JURNAL SISTEM INFORMASI DAN TENOLOGI

http://www.jurnal.umk.ac.id/sitech

MANAJEMEN RISIKO TI ISO 31000 DENGAN COBIT 5 DAN FMEA (PT. XYZ)

Finandy Ari Hardianto[1], Yogantara Setya Dharmawan[2]

[1,2] *Program Studi Sistem Informasi, Universitas Internasional Semen Indonesia*

Article Info:
Dikirim: 26 Agustus 2021
Direvisi: 25 Desember 2021
Diterima: 30 Desember 2021
Tersedia Online: 30 Desember 2021

Penulis Korespondensi:
Finandy Ari Hardianto
Sistem Informasi,
Universitas Internasional Semen Indonesia, Gresik, Indonesia
Email: nandyari13@gmail.com

Abstrak: *PT. XYZ adalah sebuah korporasi penyedia layanan Internet Service Provider atau yang dikenal dengan istilah ISP dan jasa kebutuhan layanan TI lainnya yang sedang mengembangankan bisnis nya di Kota Balikpapan, Kalimantan Timur. Adapun proses bisnis utama dari PT. XYZ adalah membantu client dalam merancang bangun serta memberikan solusi terbaik bagi kebutuhan IT, komunikasi dan jaringan dalam mendukung proses bisnis. Belum diterapkannya pengelolaan risiko pada PT. XYZ dianggap dapat menurunkan performa korporasi apabila tidak cepat diselesaikan. Merujuk pada studi permasalahan sebelumnya, studi ini akan mengkaji terkait manajemen risiko IT dengan framework COBIT 5 for risk dan FMEA berasas ISO 31000. Dimana COBIT 5 for risk memiliki kelebihan dalam mengidentifikasi risiko, proses pengkajian risiko melalui FMEA serta berasas pada ISO 31000 yang diterapkan oleh sebagian besar korporasi. Studi ini menghasilkan sebuah padanan atau ilustrasi terkait alur pengelolaan risiko dimana terdiri dari penggabungan beberapa framework pengelolaan risiko. Selanjutnya studi ini dapat berkontribusi sebagai acuan korporasi dalam pengelolaan risiko.*

Kata kunci: *IT; pengelolaan risiko; COBIT 5; FMEA; ISO 31000.*

Abstract: *PT. XYZ is an ISP service provider (Internet Service Providers) corporation and other IT service needs that are growing rapidly in balikpapan city, East Kalimantan. The main business process of PT. XYZ is assisting clients in designing builds and providing the best solutions for IT, communication and network needs in support of business processes. But at the moment PT. XYZ has not implemented risk management, so it is feared that it could reduce the company's performance if not addressed immediately. Based on the case study above, this research was made on IT risk management using COBIT 5 for risk and FMEA framework based on ISO 31000. With each of the advantages of the framework offered such as COBIT 5 for risk that excels in risk identification, FMEA in the process of risk analysis, and ISO 31000 which is the most widely used risk management standard in various companies. This study showed an equivalent or illustration related to the flow of risk management which consists of combining several risk management frameworks. Furthermore, this study can contribute as a reference for corporations in risk management.*

Keywords: *IT; risk management; COBIT 5; FMEA; ISO 31000.*

1. PENDAHULUAN

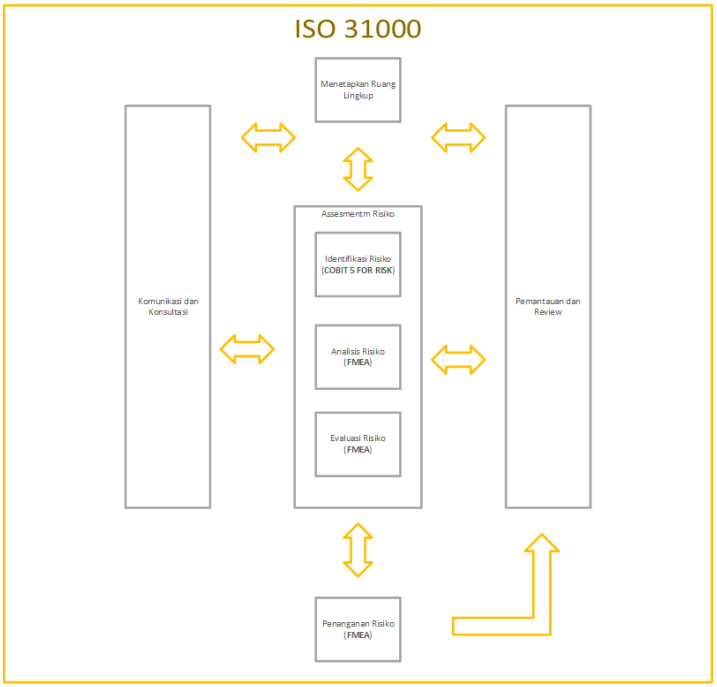
PT. XYZ berdiri pada Bulan Juni tahun 2005 merupakan sebuah korporasi penyedia layanan Internet Service Provider atau yang dikenal dengan istilah ISP dan jasa kebutuhan layanan TI lainnya yang sedang mengembangankan bisnis nya di Kota Balikpapan, Kalimantan Timur. COBIT 5 *for risk* mempunyai pandangan terhadap pengelolaan risiko dalam melakukan identifikasi risiko, kajian risiko, dan sistem untuk bereakai atas risiko. Dua domain diperlukan atas pandangan ini yaitu EDM 03 (*Ensure Risk Optimization*) dan APO 12 (*Manage Risk*) [1]. FMEA adalah sebuah metode sistematis yang digunakan untuk merekognisi serta meminimalisir kegagalan yang ada (*failure mode*). FMEA juga diterapkan untuk mengetahui titik awal dan pusat yang menyebabkan sebuah permasalahan [2]. Secara umum ISO 31000 ialah sebuah padanan pengaplikasian pengelolaan risiko meliputi 3 bagian yaitu: dasar, struktur kerja, dan alur. Penggunaan ISO 31000 bertujuan melindungi nilai atau proses di dalam korporasi dengan cara pengelolaan risiko, pendukung keputusan, dan pencapaian performa proses bisnis. ISO 31000 tentunya mempunyai kelebihan yaitu mudah digunakan,ruang lingkup ISO 31000 lebih general, dan ISO 31000 digunakan oleh banyak negara [3]. Pada penelitian, adapun acuan teknik yang diaplikasikan dalam kajian pengelolaan resiko IT yaitu menggunakan COBIT 5 *for risk* (*Control Objective for IT and Related Technology*) dan FMEA (*Failure Mode and Effect Analysis*) berbasis ISO 31000. COBIT 5 *for risk* dipilih untuk mendukung pengelolaan risiko IT dengan menghadirkan framework untuk mengatur keselarasan IT dengan proses bisnis korporasi. Namun COBIT 5 *for risk* hanya dapat memberikan petunjuk pengelolaan risiko dan tidak memberikan petunjuk implementasi praktik pengelolaan risiko, maka acuan untuk mendukung COBIT 5 *for risk* yaitu dengan menggunakan FMEA [4]. Dari proses gabungan metode tersebut diharapkan bisa mendukung keseluruhan proses selama studi kajian pengelolaan risiko IT.

2. METODOLOGI PENELITIAN

Studi ini mengambil tema pengelolaan risiko yang terfokus dari identifikasi hingga mitigasi risiko. Studi ini dilakukan dengan pendekatan kualitatif, yaitu menekankan pada aspek pemahaman terkait penggunaan studi permasalahan berupa sebuah alur yang terstruktur dalam mengkaji sebuah permasalahan, pengumpulan data, kajian data, dan laporan hasilnya. Pendekatan kualitatif ialah langkah studi untuk memperoleh data dalam bentuk kalimat tulis atau lisan bersumber dari responden atau aktivitas yang sedang dikaji [5].

Adapun permodelan framework yang digunakan ialah COBIT 5 for risk dan FMEA berasas ISO 31000. Berdasarkan penelitian maupun literatur yang telah diuji, usaha untuk menggabungkan beberapa *framework* atau kerangka kerja dipandang dapat memberikan gambaran yang paling efisien dan mudah dimengerti bagi korporasi khususnya PT. XYZ jika ingin mencoba menggunakan gabungan *framework* tersebut.

Dari proses-proses pengelolaan risiko diatas, dapat disimpulkan hasil kombinasi dari COBIT 5 *for risk*, ISO 31000, dan FMEA yang digambarkan pada sebagai berikut ini:



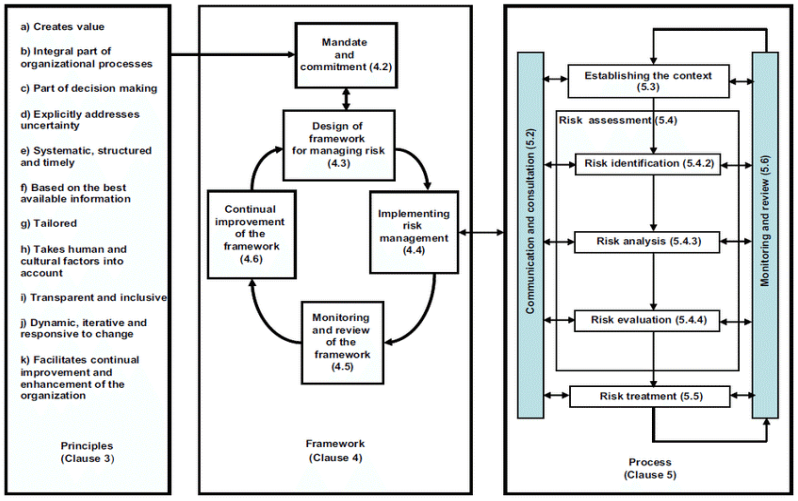
Gambar 1. Proses Manajemen Risiko Pada Penelitian Ini

Penggunaan tiap framework disesuaikan dengan kelebihan yang dimiliki. Adapun penjelasan mengenai perencanaan pada setiap proses pengelolaan risiko dari gambar diatas pada studi ini meliputi:

1) Menetapkan Ruang Lingkup
   Langkah ini diterapkan pada tahap awal pengelolaan risiko. Tahap ini bertujuan untuk penentuan ruang lingkup aktifitas proses pengelolaan risiko oleh sebuah korporasi dimana dalam pelaksanaanya akan diterapkan oleh bagian kerja, proses bisnis, dan juga lingkungan praktik yang tidak sama.
2) Proses Identifikasi Risiko
   Penggunaan risk scenario yang berasal dari COBIT 5 *for risk* dalam pelaksanaanya untuk memperoleh data dengan *risk scenario* (list risiko positif dan negative) yang telah dikategorikan dalam 20 kategori identifikasi risiko TI [6]
3) Proses Kajian Risiko
   Proses penilaian risiko yang sudah masuk dalam list alur identifikasi risiko. Dalam proses ini, FMEA yang terdiri dari alur kajian kualitatif dan kuantitatif. Hal ini berbeda dari COBIT 5 *for risk* yang mempunyai alur kajian tetapi tidak didukung dengan pernyataan yang menjelaskan lebih mendalam terkait teknik yang akan diterapkan dalam mengkaji risiko.
   Kajian yang terlebih dahulu adalah menentukan nilai dari masing-masing risiko yang terdiri dari besaran dampak, kemungkinan, dan deteksi. Selanjutnya dengan menghitung *risk priority number* untuk memperoleh besaran risiko.
4) Evaluasi Risiko
   Selanjutnya dalam evaluasi risiko, memuat proses yang menentukan bagaimana penanganan risiko yang akan diterapkan untuk melihat risiko yang perlu diperhatikan dan diperbaiki lebih mendalam. Pemetaan diterapkan pada tahap ini atas risiko-risiko yang terjadi dengan menggunakan status seperti segera ditangani.
5) Perencanaan dan Penanganan Risiko
   Setelah tahap evaluasi risiko atau pemetaan risiko selesai, maka tahap selanjutnya yaitu perencanaan dan penanganan risiko. Tahap perencanaan dan penanganan risiko merupakan langkah-langkah atau daftar untuk membuat keputusan penanganan terhadap risiko dan membuat mitigasi dari risiko yang telah diketahui atau dikajian.
6) Komunikasi dan Konsultasi
   Diperlukannya komunikasi dan konsultasi atas pengelolaan risiko dengan tujuan memberikan transparansi atas proses yang berjalan sehingga lebih tepat dalam penerapannya dan dapat dipertanggung jawabkan. Tentunya pada tahap ini harus dilaksanakan dengan pemangku kepentingan.
7) *Monitoring and Review*
   Dalam proses pengelolaan risiko diharuskan adanya pengawasan, agar implementasi dari proses pengelolaan risiko dapat berjalan dengan baik. Untuk tahapan ini harus dilakukan pada setiap proses pengelolaan risiko, dimulai dari perencanaan, pengumpulan data/informasi, kajian data, evaluasi dari yang telah diketahui, hingga pemberian rekomendasi mitigasi.

2.1 ISO 31000

ISO (*International Standard Organization*) ialah organisasi terkait standarisasi internasional yang diakui dunia. ISO 31000 ialah badan standar internasional yang dibuat untuk melahirkan dasar dan acuan yang sistematis serta terstruktur untuk penerapan pengelolaan risiko [7]. Sedangkan ISO 31000 merupakan sebuah standar yang digunakan dalam pedoman yang dipakai oleh korporasi ataupun organisasi dalam mengelola pengelolaan risiko. ISO 31000 menyediakan panduan secara umum, maksudnya adalah untuk mendukung kesamaan pengelolaan risiko pada organisasi maupun korporasi.



Gambar 2. Hubungan Antara Prinsip, Kerangka Kerja dan Alur Proses Dalam ISO 31000

Didalam ISO 31000 terdapat sebuah hubungan yang saling bergantung yang diantaranya seperti:
1) *Principles* yaitu prinsip-prinsip yang memegang komitmen dalam menjalankan proses pengelolaan risiko.
2) *Framework* yaitu kerangka kerja yang harus direncanakan dalam menjalankan pengelolaan risiko kedepannya.
3) *Process* yaitu tahapan dalam menerapkan atau menjalankan pengelolaan risiko di organisasi maupun korporasi[8].

2.2 COBIT 5 FOR RISK

Control Objectives for Information and Related Technologies atau yang dikenal dengan COBIT ialah struktur kerja atas landasan yang tersusun dari dokumentasi yang telah diterapkan secara baik serta acuan langkah terkait penerapan *IT governance*. Strukur kerja COBIT Berguna bagi auditor, pihak pengelolaan, dan penggunanya yang menghubungkan celah antara risiko bisnis, pengawasan dan permasalahan teknis [9]. COBIT 5 *for risk* berfokus pada pengembangan pengelolaan risiko terkait IT. Tujuan utama dari proses pengelolaan risiko menggunakan COBIT 5 *for risk* adalah untuk memberikan panduan tentang pengembangan risiko terkait teknologi informasi. Potensi ancaman dan risiko yang dapat menyebabkan peristiwa kerugian harus dipertimbangkan dengan sangat baik.

2.3 FMEA

Failure Mode and Effect Analysis adalah suatu metode kajian dari pengelolaan risiko yang bertujuan untuk proses pencarian, identifikasi, dan penghilangan peluang kegagalan atau eror terkait permasalahan yang ada meliputi sistem, desain, alur, atau jasa sebelum risiko tersebut menjadi lebih parah [10].

Tujuan diterapkan FMEA meliputi [11] :
1) Merekognisi risiko atau kegagalan dan tingkat dampak yang ditimbulkan.
2) Merekognisi ciri khusus kritis dari tiap risiko yang diketahui.
3) Mengurutkan daftar-daftar risiko yang potensial.
4) Membantu ketercapaian tujuan user terkait pencegahan munculnya risiko.

FMEA mempunyai variable kajian untuk merekognisi setiap kegagalan yang ada, yaitu seperti dibawah ini:
1) (*Occurrence*) Seberapa sering kegagalan yang terjadi.
2) (*Severity*) Merupakan dampak yang dihasilkan dari kegagalan yang terjadi.
3) (*Detection*) Merupakan kemampuan mendeteksi kegagalan sebelum kegagalan itu terjadi.

Tahapan dalam pembuatan FMEA meliputi [12]:
1) Identifikasi risk event. Identifikasi risiko melalui wawancara atau pengkajian.
2) Penilaian peluang, dampak, dan deteksi. Dengan adanya nilai dari masing-masing tolok ukur tersebut, sehingga mengasilkan RPN (*risk priority number*) yang berupa level prioritas risiko.
3) Penilaian ulang RPN dan penentuan nilai limit RPN.
4) Risiko dengan nilai RPN lebih dari nilai limit harus lebih didahulukan
5) Pembuatan rencana respon untuk daftar risiko seperti *avoid, mitigate, acceptance and transfer*.
6) Pengevaluasian kembali risiko dan RPN.

Risiko-risiko yang telah diidentifikasi sebelumnya, kemudian akan dinilai yang mengacu pada teknik FMEA dengan pengukuran *Severity*, *Occurrence*, dan *Detection* level untuk menghasilkan nilai RPN (*Risk Probability Number*)

3. HASIL DAN PEMBAHASAN

3.1 Risk Identification

Tahap identifikasi risiko pada penelitian ini akan menggunakan COBIT 5 *for risk*. Identifikasi risiko merupakan proses untuk menemukan setiap risiko yang mempunyai potensi dapat memperlambat maupun mengganggu dari proses bisnis dan capaian tujuan korporasi PT. XYZ yang berhubungan dengan teknologi informasi.

Mengacu kepada daftar kategori identifikasi risiko pada COBIT 5 *for risk*, maka dibuatlah daftar temuan identifikasi risiko atau risk scenario pada korporasi PT. XYZ. Adapun daftar temuan identifikasi risiko berdasarkan hasil dari observasi dan wawancara yang berhubungan dengan TI.

Tabel *risk identification* dibawah ini berisi daftar-daftar temuan.identifikasi risiko teknologi informasi yang ada pada korporasi PT.XYZ. Berikut merupakan hasil temuan identifikasi risiko pada korporasi PT. XYZ:

Tabel 1 ***Risk Identification***

No	***Kategori Risiko***	***Tipe Risiko***			***Skenario Risiko***	
		IT benefit / value enablement risk	***IT programme and project delivery risk***	***IT operations and service delivery risk***	***Risiko Negatif***	***Risiko Positif***
1.	*IT investment decision making*	P	S	S	Tidak adanya beberapa pihak seperti direksi atau stakeholder dalam rapat pengambilan keputusan pengelolaan investasi TI	Terdapatnya kerja sama antar stakeholder dalam rapat pengambilan keputusan investasi TI
2.		P	S	S	Kesalahan dalam pemilihan perangkat keras untuk investasi TI	Adanya kajian yang baik dalam melakukan investasi TI untuk kebutuhan korporasi
3.	*IT expertise and skills*	S	P	P	Tidak adanya transfer pengetahuan dari staff yang mengundurkan diri ke staff baru	Terdapat transfer pengetahuan dari staff yang mengundurkan diri ke staff baru
4.		P	S	P	Tidak adanya *training skill* untuk meningkatkan *skill* staff	Adanya *training skill* untuk meningkatkan *skill* staff
5.		P	S	P	Kurangnya skill staff dalam mendukung proses bisnis korporasi	Dengan adanya skill staff yang mumpuni, dapat mengerjakan jobdesk dengan baik
6.		P	S	S	Ketidakmampuan korporasi dalam merekrut IT staff yang mumpuni	Dengan perekrutan staff IT yang mumpuni, dapat mendukung proses bisnis korporasi
7.	*Staff operations (human error and malicious intent)*	S	P	P	Kerusakan pada peralatan IT yang diakibatkan oleh staff	Peralatan IT dijaga dengan baik
8.		S	S	P	Pencurian data korporasi oleh staff	Adanya alat Deteksi dalam menjaga data korporasi

No	*Kategori Risiko*	*Tipe Risiko*			*Skenario Risiko*	
		IT benefit / value enablement risk	***IT programme and project delivery risk***	***IT operations and service delivery risk***	***Risiko Negatif***	***Risiko Positif***
9.		S	S	P	Kesalahan dalam input data oleh staff	Kesesuaian dalam input data oleh staff
10.		S	S	P	Adanya kesalahan *troubleshooting* oleh staff	Staff korporasi mempunyai etos kerja dan profesionalitas yang baik
11.		S	P	P	Perangkat mikrotik sengaja dikonfigurasi tidak sesuai oleh staff	Seluruh perangkat keras IT telah dikonfigurasi dengan ketentuan
12.	*Information (data breach: damage, leakage and access)*	S	S	P	Adanya data-data korporasi baik di server maupun laptop dalam kondisi *corrupted*	Terdapat prosedur backup data baik di server ataupun di laptop
13.		P	S	P	Informasi yang sensitif telah tersebar luas	Para staff korporasi telah menjaga informasi korporasi
14.		P	S	P	Data-data korporasi diakses oleh pihak yang tidak berkepentingan	Adanya pengawasan dalam sistem jaringan, maka setiap akses data akan tercatat
15.	*Infrastructure*	S	S	P	Jaringan tidak bisa berjalan dengan baik ketika terjadi lonjakan volume lalu lintas data	Melakukan testing secara maksimal agar sistem dapat bertahan dengan baik
16.		S	P	P	Spesifikasi mikrotik tidak sesuai dengan yang diharapkan	Spesifikasi hardware sesuai dengan yang diharapkan
17.		S	S	P	Terputusnya jaringan intranet	Staff korporasi yang selalu siap ketika dibutuhkan
18.		S	S	P	Server sering cepat panas	Adanya mesin pendingin yang berada dalam ruangan server
19.	*Software*	S	P	P	Staff tidak bisa adaptasi dalam menggunakan software yang terbaru	Staff mampu adaptasi dengan cepat dalam menggunakan

No	*Kategori Risiko*	*Tipe Risiko*			*Skenario Risiko*	
		IT benefit / value enablement risk	*IT programme and project delivery risk*	*IT operations and service delivery risk*	*Risiko Negatif*	*Risiko Positif*
						software yang terbaru

Keterangan:
(P)*Primary* : Berarti terdapat risiko yang berhubungan dengan tipe risiko
(S)*Secondary*: Berarti terdapat risiko yang tidak berhubungan dengan tipe risiko
Dari tabel identifikasi risiko di atas, terdapat kategori risiko yang berisi:

1) Daftar kategori berdasarkan berdasarkan *COBIT 5 for risk* dan hasil dari risiko yang ditemukan.
2) Terdapat 3 tipe risiko yang diantaranya:
   a) *IT benefit / value enablement risk* apabila risiko yang muncul berhubungan dengan peluang peran teknologi informasi untuk meningkatkan nilai tambah korporasi atau penggerak dalam memulai sebuah proses bisnis yang baru.
   b) *IT programme and project delivery risk* apabila risiko yang muncul terkait program maupun proyek IT yang berkontribusi dalam meningkatkan bisnis.
   c) *IT operations and service delivery risk* apabila risiko yang muncul berhubungan dengan praktik, stabilitas, layanan, serta perlindungan teknologi informasi yang dapat mengganggu bagi bisnis korporasi.
3) Adanya 2 jenis skenario, yaitu skenario negatif dan skenario positif. Skenario negatif adalah jenis skenario yang dapat mengakibatkan gangguan kepada korporasi maupun mengurangi nilai korporasi, sedangkan skenario positif adalah jenis skenario yang dapat menciptakan nilai tambah bagi korporasi.

3.2 Risk Analysis

Langkah selanjutnya setelah membuat daftar identifikasi risiko yang mengganggu korporasi PT. XYZ menggunakan COBIT 5 *for risk*, yaitu mengkajian dan mengetahui prioritas risiko yang harus segera ditangani. Langkah kajian ini bernama FMEA (*Failure Mode and Effect Analysis*). Di dalam FMEA terdapat 3 variabel kajian yaitu kemungkinan, dampak, dan deteksi kemudian dilakukan perhitungan RPN (*Risk Priority Number*). RPN didapatkan dengan persamaan:

$$RPN = Dampak\ X\ Kemungkinan\ X\ Deteksi \quad [1]$$

Perhitungan RPN bertujuan untuk melihat risiko-risiko yang perlu didahulukan agar segara ditangani terlebih dahulu. Adapun kajian FMEA adalah sebagai berikut ini:

Tabel 2 ***Risk Analysis***

No	*Risiko*	*Dampak Risiko*	*Penyebab Risiko*	*Alat Deteksi*	*Nilai Dampak*	*Nilai Kemungkinan*	*Nilai Deteksi*	*Nilai RPN*
1	Tidak adanya beberapa pihak seperti direksi atau stakeholder dalam rapat pengambilan keputusan pengelolaan investasi TI	Tertundanya dalam pengambilan keputusan mengenai investasi TI	Beberapa Direksi atau stakeholder sedang bepergian ke luar kota	Deteksi dilakukan secara manual oleh Finance Controller Manager	1	1	2	2
2	Kesalahan dalam pemilihan perangkat keras untuk investasi TI	Mengakibatkan kerugian jangka panjang dalam hal investasi TI	Mencari merek lain lebih murah tetapi spesifikasi sama karena harga yang lebih murah	Deteksi dilakukan secara manual melalui pemeriksaan barang yang diawasi oleh Head of Technical	1	1	3	3
3	Tidak terdapat transfer pengetahuan	Staff yang baru akan kesusahaan	Tidak adanya serah terima tugas dan	Deteksi dilakukan secara manual	1	2	3	6

No	*Risiko*	*Dampak Risiko*	*Penyebab Risiko*	*Alat Deteksi*	*Nilai Dampak*	*Nilai Kemungkinan*	*Nilai Deteksi*	*Nilai RPN*
	dari staff yang mengundurkan diri kepada staff baru	dalam melakukan pekerjaannya	tanggung jawab dari staff yang resign dengan penggamtinya sehingga tidak mengetahui tugas dan tanggung jawab untuk jabatannya	dengan laporan dari staff yang diawasi oleh Head of Technical				
4	Tidak adanya *training skill* untuk meningkatkan *skill* staff	Skill staff tidak akan bisa mengikuti perkembangan kebutuhan korporasi	Tidak adanya dana atau budgeting untuk training skill yang berguna untuk meningkatkan skill staff	Deteksi dilakukan secara menual dengan membaca perkembangan staff yang diawasi oleh Head of Technical	1	2	3	6
5	Kurangnya skill staff dalam mendukung proses bisnis korporasi	Korporasi akan melakukan proses rekrut staff baru	Tidak adanya training skill untuk menambah atau meningkatkan skill staff	Deteksi dilakukan oleh Head of Technical	1	2	2	4
6	Ketidakmampuan korporasi dalam merekrut IT staff yang mumpuni	Tidak sesuai nya antara skill staff dengan kebutuhan korporasi	Tidak memiliki staff ahli di bidang IT yang telah memiliki skill dan pengalaman dengan jam terbang yang tinggi serta pernah menangani banyak proyek IT	Deteksi dilakukan secara manual pada saat proses rekrutmen yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	1	2	2	4
7	Kerusakan pada peralatan IT yang diakibatkan oleh staff	Perangkat TI tidak bisa digunakan	Staff IT yang ceroboh dalam menggunakan peralatan IT sehingga mengakibatkan kerusakan.	Deteksi dilakukan secara manual antara staff dengan Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi	1	1	3	3

No	*Risiko*	*Dampak Risiko*	*Penyebab Risiko*	*Alat Deteksi*	*Nilai Dampak*	*Nilai Kemungkinan*	*Nilai Deteksi*	*Nilai RPN*
				Network Operation Center				
8	Pencurian data korporasi oleh staff	Proses bisnis korporasi bisa diterapkan oleh kompetitor	Mendownload data penting dan merupakanrahasia korporasi yang bisa dijual atau diberikan kepada kompetitor atau pihak lain yang bisa merugikan korporasi.	Deteksi dilakukan dengan sistem yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	1	1	3	3
9	Kesalahan dalam input data oleh staff	Terjadinya perbedaan antara kontrak asli dengan yang ada di sistem	Staff tidak memiliki skill data entry sehingga sering terjadi kesalahan input.	Deteksi dilakukan secara manual dengan pemeriksaan data atau dokumen yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	2	5	2	20
10	Adanya kesalahan *troubleshooting* oleh staff	Terganggunya downtime dalam *troubleshooting*	Staff IT yang kurang kompentensi skill dan pengalaman sehingga masih dan sering terjadi kesalahan dalam trouble shooting	Deteksi dilakukan secara manual melalui komunikasi yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	2	3	3	18
11	Perangkat mikrotik sengaja dikonfigurasi	Terganggunya sistem mikrotik	Staff IT yang kurang kompetensi skill dan	Deteksi dilakukan secara manual dengan cara	3	1	3	9

No	*Risiko*	*Dampak Risiko*	*Penyebab Risiko*	*Alat Deteksi*	*Nilai Dampak*	*Nilai Kemungkinan*	*Nilai Deteksi*	*Nilai RPN*
	tidak sesuai oleh staff		pengalaman sehingga masih dan sering terjadi ketidak sesuaian perangkat mikrotik yang dikonfigurasi.	pengecekan barang oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center				
12	Adanya data-data korporasi baik di server maupun laptop dalam kondisi *corrupted*	Data tidak bisa digunakan atau dibaca	Karena server atau laptop yang sudah berumur tua sehingga bisa terjadi data corrupte	Deteksi dilakukan dengan sistem namun memerlukan waktu	2	1	3	6
13	Informasi yang sensitif telah tersebar luas	Reputasi korporasi bisa menurun	ada yang masuk kedalam sistem korporasi	Deteksi dilakukan secara manual melalui media cetak atau online yang memerlukan waktu	1	1	3	3
14	Data-data korporasi diakses oleh pihak yang tidak berkepentingan	Data-data korporasi bisa dicuri	Data-data korporasi diambil oleh hacker yang berhasil meretas system di dalam server	Deteksi dilakukan dengan sistem namun memerlukan waktu	1	1	3	3
15	Jaringan tidak bisa berjalan dengan baik ketika terjadi lonjakan volume lalu lintas data	Kapasitas lalu lintas data menjadi penuh	Lonjakan lalu lintas data dikarenakan salah satu jaringam utama atau backup sedang mati/down salah satu sehingga terjadi lonjakan volume lalu lintas data	Deteksi dilakukan dengan sistem yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	2	5	2	20
16	Spesifikasi mikrotik tidak sesuai dengan yang diharapkan	Mengakibatkan sistem tidak berjalan dengan baik	Staff IT yang diberi tugas untuk pengadaan mikrotik membeli perangkat mikrotik yang	Deteksi dilakukan secara manual dengan cara pengecekan barang oleh Head of IT & Telecommunic	2	1	3	6

No	*Risiko*	*Dampak Risiko*	*Penyebab Risiko*	*Alat Deteksi*	*Nilai Dampak*	*Nilai Kemungkinan*	*Nilai Deteksi*	*Nilai RPN*
			tidak sesuai spesifikasinya	ation didampingi oleh Head of Technical serta didampingi Network Operation Center				
17	Terputusnya jaringan intranet	Akses internet menjadi terganggu	Terputusnya jaringan fiber optic atau wireless atau VSAT sehingga terjadi gangguan utilitas jaringan intranet	Deteksi dilakukan dengan sistem yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	3	4	1	12
18	Server sering cepat panas	Dapat menurunkan performa server	Terlalu besarnya resource sehingga server menjadi panas	Deteksi dilakukan dengan sistem yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	1	1	1	1
19	Staff tidak bisa adaptasi dalam menggunakan software yang terbaru	Staff akan kesusahan dalam melakukan pekerjaan	Tidak ada training staff dalam penggunaan software baru	Deteksi dilakukan dengan sistem yang diawasi oleh Head of IT & Telecommunication didampingi oleh Head of Technical serta didampingi Network Operation Center	1	1	1	1

Dalam FMEA mempunyai variable kajian untuk merekognisi setiap kegagalan yang ada, yaitu seperti dibawah ini:

1) *Occurrence* / Kemungkinan

Seberapa sering kemungkinan kegagalan yang terjadi. Perhitungan nilai dari *Occurrence* / kemungkingan antara 1 sampai dengan 10.

2) *Severity* / Dampak
Merupakan dampak yang dihasilkan dari kegagalan yang terjadi. *Severity* / dampak mempunyai parameter yang dimulai dari 1 sampai dengan 10.
3) *Detection* / Alat Deteksi
Merupakan kemampuan mendeteksi kegagalan sebelum kegagalan itu terjadi. Pengukuran detection sama halnya dengan pengukuran severity dan occurrence yaitu dengan rentang 1 sampai 10.

3.3 Risk Evaluation

Setelah dilakukan perhitungan RPN, langkah selanjutnya yaitu perencanaan dan penanganan risiko. Perencanaan dan penanganan risiko penting dalam memetakan risiko mana saja yang akan masuk ke dalam kajian respon risiko (*accept, mitigate, transfer,* dan *avoid*). Setelah diketahui respon risiko, maka akan selanjutnya dilakukan pembuatan penanganan daftar risiko-risiko yang telah diketahui. Adapun dalam menentukan respon maupun penanganan risiko, peneliti menggunakan metode *proffesional judgement.* Penggunaan metode tersebut bertujuan untuk membantu dalam pengambilan keputusan yang tepat khususnya menentukan kriteria maupun penanganan risiko oleh pihak yang berwenang. Berikut merupakan daftar perencanaan dan penanganan risiko teknologi informasi / *Risk Evaluation*:

Tabel 3 *Risk Evaluation*

No	*Risiko*	*Kriteria Risiko*	*Respon Risiko*	*Penanganan Risiko*
1.	Kesalahan dalam input data oleh staff	Tinggi	Mitigasi	Memeriksa dengan sistem pendeteksi kesalahan input yang dilakukan oleh staff
2.	Jaringan tidak bisa berjalan dengan baik ketika terjadi lonjakan volume lalu lintas data	Tinggi	Mitigasi	Melakukan pengecekan secara berkala grafik MRTG pemakaian jika ada terjadi lojakan lalu lintas data bisa dideteksi secara awal
3.	Adanya kesalahan *troubleshooting* oleh staff	Tinggi	Mitigasi	Melakukan simulasi/percobaan terlebih dahulu sebelum melakukan troubleshooting
4.	Terputusnya jaringan intranet	Tinggi	Mitigasi	Koreksi Operator Jaringan yang disewa, kemudian mencari operator yang lebih baik kestabilannya
5.	Perangkat mikrotik sengaja dikonfigurasi tidak sesuai oleh staff	Sedang	Mitigasi	Melakukan simulasi/percobaan terlebih dahulu sebelum melakukan konfigurasi oleh staff
6.	Tidak terdapat transfer pengetahuan dari staff yang mengundurkan diri ke staff baru	Sedang	Mitigasi	Selalu melakukan serah terima data, dokumen serta alat kerja yang digunakan oleh staff yang resign kepada staff yang menggantikan
7.	Tidak adanya *training skill* untuk meningkatkan *skill* staff	Sedang	Transfer	Training Skill akan dilakukan oleh lembaga training yang memiliki sertifikasi dan uji kompetensi
8.	Adanya data-data korporasi baik di server maupun laptop dalam kondisi *corrupted*	Sedang	Mitigasi	Selalu melakukan backup berkala setiap hari untuk database, dokumen data lainnya setiap seminggu sekali dan system jaringan setiap sebulan sekali
9.	Spesifikasi mikrotik tidak sesuai dengan yang diharapkan	Sedang	Mitigasi	Melakukan searching dan browsing di internet dan komunitas pemakai mikrotik dengan cara menanyakan kepada komunitas spesifikasi mikrotik yang mana yang bisa dipakai untuk keperluan kita sesuai yang diharapkan
10.	Kurangnya skill staff dalam mendukung proses bisnis korporasi	Sedang	Transfer	Mencari vendor untuk outsoucing skill staff untuk mendukung bisnis korporasi
11.	Ketidakmampuan korporasi dalam merekrut IT staff yang mumpuni	Rendah	Transfer	Mencari vendor untuk outsoucing skill staff untuk mendukung bisnis korporasi

No	*Risiko*	*Kriteria Risiko*	*Respon Risiko*	*Penanganan Risiko*
12.	Kesalahan dalam pemilihan perangkat keras untuk investasi TI	Rendah	Mitigasi	Selalu update informasi mengenai perangkat keras serta kegunaannya
13.	Kerusakan pada peralatan IT yang diakibatkan oleh staff	Rendah	Mitigasi	Mencari alat pendeteksi kerusakan peralatan IT yang diakibatkan oleh staff
14.	Pencurian data korporasi oleh staff	Rendah	Mitigasi	Mencari dengan alat pendeteksi pencurian data korporasi yang dilakukan oleh staff
15.	Informasi yang sensitif telah tersebar luas	Rendah	Mitigasi	Melakukan pengecekan secara berkala ke system apakah ada informasi telah tersebar keluar
16.	Data-data korporasi diakses oleh pihak yang tidak berkepentingan	Rendah	Mitigasi	Melakukan update firewall
17.	Tidak adanya beberapa pihak seperti direksi atau stakeholder dalam rapat pengambilan keputusan pengelolaan investasi TI	Rendah	Mitigasi	Selalu ada direksi atau stakeholder dalam hal pengambilan keputusan pengelolaan investasi TI
18.	Server sering cepat panas	Rendah	Mitigasi	Melakukan pengecekan secara berkala di setiap server untuk resource, jumlah data, besaran tranfer data yang dimiliki apakah sesuai dengan besaran interface yang digunakan, update patch nya dan lainnya yang menyebabkan performa server meningkat dan berakibat menjadi server cepat panas
19.	Staff tidak bisa adaptasi dalam menggunakan software yang terbaru	Rendah	Mitigasi	Perlu diadakan training khusus secara berkala seandainya ada software baru atau upgade system yang menimbulkan perubahan secara struktur dan tampilannya

Di dalam tabel *risk evaluation* terdapat respon risiko, yang dimana respom risiko tersebut merupakan status penanganan terhadap risiko yang terdaftar. Berikut merupakan 4 (empat) pembahasan jenis respon risiko yang terdiri dari:

1) *Accept* (Menerima)
   Merupakan strategi menerima risiko yang terdaftar dan tidak melakukan perlakuan apapun terhadap risiko tersebut.
2) *Mitigate* (Mitigasi)
   Merupakan strategi mengurangi kejadian risiko yang terdaftar baik itu dampak maupun kemungkinannya.
3) *Transfer* (Membagi)
   Merupakan suatu tindakan untuk mengurangi adanya risiko dengan cara membagi nya oleh pihak ketiga seperti outsourcing atau perusahan yang berkepentingan.
4) *Avoid* (Menghindari)
   Menghindari adanya risiko dengan cara tidak meneruskan kegiatan yang berhubungan dengan risiko terkait.

4. KESIMPULAN

Dari hasil studi ini, peneliti memperoleh out put kajian terkait pengelolaan risiko IT dengan COBIT 5 *for risk* dan FMEA berasas ISO 31000. Yang berfokus dimulai dari *tahapan risk identification, risk analysis,* dan yang terakhir *risk evaluation*. Adapun hasil kajian tersebut tertulis dalam kesimpulan sebagai berikut ini:

1) Melalui proses pengelolaan risiko metode COBIT 5 *for risk* dan FMEA yang berbasis ISO 31000 serta dilakukannya uji verifikasi *depenability* oleh pihak yang dapat dipercaya yaitu dari Head of IT PT. XYZ, dapat disimpulkan adanya hubungan keterkaitan antara masing-masing framework pengelolaan risiko yang bisa digunakan untuk menjalakan langkah pengelolaan risiko dan sudah sesuai dengan kebutuhan korporasi.
2) Pada tahap identifikasi risiko yang menggunakan metode COBIT 5 *for risk* menemukan 19 risiko.
3) Dari 19 risiko yang telah ditentukan dengan parameter kriteria risiko terdapat 4 risiko dengan kriteria tinggi, 10 risiko dengan kriteria sedang, dan 9 risiko dengan kriteria rendah.
4) Dari 19 risiko terdapat respon penanganan mitigasi risiko berjumlah 16 risiko. Selain itu terdapat juga 3 respon penanganan risiko yaitu transfer.

DAFTAR PUSTAKA

[1] Dwi R, Putra A, Setiawan E, Ambarwati A. Evaluasi Pengelolaan Risiko Teknologi Informasi Berdasarkan. 2019;11(2):1754–62.

[2] Suparjo, Rochman A. Manajemen Risiko Praktik Pada PT. ABC dengan Menggunakan Metode FMEA. J Has Penelit LPPM Untag Surabaya. 2018;03(02):106–12.

[3] Tampubolon AR, Suhardi. Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010. J Telemat. 2011;7(2):1–10.

[4] Iin H, Tjahyanto A. Manajemen Risiko Teknologi Informasi Pada Proyek Korporasi XYZ Melalui Kombinasi COBIT, PMBOK, Dan ISO 31000. J Ilm Teknol dan Rekayasa [Internet]. 2017;9(2):43–50. Available from: http://repository.its.ac.id/46540/

[5] Moleong LJ. Metodologi Penelitian Kualitatif (Edisi Revisi). In: PT Remaja Rosda Karya. 2017.

[6] Babb S, Anton E, Bleicher J. COBIT 5 for Risk. Isaca. 2013;

[7] Pribadi HI. Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000 : 2018 Dengan FMEA (Studi Kasus PT Pertamina). 2020;01:28–35.

[8] Retna Maharani A. Perancangan Manajemen Risiko Praktik Di Pt . X Dengan Menggunakan Metode House of Risk. 2018. 1–140 p.

[9] Megawati M, Syntia A. Evaluasi Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5.0. J Ilm Rekayasa dan Manaj Sist Inf. 2018;4(2):118.

[10] Puspitasari NB, Martanto A. Penggunaan Fmea Dalam Mengidentidikasi Resiko Kegagalan Proses Produksi Sarung Atm (Alat Tenun Mesin) (Studi Kasus Pt. Asaputex Jaya Tegal). J@Ti Undip J Tek Ind. 2014;9(2):93–8.

[11] Muttaqin AZ, Kusuma YA. Kajian Failure Mode And Effect Analysis Proyek X Di Kota Madiun. JATI UNIK J Ilm Tek dan Manaj Ind. 2018;

[12] Carbone TA, Tippett DD. Project risk management using the project risk fmea. EMJ - Eng Manag J. 2004;