support Staff	K1-2
	Implementation Plan	K1-3
	Final Acceptance Test	K1-4
Software Integrity	*Development of Application Software*	K2-1
	Application Software Maintenance	K2-2
	Change Standards and Procedures	K2-3
	Post-implementation Review	K2-4
	Identity Management	K2-5
	Configuration Integrity Review	K2-6
	Accuracy, Completeness and Authenticity Checks	K2-7
	Processing Integrity and Validity	K2-8
	Output Review, Reconciliation and Error Handling	K2-9
	Transaction Authentication and Integrity	K2-10
Software Performance	*Application Software Maintenance*	K3-1
	Monitoring and Reporting	K3-2
	Problem Tracking and Resolution	K3-3
Malware	*Security Testing, Surveillance and Monitoring*	K4-1
	Malicious Software Prevention, Detection and Correction	K4-2
Logical Attack	*IT Policies Management*	K5-1
	IT Continuity Plans	K5-2
	Security Testing, Surveillance and Monitoring	K5-3
	Malicious Software Prevention, Detection and Correction	K5-4
	Network Security	K5-5
	Security Requirements for Data Management	K5-6
Staff Operations	*Personnel Training*	K7-1
	IT Services Recovery and Resumption	K7-2
	Identification of Education and Training Needs	K7-3
	Delivery of Training and Education	K7-4
	Operations Procedures and Instructions	K7-5
IT Expertise skills	*Personnel Recruitment and Retention*	K8-1
	Personnel Training	K8-2
	Dependence Upon Individuals	K8-3
	Employee Job Performance Evaluation	K8-4
Information media	*Storage and Retention Arrangements*	K9-1
	Disposal	K9-2
	Backup and Restoration	K9-3

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:

Tabel Nilai Risiko Aset Aplikasi

Threat	Aplikasi					
	ERP Agresso	*Cash Flow*	Pengadaan	*E-Procurement*	*Monitoring* Pengadaan	SIM Perusahaan
Kesalahan operasional saat perangkat lunak baru dibuat	[6] Sedang	[2] Rendah	[9] Sedang	[3] Rendah	[6] Sedang	[4] Rendah
pengguna tidak siap untuk menggunakan dan memanfaatkan perangkat lunak aplikasi baru	[3] Rendah	[6] Sedang	[3] Rendah	[3] Rendah	[3] Rendah	[4] Rendah

Modifikasi perangkat lunak yang disengaja yang mengarah ke data yang salah atau tindakan curang/menipu.	[4] Rendah	[4] Rendah	[4] Rendah	[4] Rendah	[3] Rendah	[4] Rendah
Modifikasi perangkat lunak yang tidak disengaja mengarah pada hasil yang tidak diharapkan	[4] Rendah	[6] Sedang	[6] Sedang	[6] Sedang	[6] Sedang	[9] Sedang
Kesalahan konfigurasi dan kesalahan pengelolaan yang tidak disengaja	[4] Rendah	[6] Sedang	[8] Sedang	[8] Sedang	[8] Sedang	[8] Sedang
Perangkat lunak biasa mengalami malfungsi terhadap perangkat lunak aplikasi kritis	[8] Sedang	[6] Sedang	[8] Sedang	[3] Rendah	[3] Rendah	[4] Rendah
Masalah perangkat lunak intermiten dengan perangkat lunak sistem yang penting	[3] Rendah	[6] Sedang	[6] Sedang	[6] Sedang	[6] Sedang	[6] Sedang
Infeksi malware pada komputer	[9] Sedang	[6] Sedang	[9] Sedang	[6] Sedang	[9] Sedang	[4] Rendah
Serangan virus	[9] Sedang	[9] Sedang	[9] Sedang	[9] Sedang	[6] Sedang	[9] Sedang
Pengguna yang tidak berwenang mencoba masuk ke sistem	[4] Rendah	[4] Rendah	[4] Rendah	[12] Tinggi	[4] Rendah	[4] Rendah
Serangan dos (*denial-of-service*)	[3] Rendah	[2] Rendah	[3] Rendah	[9] Sedang	[3] Rendah	[3] Rendah
Spionase industri	[6] Sedang	[8] Sedang	[6] Sedang	[12] Tinggi	[6] Sedang	[8] Sedang
Terjadi eror pada operator/IT staff (selama *backup*, *upgrade* sistem, *maintenance* sistem)	[3] Rendah	[3] Rendah	[3] Rendah	[3] Rendah	[3] Rendah	[3] Rendah
Terjadi kesalahan pada input data	[12] Tinggi	[12] Tinggi	[12] Tinggi	[16] Tinggi	[6] Sedang	[16] Tinggi
Ketidaksesuaian atau ketidakcocokan keterampilan terkait TI di dalam TI (mis., Karena teknologi baru)	[8] Sedang	[8] Sedang	[8] Sedang	[8] Sedang	[8] Sedang	[8] Sedang
Kurangnya pemahaman bisnis oleh staf TI	[8] Sedang	[8] Sedang	[12] Tinggi	[12] Tinggi	[8] Sedang	[12] Tinggi
Kehilangan / pengungkapan media portabel yang berisi data sensitif (mis., CD, drive USB, disk portabel)	[6] Sedang	[6] Sedang	[6] Sedang	[8] Sedang	[6] Sedang	[6] Sedang
Pengungkapan informasi sensitif yang tidak disengaja karena tidak mengikuti panduan penanganan informasi	[4] Rendah	[4] Rendah	[4] Rendah	[4] Rendah	[4] Rendah	[4] Rendah

5.1.2. 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 dari suatu ancaman. Maka, *treatment* yang diusulkan sebagai berikut:

No.	*Threat*	Aset	*Risk Response*	*Treatment*
1.	Terjadi kesalahan pada input data	ERP Agresso, *Cash Flow*, Pengadaan, *E-procurement*, SIM Perusahaan	*Mitigate*	Risiko dapat lakukan mitigasi atau pengurangan potensi terjadinya risiko dengan mengurangi *likelihood* dari *threat* itu sendiri. Likelihood dapat dikurangi dengan menerapkan pemberian sanksi terhadap pegawai yang melakukan kesalahan pada penginputan data tergantung keputusan atasan dari setiap bagian sehingga pegawai akan lebih berhati-hati dalam melakukan penginputan data.
2.	Pengguna yang tidak berwenang mencoba masuk ke sistem	*E-procurement*	*Mitigate*	*Likelihood* atau frekuensi dapat dikurangi dengan cara memberikan peraturan atau kebijakan terhadap user dari pihak luar/ mitra perusahaan dalam menggunakan aplikasi *e-procurement*, agar tidak sembarang orang dapat membuka dan mengubah data pada aplikasi secara bebas. Dampak dapat dikurangi dengan memperkuat *Public Relation* agar dapat menumbuhkan dan

				mengembangkan hubungan baik antar organisasi dengan publiknya/mitranya, internal maupun eksternal.
3.	Spionase industri	*E-procurement*	*Mitigate*	Dampak dapat dikurangi dengan selalu menjaga kebijakan pegawai agar tetap dipatuhi dan memprekuat *Public Relation* agar dapat menumbuhkan dan mengembangkan hubungan baik antar organisasi dengan publiknya/mitranya.
4.	Kurangnya pemahaman bisnis oleh staf TI	Pengadaan, *E-procurement*, SIM Perusahaan	*Mitigate*	*Likelihood* dapat dikurangi dengan memberikan karyawan TI orientasi yang sesuai saat pelatihan, berikan staf TI spesifikasi kebutuhan perangkat lunak dari aplikasi Pengadaan, *E-procurement*, dan SIM Perusahaan meliputi HRIS, *Monitoring* Proyek, dan *Monitoring Marketing*/ Perolehan kontrak yang sedang dalam tahap pengembangan agar lebih mengerti fungsi-fungsi dari aplikasi tersebut untuk dapat dilakukan pemrogramannya.

6. Kesimpulan

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

1. Profil risiko saat ini dari seluruh aset aplikasi adalah, sebagai berikut:

Rendah	Sedang	Tinggi	Ekstrim
43	55	10	0

2. Beberapa risiko yang harus dimitigasi dan diberikan rekomendasi penanganan atas risiko tersebut ialah:
   a. Pengguna yang tidak berwenang mencoba masuk ke sistem, pada aset aplikasi *e-procurement*.
   b. Spionase Industri, pada aset aplikasi *e-procurement.*
   c. Terjadi kesalahan pada input data, pada aset aplikasi ERP Agresso,aplikasi *Cash Flow*, aplikasi Pengadaan, aplikasi *e-procurement*, dan aplikasi SIM Perusahaan.
   d. Kurangnya pemahaman bisnis oleh staf TI, pada seluruh aplikasi yang dibuat dan dikembangkan sendiri oleh PT. XYZ.
3. 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:
   a. Memberikan peraturan atau kebijakan terhadap user dari pihak luar/ mitra perusahaan.
   b. Menjaga kebijakan pegawai untuk tetap dipaptuhi dan diawasi oleh atasan.
   c. Menjaga hubungan baik dengan mitra perusahaan
   d. Menerapkan pemberian sanksi terhadap pegawai yang melakukan kesalahan penginputan data
   e. Memberikan orientasi yang tepat kepada staf TI saat pelatihan
   f. Memberikan spesifikasi kebutuhan perangkat lunak kepada staf TI

Referensi:

[1] ISACA (2013). COBIT 5 for risk. United State of America: ISACA.
[2] ISACA. (2009). *The Risk IT Framework*. USA.
[3] International Standard. (2008). *ISO 27005: Information Technology-Security Techniques-Information Security Risk Managament.* United Kingdom: ISO/IEC.
[4] Darmawi, H. (2010). Manajemen Risiko. Jakarta: Bumi Aksara.
[5] Fahmi, I. (2010). Manajemen Risiko: Teori, Kasus, dan Solusi.
[6] Wahyunigtias, D. (2016). PERANCANGAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA KEY SUPPORTING PROCESS APO02, APO06 DAN APO08 DI DINAS KOMUNIKASI DAN INFORMATIKA (DISKOMINFO) PEMERINTAH KOTA BANDUNG MENGGUNAKAN FRAMEWORK COBIT 5.