Pengukuran Tingkat Risiko Terhadap Kapabilitas Tata Kelola Teknologi Informasi Berdasarkan Framework COBIT 5

Rumondang Martha Ambarita[1,*], Widya Cholil[1]

[1] Program Pascasarjana, Magister Teknik Informatika, Universitas Bina Darma, Palembang, Indonesia
Email: [1,*)]monambarita@outlook.com, [1]widya@binadarma.ac.id

Abstrak—Pengukuran tingkat kapabilitas tata kelola teknologi informasi dibutuhkan untuk mengetahui kondisi tata kelola teknologi informasi perusahaan saat ini. Penerapan tata kelola teknologi informasi tidak lepas dari kemungkinan adanya risiko teknologi informasi sehingga diperlukan sebuah *framework* yang dapat digunakan untuk mengukur tingkat kapabilitas tata kelola teknologi informasi, serta dapat digunakan sebagai pedoman pengukuran tingkat risiko dan perumusan mitigasi risiko. Tingkat kapabilitas teknologi informasi diukur berdasarkan metode *Process Assesment Model* (PAM) yang ada pada COBIT 5. Pengukuran tingkat kapabilitas dilakukan pada dua proses COBIT 5 yaitu EDM03 *Ensure Risk Optimization* dan APO12 *Manage Risk*. Identifikasi risiko dilakukan berdasarkan hasil pengukuran tingkat kapabilitas, di mana diperoleh empat *potential risk* yang kemudian diukur berdasarkan COBIT 5 *for Risk*. Hasil pengukuran tingkat risiko untuk *potential risk 1*, *potential risk 2*, dan *potential risk 4* berada pada level *medium*, sedangkan *potential risk 3* berada pada level *low*. Hasil yang diperoleh dari pengukuran tingkat risiko untuk keempat *potential risk* tersebut digunakan sebagai dasar untuk merumuskan rekomendasi langkah – langkah mitigasi risiko.

Kata Kunci: tata kelola teknologi informasi, kapabilitas tata kelola teknologi informasi, risiko teknologi informasi, mitigasi risiko, COBIT 5

Abstract—Capability level assessment of information technology governance is needed to determine the current condition of enterprise information technology governance. The implementation of information technology governance is inseparable from the possibility of information technology risk, so we need a framework that can be used to assess the level of information technology governance capability and also can be used as a guideline for assessing risk levels and formulating risk mitigation. The level of information technology capability is assessed based on the Process Assessment Model (PAM) method in COBIT 5. Capability level assessments are carried out in two COBIT 5 processes, which are EDM03 Ensure Risk Optimization and APO12 Manage Risk. Risk identification is carried out based on the assessment of the capability level, where four potential risks are obtained which then be assessed based on COBIT 5 for Risk. The results of risk assessments for potential risk 1, potential risk 2, and potential risk 4 are at a medium level, while potential risk 3 is at a low level. The results obtained from assessing the risk level for the four potential risks are used as the basis for formulating recommendations for risk mitigations.

Keywords: information technology governance, information technology governance capability, information technology risk, risk mitigation, COBIT 5

1. PENDAHULUAN

Kedewasaan sebuah perusahaan dapat diukur dari kemampuannya menyelaraskan antara kemajuan teknologi dengan strategi bisnis yang akan meningkatkan daya saing perusahaan. Salah satu upaya tersebut adalah dengan dilakukan penerapan tata kelola teknologi informasi. Tata kelola teknologi informasi bertujuan untuk memastikan bahwa harapan terhadap teknologi informasi perusahaan telah terpenuhi dan risiko-risiko teknologi informasi telah termitigasi [7]. Dalam penerapan tata kelola teknologi informasi, tidak jarang bahwa semua jenis perusahaan semakin terpapar berbagai jenis risiko teknologi informasi. Untuk mencegah kerugian atau efek negatif akibat risiko, risiko teknologi informasi perlu untuk diidentifikasi, dievaluasi, dianalisis, ditangani, dan dilaporkan dengan baik [15].

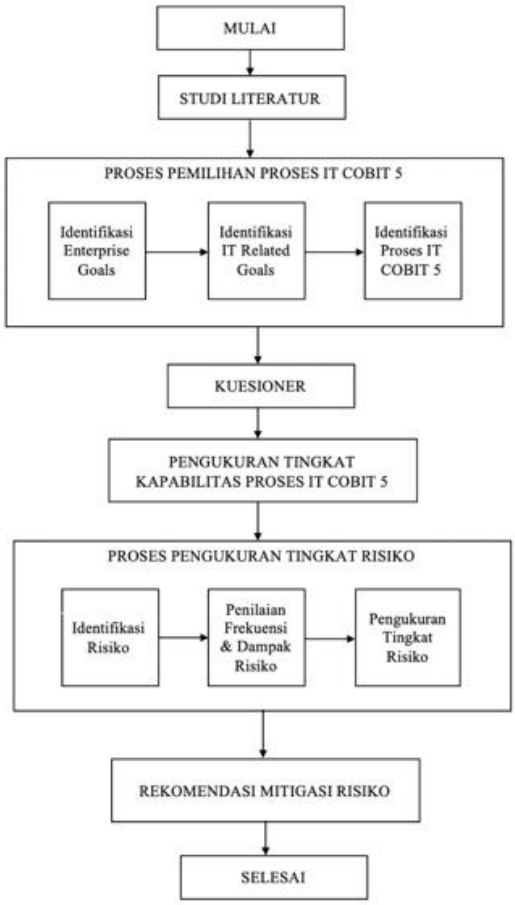
PT XYZ merupakan salah satu perusahaan yang telah menerapkan tata kelola teknologi informasi. Dengan kemampuan untuk memproses jumlah transaksi yang besar dan mengintegrasikan operasi bisnis yang ada di cabang-cabang di seluruh Indonesia, teknologi informasi merupakan *enabler* penting dalam mendukung pertumbuhan bisnis PT XYZ. Mengingat pentingnya peran teknologi informasi dalam perusahaan, maka perlu didukung oleh sebuah tata kelola teknologi informasi yang baik dalam mendukung dan memungkinkan tercapainya tujuan perusahaan. Namun, dalam penerapan tata kelola teknologi informasi tersebut tidak terlepas dari kemungkinan adanya risiko. Oleh karena itu, diperlukan suatu standar kontrol internasional yang dapat digunakan untuk pengukuran tata kelola teknologi informasi untuk menunjukkan kinerja tata kelola teknologi informasi dalam mencapai tujuan pengendalian, serta dapat digunakan untuk pengukuran risiko teknologi informasi dan memberikan pedoman dalam merumuskan langkah mitigasi risiko.

COBIT 5 menyediakan *framework* komprehensif yang menuntun perusahaan dalam mencapai tujuan perusahaan untuk tata kelola dan manajemen teknologi informasi perusahaan. *Framework* COBIT 5 menyediakan *Process Assessment Model* (PAM) yang mengacu pada ISO/IEC 15504 sebagai alat untuk mengukur kapabilitas sebuah tata keloa teknologi informasi, sehingga hasil yang didapatkan akan lebih akurat dan mewakilkan kebutuhan perusahaan. COBIT 5 juga menyediakan pedoman untuk mengukur tingkat level risiko teknologi informasi hingga bagaimana merumuskan langkah mitigasi terhadap risiko.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian dilakukan dengan menyesuaikan dengan tahapan – tahapan dalam pengukuran tingkat kapabilitas tata kelola teknologi informasi dan tahapan – tahapan dalam pengukuran tingkat risiko yang ada pada *framework* COBIT 5. Berikut merupakan kerangka pikir penelitian.



Gambar 1. Metodologi Penelitian

2.2 Pengukuran Tingkat Kapabilitas Proses COBIT 5

Kemampuan suatu perusahaan dalam menjalankan proses TI dinyatakan dalam tingkat kapabilitas (*capability level*). Pengukuran tingkat kapabilitas perusahaan pada COBIT 5 dilakukan menggunakan metode *Process Assessment Model* (PAM) yang mengacu pada ISO/IEC 15504. Pada COBIT 5 terdapat enam level kapabilitas yang harus dipenuhi. Kapabilitas tiap-tiap proses dinyatakan dalam tingkat proses yaitu *0-incomplete*, *1-performed*, *2-managed*, *3-established*, *4-predictable*, dan *5-optimizing*. Suatu proses dinyatakan telah mencapai tingkat kapabilitas tertentu jika atribut proses pada tingkat tersebut telah mencapai nilai L (*Largely Achieved*) atau F (*Fully Achieved*), serta telah mencapai nilai F (*Fully Achieved*) untuk seluruh atribut proses di tingkat yang lebih rendah.

Tabel 1. Tingkat Kapabilitas Proses

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
PA 5.2 – *Optimization* PA 5.1 – *Innovation*					L/F
PA 4.2 – *Control* PA 4.1 – *Measurement*				L/F	F
PA 3.2 – *Deployment* PA 3.1 – *Definition*			L/F	F	F
PA 2.2 – *Work Product* PA 2.1 – *Performance Management*		L/F	F	F	F
PA 1.1 – *Process Performance*	L/F	F	F	F	F

2.3 Analisis Risiko

Analisis risiko diawali dengan mengidentifikasi risiko yang mungkin terjadi. Setelah risiko telah diidentifikasi kemudian risiko tersebut akan dikategorikan ke dalam tiga tipe risiko berdasarkan COBIT 5 *for Risk*. Setelah dilakukan identifikasi tipe risiko, risiko kemudian dikelompokkan ke dalam 20 kategori risiko berdasarkan COBIT 5 *for Risk.*

2.4 Pengukuran Tingkat Risiko

Pengukuran tingkat risiko dilakukan berdasarkan standar penilaian risiko yang ada pada COBIT 5 *for Risk*. COBIT 5 *for Risk* merupakan sebuah panduan komprehensif yang dibuat untuk mengidentifikasi, menganalisis, dan merespon risiko [12]. Penilaian risiko berdasarkan COBIT 5 *for Risk* terbagi menjadi dua aspek yaitu frekuensi dan dampak. Penilaian frekuensi dan dampak memiliki skala peringkat 1 (*very low*), 2 (*low*), 3 (*moderate*), 4 (*high*), dan 5 (*very high*). Tabel 2 menjelaskan skala frekuensi risiko.

Tabel 2. Skala Penilaian Frekuensi Risiko

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
1	$N \leq 0{,}1$	*Very Low* • Kemungkinan skenario risiko terjadi sangat rendah. • Ada kemungkinan terjadinya risiko dalam keadaan yang sangat khusus (kemungkinan kecil). • Frekuensi kegagalan terjadi kurang dari sama dengan 0,1 kali dalam setahun.
2	$0{,}1 < N \leq 1$	*Low* • Kemungkinan skenario risiko terjadi rendah. • Risiko mungkin terjadi dalam beberapa keadaan. • Frekuensi kegagalan terjadi lebih dari 0,1 kali dan kurang dari sama dengan 1 kali dalam satu tahun.
3	$1 < N \leq 10$	*Moderate* • Kemungkinan skenario risiko terjadi cukup tinggi. • Risiko terjadi pada beberapa keadaan (kadang-kadang terjadi). • Frekuensi kegagalan terjadi lebih dari 1 dan kurang dari sama dengan 10 kali dalam satu tahun.
4	$10 < N \leq 100$	*High* • Kemungkinan skenario risiko terjadi tinggi. • Ada kemungkinan terjadinya risiko pada sebagian besar keadaan (mungkin terjadi).

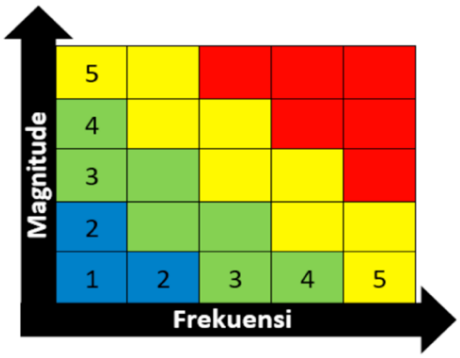
		• Frekuensi kegagalan terjadi lebih dari 10 kali dan kurang dari sama dengan 100 kali dalam satu tahun.
5	100 < N	*Very High* • Skenario risiko sangat tidak mungkin untuk dihindari. • Risiko cenderung terjadi pada sebagian besar keadaan (sering terjadi). • Frekuensi terjadinya kegagalan sangat tinggi, yaitu lebih dari 100 kali dalam satu tahun.

Dampak risiko terbagi ke dalam empat aspek dengan skala penilaian 1 sampai dengan 5. Skala ke-empat dampak risiko tersebut kemudian diambil rata-ratanya sehingga diperoleh satu nilai peringkat dampak. Skala penilaian untuk setiap peringkat dampak dapat dilihat pada Tabel 3.

Tabel 3. Skala Penilaian Dampak Risiko

Peringkat Dampak	Skala Penilaian Dampak			
	Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum
	Kerugian Pendapatan Selama Satu Tahun	Biaya Terkait Pengelolaan Kejadian yang Merugikan	Penurunan Kepuasan Pelanggan	Kepatuhan terhadap Peraturan
1	0,1% < I ≤ 1%	Rp 100rb < I ≤ Rp 1juta	0,5 < I ≤ 1	< Rp 1 juta
2	1% < I ≤ 3%	Rp 1juta < I ≤ Rp 10juta	1 < I ≤ 1,5	< Rp 10 juta
3	3% < I ≤ 5%	Rp 10juta < I ≤ Rp 100juta	1,5 < I ≤ 2	< Rp 100 juta
4	5% < I ≤ 10 %	Rp 100juta < I ≤ Rp 500juta	2 < I ≤ 2,5	< Rp 500 juta
5	10% < I	Rp 500juta < I	2,5 < I	> Rp 500 juta

Hasil yang diperoleh dari penilaian frekuensi dan dampak kemudian dipetakan ke dalam peta risiko berdasarkan nilai frekuensi dan dampak [12]. Berikut merupakan gambar peta risiko.



Gambar 2. Peta Risiko

2.5 Perumusan Langkah Mitigasi Risiko

Langkah – langkah mitigasi risiko dirumuskan berdasarkan pemetaan proses COBIT 5 terhadap kategori risiko yang ada pada COBIT 5 *for Risk*. Perumusan langkah – langkah mitigasi risiko berfokus pada *key management practices* yang ada pada proses – proses COBIT 5 hasil pemetaan dengan kategori risiko.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengukuran Tingkat Kapabilitas

Dalam penelitian ini, kuesioner digunakan sebagai alat untuk memperoleh data yang diperlukan dalam pengukuran tingkat kapabilitas proses COBIT 5. Kuesioner tersebut didesain dengan mengacu pada indikator setiap atribut proses yang ada pada metode *Process Assessment Model* (PAM). Berikut merupakan hasil pengukuran tingkat kapabilitas proses EDM03 berdasarkan hasil kuesioner.

Tabel 4. Pengukuran Tingkat Kapabilitas Proses EDM03

Rating Criteria by Responden	Pengukuran Tingkat Kapabilitas Proses EDM03										Level Kapabilitas
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5		
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2	
IT system analyst & system project staff	FALSE	F	L	L	L	L	L	L	L	P	2
Project Manager Core System	FALSE	F	L	L	L	L	L	P	P	P	2
IT Business Solution Dept. Head	FALSE	F	L	L	L	L	L	L	P	P	2
IT Application & Development Dept. Head	FALSE	F	L	L	L	L	L	P	P	P	2
IT Planning & Security Dept. Head	FALSE	F	L	L	L	L	L	L	P	P	2
IT Operation & Network Dept. Head	FALSE	F	F	F	L	L	L	P	P	P	3
IT Network Staff	FALSE	F	F	F	L	L	L	L	L	P	3
IT Application Support Supervisor	FALSE	F	L	L	L	L	L	P	P	P	2
Level kapabilitas proses EDM03											2

Berdasarkan hasil pengukuran di atas, nilai rata – rata pencapaian kapabilitas proses EDM03 ada pada level 2 (*managed*) di mana proses optimalisasi risiko telah diimplementasikan dan telah direncanakan, dimonitor, didokumentasikan, dan telah disesuaikan.

Berikut merupakan hasil pengukuran tingkat kapabilitas proses APO12 berdasarkan hasil kuesioner.

Tabel 5. Pengukuran Tingkat Kapabilitas Proses APO12

Rating Criteria by Responden	Pengukuran Tingkat Kapabilitas Proses APO12										Level Kapabilitas
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5		
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2	
IT system analyst & system project staff	FALSE	F	L	L	L	L	L	L	P	P	2
Project Manager Core System	FALSE	F	L	L	L	L	L	L	P	P	2
IT Business Solution Dept. Head	FALSE	F	L	L	L	L	L	P	P	P	2
IT Application & Development Dept. Head	FALSE	F	L	L	L	L	L	L	P	P	2
IT Planning & Security Dept. Head	FALSE	F	L	L	L	L	L	P	P	P	2
IT Operation & Network Dept. Head	FALSE	F	F	F	F	L	L	P	P	P	3
IT Network Staff	FALSE	F	F	F	L	L	L	P	P	P	3
IT Application Support Supervisor	FALSE	F	L	L	L	L	L	P	P	P	2
Level kapabilitas proses APO12											2

Berdasarkan hasil pengukuran di atas, nilai rata – rata pencapaian kapabilitas proses APO12 manajemen risiko ada pada level 2 (*managed*) di mana proses manajemen risiko telah diimplementasikan dan telah direncanakan, dimonitor, didokumentasikan, dan telah disesuaikan. *Work product* dari proses tersebut juga telah tepat pada sasaran dan telah terkontrol serta terpelihara dengan baik. Pengukuran tingkat kapabilitas tercapai pada

level 2 dengan skala L (*Largely Achieved*) di mana terdapat adanya bukti pendekatan sistematik dan adanya pencapaian yang signifikan dari atribut proses yang dinilai. Namun, terdapat adanya kelemahan terkait dengan atribut proses.

3.2 Hasil Analisis Risiko

Analisis risiko diawali dengan proses identifikasi risiko berdasarkan hasil kuesioner pengukuran tingkat kapabilitas tata kelola teknologi informasi. Dari hasil penyebaran kuesioner, diketahui PT XYZ belum memenuhi salah satu indikator kapabilitas level pada *process attribute 2.1 performance management*. Kekurangan tersebut kemudian dianalisis untuk mengetahui risiko yang berpotensi untuk terjadi.

Tabel 6. Contoh Proses Identifikasi *Potential Risk*

Indikator Kapabilitas Level	Potensi Risiko	Perincian Potensi Risiko	Keterangan	Penyebab
Process Attribute 2.1 Performance Management GP 2.1.3 Menyesuaikan kinerja proses. Tindakan diambil apabila kinerja yang telah direncanakan tidak tercapai. Tindakan termasuk identifikasi masalah kinerja proses dan penyesuaian rencana dan jadwal yang sesuai. GWP 4.0 Dokumen *quality record* harus memberikan rincian tindakan yang diambil ketika kinerja proses tidak tercapai.	Ketidaksiapan perusahaan dalam memenuhi kinerja proses ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).	Tidak ada *Business Continuity Plans* yang telah dirancang untuk mempertahankan keberlangsungan proses bisnis perusahaan ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).	Perusahaan tidak memiliki perencanaan keberlangsungan untuk menyingkapi dampak akibat terjadinya *special case* tersebut (pandemi COVID-19).	Karena risiko disebabkan oleh hal yang belum diprediksi oleh perusahaan, maka perusahaan belum memiliki SOP untuk mengantisipasi risiko tersebut.
		Spesifikasi infrastruktur teknologi informasi tidak mendukung perubahan proses bisnis.	Spesifikasi infrastruktur teknologi informasi terutama yang ada di cabang-cabang tidak mendukung perubahan proses bisnis.	Terjadinya pandemi COVID-19 menyebabkan perusahaan harus mengembangkan suatu sistem digital yang baru dan melakukan peningkatan terhadap sistem yang sudah ada. Oleh karena itu, diperlukan spesifikasi infrastruktur TI yang mampu mendukung perubahan proses bisnis.
		SDM perusahaan tidak dapat mengikuti perubahan yang terjadi.	SDM dari tim IT perusahaan tidak mampu mengikuti perubahan signifikan yang terjadi sehingga terjadi penurunan peforma SDM.	Pengembangan sistem digital yang baru dan peningkatan-peningkatan terhadap sistem yang sudah ada beberapa menuntut SDM IT perusahaan untuk memiliki *skill* tertentu. Tidak semua SDM pada

				tim IT perusahaan mampu menerima *skill* baru sehingga kegiatan operasional tidak berjalan dengan optimal.
		Perusahaan lebih rentan akan ancaman keamanan informasi.	Perubahan pada proses bisnis perusahaan menyebabkan perusahaan menjadi lebih rentan akan ancaman keamanan informasi.	Perubahan proses bisnis yang sebelumnya prosedur proses penginputan dokumen *customer* dilakukan oleh kantor-kantor cabang saat ini, telah dilakukan secara langsung oleh *customer* di mana *customer* dapat mengakses sistem untuk menginput data. Hal ini dikarenakan adanya himbauan pemerintah untuk diberlakukannya *social distancing* sehingga *customer* tidak datang langsung ke kantor cabang untuk memberikan persyaratan dokumen.

Setelah *potential risk* telah terdefinisi, *potential risk* tersebut kemudian akan dikelompokkan ke dalam kategori skenario risiko dan tipe risiko yang ada dalam COBIT 5 *for Risk*.

Tabel 7. Contoh Proses Identifikasi Tipe Risiko

No	*Potential Risk*	*Risk Type*		
		IT Benefit/Value Enablement Risk	*IT Programme and Project Delivery Risk*	*IT Operations and Service Delivery Risk*
1	Tidak ada *Business Continuity Plans* yang telah dirancang untuk mempertahankan keberlangsungan proses bisnis perusahaan ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).	S	P	P
2	Spesifikasi infrastruktur teknologi informasi tidak mendukung perubahan proses bisnis.	P	P	P
3	SDM perusahaan tidak dapat mengikuti perubahan yang terjadi.	-	-	P
4	Perusahaan lebih rentan akan ancaman keamanan informasi.	-	-	P

Nilai ‘P’ menunjukan kecocokan primer (terkait langsung), nilai ‘S’ mewakili kecocokan sekunder (tidak terkait langsung). Sedangkan nilai yang kosong menunjukan tidak ada keterkaitan risiko dengan tipe risiko.

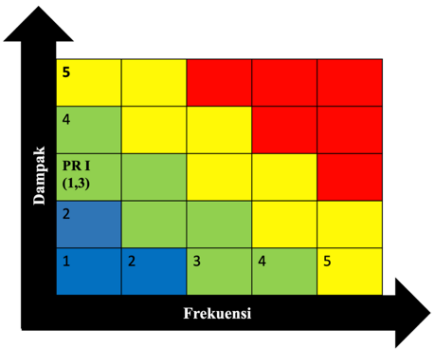
Setelah dilakukan identifikasi tipe risiko, *potential risk* kemudian akan dikelompokan ke dalam kategori skenario risiko. Identifikasi tersebut bertujuan untuk digunakan sebagai dasar dalam proses perumusan mitigasi risiko. Dalam COBIT 5 *for Risk*, risiko dapat dikelompokan dalam 20 kategori skenario risiko.

Tabel 8. Contoh Proses Identifikasi Skenario Risiko

No	Kategori Risiko TI	ID Risiko	Risiko
1	*Acts of nature*	AON001	Tidak ada *Business Continuity Plans* yang telah dirancang untuk mempertahankan keberlangsungan proses bisnis perusahaan ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).
2	*Infrastructure (hardware, operating system and controlling technology) (selection/implementation, operations and decommissioning)*	IFS001	Spesifikasi infrastruktur teknologi informasi tidak mendukung perubahan proses bisnis.
3	*IT expertise and skills*	IES001	SDM perusahaan tidak dapat mengikuti perubahan yang terjadi.
4	*Information (data breach: damage, leakage and access)*	INF001	Perusahaan lebih rentan akan ancaman keamanan informasi.

3.3 Hasil Pengukuran Tingkat Risiko

Risiko yang telah didefinisikan akan diukur berdasarkan perkiraan frekuensi dan dampaknya dalam perusahaan. Pengukuran risiko berdasarkan COBIT 5 *for Risk* terbagi menjadi dua aspek yaitu frekuensi dan dampak. Penilaian rata-rata dampak risiko mengikuti aturan pembulatan desimal. Nilai rata-rata dampak risiko yang diperoleh bernilai di bawah 0.5, maka akan dibulatkan ke angka di bawah, sedangkan apabila nilai rata-rata dampak risiko mencapai di atas 0.5, maka akan dibulatkan ke angka di atas. Nilai frekuensi dan dampak risiko yang telah diperoleh kemudian akan dipetakan ke dalam peta level risiko sebagaimana yang digambarkan pada gambar di bawah ini.



Gambar 3. Contoh Hasil Pemetaan Frekuensi dan Dampak *Potential Risk 1*

Berdasarkan hasil pemetaan dampak dan frekuensi risiko yang telah digambarkan pada Gambar 2, diketahui bahwa level untuk *potential risk* nomor satu berada pada warna hijau yang menunjukan risiko tersebut berada pada level *medium*.

Tabel 9. Contoh Hasil Proses Pengukuran Tingkat Risiko

No	Kategori Risiko TI	ID Risiko	Risiko	Frekuensi	Rata-rata Peringkat Dampak	(Frekuensi, Dampak)	Level Risiko
1	*Acts of nature*	AON001	Tidak ada *Business Continuity Plans* yang telah dirancang untuk mempertahankan keberlangsungan proses bisnis perusahaan ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).	1	3,33	(1,3)	*Medium*
2	*Infrastructure*	IFS001	Spesifikasi infrastruktur teknologi informasi tidak mendukung perubahan proses bisnis.	1	3	(1,3)	*Medium*
3	*IT expertise and skills*	IES001	SDM perusahaan tidak dapat mengikuti perubahan yang terjadi.	1	2	(1,2)	*Low*
4	*Information*	INF001	Perusahaan lebih rentan akan ancaman informasi.	1	2,6	(1,3)	*Medium*

3.4 Perumusan Mitigasi Risiko

Langkah – langkah mitigasi risiko dirumuskan berdasarkan hasil pemetaan skenario risiko dengan proses – proses TI yang ada di COBIT 5. Langkah mitigasi risiko dirumuskan berdasarkan *key management practices* yang sesuai yang ada pada proses – proses TI COBIT 5 yang telah dipetakan. *Key management practices* dari proses-proses tersebut tidak seluruhnya diambil untuk dijadikan dasar dalam perumusan langkah mitigasi risiko, melainkan hanya *key management practices* yang relevan dengan risiko yang akan dipilih.

Tabel 10. Contoh Hasil Perumusan Langkah Mitigasi

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Proses COBIT 5	Langkah – langkah Mitigasi
1	*Acts of nature*	AON001	Tidak ada *Business Continuity Plans* yang telah dirancang untuk mempertahankan keberlangsungan proses bisnis perusahaan ketika terjadi *special case* yang tidak terprediksi (pandemi COVID-19).	*Medium*	DSS04 *Manage Continuity*	DSS04.01 Menentukan kebijakan, tujuan, dan ruang lingkup bisnis yang berkelanjutan • Mendefinisikan dan mendokumentasikan tujuan, serta ruang lingkup kebijakan minimum yang telah disepakati untuk kelangsungan bisnis dan menanamkan kebutuhan untuk perencanaan kesinambungan dalam perusahaan. DSS04.02 Mempertahankan strategi kontinuitas • Menilai kemungkinan ancaman yang dapat menyebabkan hilangnya kelangsungan bisnis

						dan mengidentifikasi langkah – langkah yang akan mengurangi kemungkinan dan dampak melalui pencegahan yang lebih baik dan peningkatan ketahanan. DSS04.03 Mengembangkan dan menerapkan respon kelangsungan bisnis • Mengembangkan dan memelihara rencana kesinambungan bisnis operasional yang berisi prosedur yang harus diikuti untuk memungkinkan kelanjutan operasi proses bisnis penting dan pengaturan pemrosesan sementara, termasuk hubungan ke rencana penyedia layanan yang dialihdayakan.
2	*Infrastructure*	IFS001	Spesifikasi infrastruktur teknologi informasi tidak mendukung perubahan proses bisnis.	*Medium*	APO02 *Manage Strategy*	APO02.04 Melakukan analisis kesenjangan • Menilai dampak akibat adanya perubahan potensial pada proses bisnis dan model operasi TI terhadap infrastruktur TI.
					BAI03 *Manage Solutions Identification and Build*	BAI03.02 Merancang komponen-komponen solusi terperinci • Mengevaluasi secara proaktif kelemahan desain infrastruktur TI perusahaan untuk mengetahui potensi kekurangannya. BAI03.04 Mendapatkan komponen solusi • Membuat perencanaan untuk akuisisi komponen solusi dengan cara mempertimbangkan kemungkinan di masa depan untuk adanya penambahan kapasitas, biaya transisi, risiko yang mungkin terjadi, dan kemungkinan adanya peningkatan.
3	*IT expertise and skills*	IES001	SDM perusahaan tidak dapat mengikuti perubahan yang terjadi.	*Low*	APO07 *Manage Human Resource*	APO07.01 Mempertahankan staf yang memadai dan tepat • Mengevaluasi persyaratan kepegawaian secara teratur atau pada perubahan besar untuk memastikan bahwa fungsi TI memiliki sumber daya yang cukup untuk

						mendukung tujuan dan sasaran perusahaan secara memadai dan tepat. APO07.03 Mempertahankan *skill* dan kompetensi personel • Menentukan keterampilan dan kompetensi yang dibutuhkan dan yang saat ini tersedia dari sumber daya internal dan eksternal untuk mencapai tujuan perusahaan, TI, dan proses. APO07.04 Mengevaluasi performa kinerja pegawai. • Menetapkan tujuan individu setiap pegawai yang selaras dengan tujuan proses yang relevan sehingga ada kontribusi yang jelas untuk tujuan TI dan perusahaan.
4	*Information*	INF001	Perusahaan lebih rentan akan ancaman keamanan informasi.	*Medium*	DSS05 *Manage Security Services*	DSS05.01 Perlindungan dari malware • Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru. DSS05.02 Mengelola jaringan dan keamanan konektivitas • Menerapkan mekanisme penyaringan jaringan, seperti *firewall* dan perangkat lunak pendeteksi intrusi, dengan kebijakan yang sesuai untuk mengontrol lalu lintas masuk dan keluar. DSS05.03 Mengelola keamanan *endpoint* • Menerapkan pemfilteran lalu lintas jaringan pada perangkat *endpoint.*

4. KESIMPULAN

Proses pengukuran tingkat kapabilitas tata kelola teknologi informasi pada penelitian ini dilakukan berdasarkan *framework* COBIT 5 dengan model pengukuran yang digunakan yaitu *Process Assesment Model* (PAM). Proses COBIT 5 yang akan diukur dalam penelitian merupakan proses yang berkaitan dengan risiko teknologi informasi yaitu EDM03 *Ensure Risk Optimization* dan APO12 *Manage Risk*. Dari hasil pengukuran yang dilakukan, diperoleh tingkat kapabilitas tata kelola teknologi informasi untuk proses EDM03 *Ensure Risk Optimization* dan APO12 *Manage Risk* keduanya berada pada level 2 (*managed*).

Proses pengukuran tingkat risiko dilakukan berdasarkan metode pengukuran yang ada pada COBIT 5 *for Risk*. Pengukuran tingkat risiko diawali dengan proses identifikasi risko. Dari proses tersebut diperoleh empat risiko yang kemudian diklasifikasikan ke dalam tipe risiko dan kategori risiko yang ada pada COBIT 5 *for Risk*. Kemudian dilakukan proses pengukuran tingkat risiko berdasarkan frekuensi dan dampaknya. Nilai frekuensi dan

dampak risiko kemudian dipetakan ke dalam peta risiko yang ada pada COBIT 5 *for Risk*. Dari hasil pemetaan tersebut diperoleh level risiko *potential risk 1* berada pada level *medium*, *potential risk 2* berada pada level *medium*, *potential risk 3* berada pada level *low*, dan *potential risk 4* berada pada level *medium*. Perumusan langkah – langkah mitigasi diperoleh dari analisis *key management practice* yang relevan dengan risiko.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada pihak – pihak yang telah terlibat dan mendukung penelitian ini.

REFERENCES

[1] M. K. S. Firdaus, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5," *Skripsi*, Program Studi Sistem Informasi, Univ. Islam Negeri Syarif Hidayatullah, Jakarta, 2018.

[2] D. R. Indah, et. all., "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk," *The 1st International Conference on Computer Science and Engineering*, 2014.

[3] ISACA, "COBIT 5 Enabling Process," Illinois, 2012.

[4] ISACA, "COBIT 5 Implementation," Illinois, 2013.

[5] ISACA, "COBIT 5 for Risk," Illinois, 2013.

[6] ISACA, "Process Assesment Model (PAM): Using COBIT 5," Illinois, 2013.

[7] IT Governance Institute (ITGI), "Board Briefing on IT Governance," Illinois, 2003.

[8] M. S. Lamato, A. Setyanto, and A. Nasiri, "Evaluasi Tingkat Kematangan Tata Kelola Infrastruktur IT Menggunakan COBIT 5," *Jurnal Sistem Informasi dan Teknologi Informasi*, Vol.8, No.2, 2019.

[9] Megawati and A. Syntia, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5.0," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, Vol.4, No.2, Hal.118-122, 2018.

[10] C. U. Putri, "Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 pada Helpdesk Subdirektorat Layanan Teknologi dan Sistem Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember," *Tugas Akhir*, Program Studi Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, 2017.

[11] R. E. Putri, "Penilaian Kapabilitas Proses Tata Kelola TI Berdasarkan Proses DSS01 pada Framework COBIT 5," *Jurnal CoreIT*, Vol.2, No.1, 2016.

[12] S. P. Ramadhani, A. Herdiyanti, and H. M. Astuti, "Pembuatan Perangkat Audit Berbasis Risiko Berdasarkan COBIT 5 dan Service Desk Standard pada Service Desk," *Jurnal Sisfo*, Vol.07, No.01, 2017.

[13] D. Rohandy, "Evaluasi Tata Kelola Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5: Studi Kasus PT Nata Solusi Pratama," *Karya Akhir*, Program Studi Magister Teknologi Informasi, Universitas Indonesia, Jakarta, 2015.

[14] G. Waluyan and A. D. Manuputty, "Evaluasi Kinerja Tata Kelola TI Terhadap Penerapan Sistem Informsi Starlick Framework COBIT 5 (Studi Kasus: PT. Telekomunikasi Indonesia, Tbk Semarang), *TEKNOSI*, Vol.02, No.03, 2016.

[15] S. A. Wulandari, et.all., "Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service," *The Fifth Information Systems International Conference 2019*, 2019.