ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PT. XYZ MENGGUNAKAN *FRAMEWORK* COBIT 2019 Pada *Risk Profile*

1st Rydho Helmy Pramoedya
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
rydhohelmy@student.telkomuniversity.ac.id

2nd Widyatasya Agustika Nurtrisha
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
widyatasya@telkomuniversity.ac.id

3rd Dhata Praditya
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
dhatap@telkomuniversity.ac.id

Abstrak*— PT. XYZ sudah mempunyai divisi ERM (Enterprise Risk Management) untuk mengelola manajemen risiko secara umum dan belum melakukan manajemen risiko TI secara khusus. Penelitian ini dilakukan untuk mengevaluasi risiko yang mungkin akan muncul dalam operasional divisi IT PT. XYZ karena pada divisi IT tersebut belum menerapkan manajemen risiko TI. Penelitian ini menggunakan framework ISO 27005 sebagai panduan utama dalam pengelolaan risiko, dan untuk COBIT 2019 digunakan sebagai identifikasi risiko dan sumber risiko yang digunakan dalam penelitian ini. Peneliti mengumpulkan data melalui penyebaran kuesioner yang digunakan untuk mengumpulkan informasi dari Expert Head unit TI dan Staff unit TI mengenai pandangan dan pengalaman terkait pengelolaan risiko dan melakukan wawancara mendalam untuk memvalidasi hasil dari kuesioner. Hasil dari identifikasi yang peneliti dapatkan 4 risk profile yang sudah dilakukan penentuan oleh PT. XYZ dengan total 21 risiko yang telah diidentifikasi bahwa Divisi IT memerlukan manajemen risiko yang menyeluruh untuk mengantisipasi berbagai ancaman dan kelemahan yang dapat mempengaruhi IT operasional dan keberlangsungan Perusahaan.

***Kata kunci*— Manajemen Risiko, Teknologi Informasi, ISO/IEC 27005, COBIT 2019**

I. PENDAHULUAN

Dengan kemajuan teknologi yang pesat saat ini, berbagai faktor terkena dampaknya. Teknologi informasi memainkan peran krusial dalam operasional perusahaan. Pemanfaatan teknologi informasi yang tepat dapat memperkuat manajemen risiko, sehingga operasional perusahaan dalam mengelola risiko dapat berjalan dengan optimal. Manajemen risiko adalah suatu proses yang sistematis dan terencana untuk memitigasi atau mengendalikan kemungkinan terjadinya kesalahan atau kerugian yang timbul dari risiko yang ada di perusahaan. Proses ini sering dianggap sebagai salah satu langkah penting menuju perbaikan yang berkelanjutan. Setiap perusahaan dihadapkan pada risiko yang menjadi bagian dari kegiatan operasionalnya. Risiko adalah sesuatu yang belum tentu terjadi, dan tidak semua risiko memiliki dampak negatif bagi perusahaan. Namun, apabila perusahaan mampu mengelola risiko dengan baik, risiko tersebut dapat diminimalisir. Risiko dapat muncul dari lingkungan internal maupun eksternal. Dengan mengidentifikasi potensi risiko lebih awal, perusahaan dapat mengalokasikan sumber daya dengan lebih efisien, meningkatkan kualitas layanan, serta membangun reputasi yang lebih baik di mata para pemangku kepentingan. [1].

IT (Information Technology) Manajemen risiko merupakan salah satu solusi untuk mengelola risiko dalam hal Teknologi Informasi [2]. Manajemen risiko juga merupakan tindakan untuk mengevaluasi dan memprediksi risiko yang melibatkan identifikasi prosedur untuk meminimalkan dampaknya [2]. Dengan penggunaan framework ISO 27005 untuk pengelolaan risiko, PT XYZ dapat mengidentifikasi, menganalisis, dan mengelola risiko dengan lebih efektif. ISO 27005 menyediakan kerangka kerja yang berstandar internasional untuk manajemen risiko, sehingga dapat membantu PT XYZ memastikan bahwa strategi pengelolaan risiko mereka sesuai.

Dalam menghadapi berbagai risiko yang mungkin muncul di dalam perusahaan, pengelolaan dan pengendalian risiko menjadi sangat penting untuk memastikan kelangsungan dan pertumbuhan perusahaan, terutama di era persaingan yang sangat ketat seperti sekarang. Salah satu cara untuk mengelola dan mengurangi dampak risiko adalah dengan menerapkan manajemen risiko yang efektif. Manajemen risiko meliputi identifikasi, analisis, dan penilaian risiko yang dihadapi perusahaan, serta pengembangan strategi untuk memitigasi atau mengendalikan risiko tersebut. [3].

PT XYZ menganggap manajemen risiko bukan hanya tugas divisi TI saja itu adalah bagian penting dari strategi bisnis yang luas. Perusahaan ini menyadari bahwa dengan mengidentifikasi, mengevaluasi, dan mengelola risiko secara proaktif, sehingga dapat mengurangi kemungkinan terjadinya kejadian merugikan dan merespons dengan cepat jika terjadi. PT XYZ harus memiliki sistem manajemen risiko yang komprehensif karena kompleksitas operasional perawatan pesawat. PT XYZ juga sadar akan pentingnya transparansi dalam pelaporan risiko kepada semua pemangku kepentingan, termasuk karyawan, mitra bisnis, dan investor. Dengan memberikan informasi yang jelas tentang risiko yang dihadapi, perusahaan dapat membangun kepercayaan dan mengajak semua pihak yang terlibat untuk membantu meminimalkan risiko.

PT XYZ merupakan perusahaan yang beroperasi di bidang perawatan dan perbaikan. Sebagai bagian dari industri penerbangan PT XYZ menghadapi berbagai risiko yang dapat mempengaruhi kinerja dan kelangsungan bisnisnya.

Akibatnya, untuk mengidentifikasi, menganalisis, dan mengelola risiko yang dihadapi, PT XYZ harus menerapkan manajemen risiko yang efektif dan efisien. Perusahaan dapat mengunakan kerangka kerja ISO 27005 standar internasional yang memberikan panduan mengenai manajemen risiko yang dapat disesuaikan dengan kebutuhan dan konteks organisasi. Dengan menerapkan ISO 27005, PT XYZ dapat mengidentifikasi risiko yang dihadapi oleh perusahaan secara sistematis dan terstruktur dan dapat mengelola risiko dengan lebih efektif dan efisien.

II. KAJIAN TEORI

Menyajikan dan menjelaskan teori-teori yang berkaitan dengan variabel-variabel penelitian. Poin subjudul ditulis dalam abjad.

A. Risiko

Risiko adalah faktor yang menimbulkan ketidakpastian mengenai kemungkinan terjadinya suatu peristiwa dalam jangka waktu tertentu, yang pada akhirnya dapat menyebabkan kerugian, baik dalam bentuk yang tidak terlalu signifikan maupun yang memiliki dampak lebih serius terhadap kelangsungan operasional perusahaan[4].

B. Manajemen Risiko

Manajemen Risiko adalah tindakan yang mencakup identifikasi, pengukuran, serta perlindungan dari risiko, dan penyusunan strategi untuk mengatasinya. Proses ini melibatkan berbagai langkah, metode, dan teknik yang membantu manajer proyek dalam meningkatkan peluang serta dampak dari kejadian yang menguntungkan, sekaligus mengurangi kemungkinan dan dampak dari kejadian yang tidak diinginkan. Dalam konteks manajemen proyek, manajemen risiko merujuk pada kombinasi pengetahuan dan praktik yang digunakan untuk mengidentifikasi, menganalisis, dan merespons risiko sepanjang siklus hidup proyek, sambil memastikan tercapainya tujuan proyek. Penerapan manajemen risiko yang efisien dalam proyek dapat secara signifikan meningkatkan tingkat keberhasilan proyek dan memberikan manfaat positif dalam hal pemilihan proyek, penetapan ruang lingkup proyek, perencanaan jadwal yang realistis, serta perkiraan biaya yang akurat[5].

C. IT Manajemen Resiko

Pemahaman tentang risiko sangat krusial bagi perusahaan atau perusahaan, karena dapat mempengaruhi secara baik maupun buruk terhadap kelangsungan operasional mereka. Institusi pendidikan tinggi, sebagai salah satu jenis perusahaan, juga tidak bisa menghindari risiko yang mungkin timbul. Risiko dapat diartikan sebagai peristiwa yang memiliki potensi untuk memengaruhi pencapaian, hasil, dan dampak yang telah ditetapkan[6]. Kegagalan dalam pengawasan dan pengelolaan perusahaan oleh manajemen perusahaan adalah penyebab munculnya risiko. Ketidakefektifan dalam menerapkan Tata Kelola TI dan kurangnya kesadaran serta pemahaman sumber daya dalam perusahaan terhadap risiko dapat mengakibatkan risiko yang timbul di perusahaan. Oleh karena itu, untuk mencegah risiko, penting untuk menerapkan Manajemen Risiko TI dalam perusahaan.

Manajemen Risiko TI merupakan pendekatan untuk mengelola risiko yang berkaitan dengan teknologi informasi dalam kerangka manajemen perusahaan[2]. Tiap perusahaan akan menghadapi beragam risiko yang dapat memengaruhi hasil operasional mereka. Dengan menerapkan Manajemen Risiko TI, perusahaan dapat menganalisis dan mengelola risiko yang berasal dari potensi ancaman yang mungkin terjadi[7].

D. COBIT 2019

COBIT, merupakan singkatan dari Control Objectives for Information and Related Technology, yaitu sebagai standar audit atau praktik untuk manajemen TI yang dikeluarkan oleh ISACA [8]. COBIT 2019 juga mendefinisikan komponen yang diperlukan untuk membangun dan menopang tata kelola, termasuk struktur organisasi, proses, kebijakan dan prosedur, arus informasi, budaya dan perilaku, keterampilan, dan infrastruktur (Muhammad Saleh, 2021). COBIT adalah framework tata kelola IT yang dirancang untuk mengumpulkan nilai dari GAP teknis, resiko, dan pengendalian. Dan memberikan pedoman komprehensif untuk mengelola dan mengawasi penggunaan teknologi informasi dalam organisasi untuk memastikan bahwa TI dapat berjalan dengan tujuan bisnis dan mengurangi risiko operasional [9].

E. ISO/IEC 27005: 2018

Komite Teknis Gabungan ISO/IEC JTC1, telah bekerja untuk membuat standar ISO/IEC 27005, terutama berkat dedikasi subkomite SC 27 yang berfokus pada teknologi informasi dan teknik keamanan TI. Standar ini merangkum konsep, model, proses, dan terminologi yang telah terstandarisasi dalam ISO/IEC 27001 dan sangat bermanfaat untuk manajemen risiko keamanan informasi. Pertama, pembuatan konteks yang menyeluruh diperlukan untuk menerapkan standar ini sebagai pengantar praktis. Ini termasuk menetapkan tujuan organisasi, menetapkan standar dasar, seperti standar evaluasi risiko dan batasan penerimaan risiko, dan memberikan penjelasan tentang lingkup dan keterbatasan manajemen risiko keamanan informasi[10].

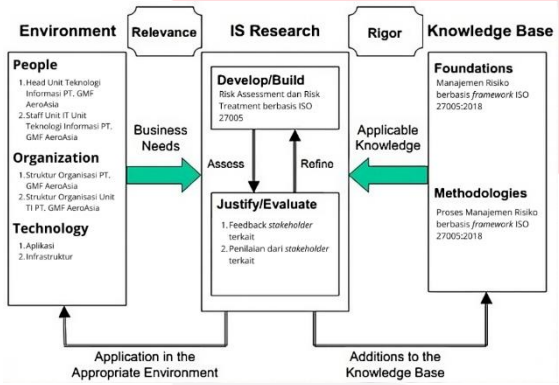
F. Perbandingan Framework ISO/IEC 27005 dan ISO 31000

ISO 27005 dan ISO 31000 adalah dua kerangka kerja yang digunakan untuk manajemen risiko, namun keduanya memiliki fokus dan pendekatan yang berbeda. ISO 27005 adalah standar internasional yang memberikan panduan untuk manajemen risiko keamanan informasi (ISO/IEC 27005, 2018). Kerangka kerja ini berfokus pada identifikasi, penilaian, dan penanganan risiko yang berkaitan dengan keamanan informasi, serta mendukung implementasi manajemen risiko di bidang teknologi informasi. Sedangkan untuk, ISO 31000 memberikan panduan umum untuk manajemen risiko di seluruh organisasi, tidak hanya berfokus pada teknologi informasi saja. ISO 31000 mencakup prinsip-prinsip dan pedoman untuk mengelola risiko secara keseluruhan, yang dapat diterapkan di berbagai industry PT. XYZ sendiri sudah menerapkan framework ISO 31000 yang dikelola oleh divisi ERM (Enterprise Risk Manajement). Fokus utama ISO 31000 adalah untuk membantu organisasi dalam mengelola risiko yang dapat mempengaruhi pencapaian tujuan perusahaan[11]. Dengan demikian, sementara ISO/IEC 27005 memberikan pendekatan yang lebih spesifik terhadap risiko keamanan informasi dan teknologi informasi yang dapat dikelola pada divisi IT, dan

ISO 31000 menawarkan pendekatan yang lebih komprehensif untuk manajemen risiko secara umum.

III. METODE

Metode konseptual merupakan kerangka pikir yang menjelaskan gagasan tentang keterlibatan subjek penelitian, situasi, atau fenomena dengan penelitian ilmu pengetahuan yang diteliti. Metode ini digunakan untuk menyelidiki dan memahami fenomena atau hubungan antar variabel dengan lebih mendalam. Ini memberi mereka landasan teoritis yang kokoh, yang memungkinkan mereka untuk menetapkan kerangka kerja untuk menguraikan dan menganalisis informasi yang dikumpulkan.



Gambar 1. Model Konseptual

Pada gambar III.1 menunjukkan penjelasan mengenai tiga elemen yang ada beserta hubungannya dengan kerangka teori yang digunakan dalam penelitian ini. Berikut penjelasan tiga elemen tersebut adalah sebagai berikut:

- Environment
  Environment berkaitan dengan lingkungan yang digunakan sebagai tempat dilaksanakannya penelitian, dalam hal ini adalah PT XYZ pada Head unit TI dan Staff Unit IT TI sebagai sumber informasi peniliti untuk dapat membantu mengumpulkan informasi yang dapat digunakan sebagai data penelitian.
- Knowledge Base
  Pada hal ini merujuk pada bagian dari model konseptual yang mengumpulkan, menyimpan, dan mengelola pengetahuan yang relevan dengan organisasi atau sistem tersebut. Foundations merupakan hal yang menjadi topik utama yaitu penilaian resiko manajemen bedasarkan kategori dan metode penelitian yang digunakan yaitu metode kualitatif, Dalam penelitian ini, Methodology merupakan pendekatan sistematis yang digunakan yaitu: ISO/IEC 27005
- IS Research
  merupakan suatu pendekatan akademis yang berpusat pada pengembangan, analisis, dan evaluasi konsep-konsep penting yang terkait dengan sistem informasi. Dalam hal ini, develop/build mengacu pada hasil penelitian yang dilakukan, sedangkan untuk Justify/Evaluate merupakan melakukan evaluasi penilaian dari para pihak yang terbilang ahli dan menerapkan rekomendasi.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini akan menjelaskan mengenai hasil dari analisis manajemen risiko teknologi informasi pada PT XYZ menggunakan framework ISO/IEC 27005 pada *risk profile* sebagai berikut.

A. Matriks Risiko

Matriks risiko merupakan suatu alat dalam manajemen risiko yang digunakan untuk dapat mengukur tingkat risiko. Matriks didapat dari tingkat kemungkinan *(Likelihood)* dan tingkat dampak *(Consequence)* yang dapat menghasilkan skala besaran risiko. Sehingga besaran risiko ini yang akan digunakan untuk mengetahui tingkat risiko yang ada pada organisasi. Dapat dilihat pada tabel matriks yang menjadi acuan dalam penelitian ini.

Table 1. Matrik Risiko

Likelihood (L)						
	Certain	5 Medium	10 High	15 High	20 Crisis	25 Crisis
	Likely	4 Low	8 Medium	12 High	16 Crisis	20 Crisis
	Possible	3 Low	6 Medium	9 High	12 High	15 High
	Unlikely	2 Low	4 Low	6 Medium	8 Medium	10 High
	Rare	1 Low	2 Low	3 Low	4 Low	5 Medium
		Insignificant	Minor	Moderate	Major	Catastrophic
	Consequence (C)					

Level risiko mengacu pada tingkat risiko yang dihasilkan oleh risiko – risiko yang terjadi. Penilaian tingkat risiko ini sangat penting untuk menentukan tindakan yang perlu diambil dalam mengelola risiko. Dengan mengetahui tingkat risiko yang ada, organisasi dapat membuat keputusan yang lebih baik untuk mengurangi risiko. Pada tabel ini menunjukkan penilaian tingkat risiko yang menunjukkan prioritas dan urgensi dari setiap risiko yang telah diidentifikasi.

Table 2. Level Risiko

No	Level Risiko	Besaran Risiko	Keterangan
1.	Low	1 s.d. 4	
2.	Medium	5 s.d. 9	
3.	High	10 s.d. 15	
4.	Crisis	16 s.d. 25	

B. Analisis Risiko

Analisis risiko merupakan langkah berikutnya setelah melakukan identifikasi risiko, yang bertujuan untuk memahami secara lebih mendalam dampak dan kemungkinan terjadinya risiko-risiko yang telah ditemukan. Sehingga setiap risiko dapat dievaluasi untuk menentukan tingkat prioritas penanganannya seperti pada tabel berikut ini.

Table 3. Analisis Risiko

Risk ID	Risk Profile	Risiko	Besaran Risiko	Level Risiko
R1	Data and information management (19)	Tersebarnya informasi sensitif karena arsip/pembuangan informasi yang tidak efektiif.	1	Low
R2		Melakukan perubahan data yang bersifat melanggar dengan sengaja.	9	High
R3		Pembukaan informasi sensitif yang tidak diizinkan oleh perusahaan.	8	Medium
R4		Terjadinya kebocoran informasi yang bersifat kompetitif.	6	Medium
R16	IT cost and oversight (3)	Kelebihan biaya dan/atau ketidakefektifan pembelian terkait TI di luar proses pengadaan barang dan jasa	2	Low
R17		Ketergantungan yang luas pada aplikasi yang dibuat, didefinisikan, dan dipelihara oleh pengguna serta solusi ad hoc.	6	Medium
R18		Kurangnya dana investasi terkait TI	15	High
R19		Persyaratan yang tidak memadai yang menyebabkan Service Level Agreements (SLA) tidak efektif	6	Medium
R20	IT expertise, skills, and behavior (4)	Ketidakmampuan untuk merekrut dan mempertahankan staf TI	8	Medium
R21		Perekrutan profil yang tidak sesuai karena kurangnya uji tuntas dalam proses perekrutanproses rekrutmen	4	Low
R22		Kurangnya pelatihan TI	12	High
R23		Kurangnya atau ketidaksesuaian keterampilan terkait TI dalam TI itu sendiri (misalnya, karena teknologi baru ataumetode kerja)	6	Medium
R24		Ketergantungan yang berlebihan untuk layanan I&T pada staf kunci	8	Medium
R25		Kurangnya pemahaman bisnis oleh staf TI yang mempengaruhi kualitas layanan/proyek	16	Crisis
R54	Software failures (10)	Ketidakmampuan untuk kembali ke versi sebelumnya jika terjadi masalah operasional dengan yang versi baru	6	Medium
R55		Data (basis data) yang rusak akibat perangkat lunak yang menyebabkan data tidak dapat diakses	6	Medium
R56		Kerusakan perangkat lunak yang biasa terjadi pada perangkat lunak aplikasi penting	15	High
R57		Perangkat lunak aplikasi yang sudah usang (usang, tidak terdokumentasi dengan baik, mahal untuk dipelihara, sulit untuk dikembangkan, tidak terintegrasi dalam arsitektur saat ini, dll.)	15	High
R58		Gangguan operasional ketika perangkat lunak baru dibuat operasional	6	Medium
R59		Ketidakmampuan untuk menggunakan perangkat lunak untuk mewujudkan hasil yang diinginkan (model bisnis atau perubahan organisasi yang diperlukan)	6	Medium
R60		Implementasi perangkat lunak yang belum matang (pengguna awal, bug, dll.)	6	Medium

C. Respon Risiko

Menurut ISO 27005, respon terhadap risiko merupakan suatu langkah atau tindakan untuk mengurangi, mentolerir, membagi risiko dan menghindari, sesuai dengan tingkat keparahan dan kemungkinan terjadinya. Respons risiko ditentukan oleh nilai risiko yang telah diidentifikasi, sebagaimana dijelaskan pada tabel.

Table 4. Respon Risiko

Kriteria	
Penanganan / Perlakuan Risiko	**Deskripsi**
Modification	**Modifikasi** • Tingkat risiko harus dikelola dengan memperkenalkan, menghapus, atau mengubah pengendalian sehingga risiko yang tersisa dapat dinilai kembali sebagai risiko yang dapat diterima.
Retention	**Retensi Risiko** • jika tingkat risiko memenuhi kriteria penerimaan risiko, maka tidak diperlukan penerapan pengendalian tambahan dan risiko dapat dipertahankan.
Share/Transfer	**Membagi Risiko** • Respon share kita pilih apabila diperlukan kontrol dari pihak lain di dalam perusahaan. • Respon transfer kita pilih antara lain dengan cara mengasuransi atau outsource ke pihak ketiga.
Avoidance	**Menghindari Risiko** • Respon ini kita pilih dengan tujuan agar risiko tersebut tidak akan pernah terjadi. • Cara yang dapat dilakukan adalah dengan menghilangkan proses tersebut. Dengan demikian, risiko yang melekat pada proses tersebut tidak akan pernah ada karena prosesnya tidak ada.

D. Evaluasi Risiko

Evaluasi risiko bertujuan untuk menilai seberapa besar dampak dan kemungkinan terjadinya risiko yang telah diidentifikasi dan dianalisis, sehingga dapat diberikan respon yang sesuai dengan daftar risiko, seperti pada tabel berikut.

Table 5. Evaluasi Risiko

Risk ID	Risk Profile	Risiko	Level Risiko	Respon Risiko
R1	Data and information management (19)	Tersebarnya informasi sensitif karena arsip/pembuangan informasi yang tidak efektiif.	Low	Retention
R2		Melakukan perubahan data yang bersifat melanggar dengan sengaja.	High	Modification
R3		Pembukaan informasi sensitif yang tidak diizinkan oleh perusahaan.	Medium	Modification
R4		Terjadinya kebocoran informasi yang bersifat kompetitif.	Medium	Retention
R16	IT cost and oversight (3)	Kelebihan biaya dan/atau ketidakefektifan pembelian terkait TI di luar proses pengadaan barang dan jasa	Low	Retention
R17		Ketergantungan yang luas pada aplikasi yang dibuat, didefinisikan, dan dipelihara oleh pengguna serta solusi ad hoc.	Medium	Modification
R18		Kurangnya dana investasi terkait TI	High	Modification
R19		Persyaratan yang tidak memadai yang menyebabkan Service Level Agreements (SLA) tidak efektif	Medium	Modification
R20	IT expertise, skills, and behavior (4)	Ketidakmampuan untuk merekrut dan mempertahankan staf TI	Medium	Modification
R21		Perekrutan profil yang tidak sesuai karena kurangnya uji tuntas dalam proses perekrutanproses rekrutmen	Low	Retention
R22		Kurangnya pelatihan TI	High	Modification
R23		Kurangnya atau ketidaksesuaian keterampilan terkait TI dalam TI itu sendiri (misalnya, karena teknologi baru ataumetode kerja)	Medium	Modification
R24		Ketergantungan yang berlebihan untuk layanan I&T pada staf kunci	Medium	Modification
R25		Kurangnya pemahaman bisnis oleh staf TI yang mempengaruhi kualitas layanan/proyek	Crisis	Modification
R54	Software failures (10)	Ketidakmampuan untuk kembali ke versi sebelumnya jika terjadi masalah operasional dengan yang versi baru	Medium	Modification
R55		Data (basis data) yang rusak akibat perangkat lunak yang menyebabkan data tidak dapat diakses	Medium	Modification
R56		Kerusakan perangkat lunak yang biasa terjadi pada perangkat lunak aplikasi penting	High	Modification
R57		Perangkat lunak aplikasi yang sudah usang (usang, tidak terdokumentasi dengan baik, mahal untuk dipelihara, sulit untuk dikembangkan, tidak terintegrasi dalam arsitektur saat ini, dll.)	High	Modification
R58		Gangguan operasional ketika perangkat lunak baru dibuat operasional	Medium	Modification
R59		Ketidakmampuan untuk menggunakan perangkat lunak untuk mewujudkan hasil yang diinginkan (mis. model bisnis atau perubahan organisasi yang diperlukan)	Medium	Modification
R60		Implementasi perangkat lunak yang belum matang (pengguna awal, bug, dll.)	Medium	Modification

E. Penerapan Kontrol Proses

Proses penetapan kontrol didasarkan pada penilaian dan evaluasi risiko yang memerlukan kontrol untuk mengurangi dampak pada perusahaan. Langkah ini penting untuk menjamin bahwa setiap kontrol yang diterapkan dapat mengelola risiko dengan baik. Pada table 6 merupakan kontrol yang telah divalidasi oleh para penanggung jawab risiko, hal ini bertujuan untuk memastikan bahwa implementasi kontrol tersebut sesuai dengan kondisi yang dihadapi Perusahaan saat ini, sehingga mampu untuk mengatasi risiko dengan tepat dan efisien.

Table 6. Penerapan Kontrol Proses

Risk ID	Judul Kontrol	Deskripsi
R1	**DSS05.06** - Manage sensitive documents and output devices.	Mengimplementasikan perlindungan fisik yang memadai, teknik akuntansi, dan manajemen inventaris untuk aset TI sensitif seperti formulir khusus, dokumen penting, printer khusus, atau token keamanan.
R2	**DSS05.04** - Manage user identity and logical access. **APO13.02** - Define and manage an information security and privacy risk treatment plan.	Memelihara rencana keamanan informasi yang menjelaskan cara pengelolaan risiko keamanan informasi yang disesuaikan dengan strategi dan arsitektur perusahaan. Pastikan bahwa rekomendasi untuk peningkatan keamanan didasarkan pada kasus bisnis dan dapat diterapkan sebagai bagian dari pengembangan layanan, solusi, atau operasi bisnis
R3	**DSS05.06** - Manage sensitive documents and output devices. **DSS05.02** - Manage network and connectivity security.	Menggunakan perlindungan fisik yang tepat, teknik akuntansi, dan manajemen inventaris untuk aset TI sensitif. Melindungi data pada semua metode konektivitas dengan menerapkan protokol keamanan yang sesuai dan manajemen terkait.
R4	**APO13.02** - Define and manage an information security and privacy risk treatment plan.	Menetapkan dan mengelola rencana penanganan risiko keamanan informasi dan privasi yang selaras dengan kebijakan dan strategi perusahaan.
R16	**APO06.01** - Manage finance and accounting. **APO06.04** - Model and allocate costs.	Mengelola dan mencatat semua biaya, investasi, dan penurunan nilai TI sebagai bagian dari sistem keuangan perusahaan. Laporan

		dibuat dengan sistem pengukuran keuangan perusahaan. Membuat dan menerapkan model biaya TI berdasarkan layanan. Ini memastikan identifikasi, pengukuran, dan prediksi alokasi biaya serta mendorong penggunaan sumber daya yang bijak.
R17	**APO06.02** - Prioritize resource allocation.	Menerapkan prosedur pengambilan keputusan untuk menentukan prioritas alokasi sumber daya dan menetapkan aturan untuk investasi bebas oleh unit bisnis.
R18	**APO06.05** - Manage costs.	Menerapkan proses untuk membandingkan biaya aktual dengan anggaran yang ditetapkan. Biaya harus dipantau, dilaporkan, dan penyimpangan dari anggaran harus segera diidentifikasi serta dampaknya dievaluasi.
R19	**APO09.02** - Catalog I&T-enabled services. **APO09.03** - Define and prepare service agreements.	Membuat dan memelihara katalog layanan untuk kelompok sasaran yang relevan. Perjanjian layanan disusun berdasarkan opsi dalam katalog layanan, dan perjanjian operasional internal disertakan.
R20	**APO07.06 -** Manage contract staff. **APO07.01 -** Acquire and maintain adequate and appropriate staffing.	Memastikan bahwa konsultan dan staf kontrak memahami dan mematuhi kebijakan organisasi serta memenuhi persyaratan kontrak.
R21	**APO07.01 -** Acquire and maintain adequate and appropriate staffing.	Memastikan proses perekrutan dilakukan dengan uji tuntas yang memadai untuk mendapatkan karyawan yang sesuai dengan kebutuhan bisnis.
R22	**APO07.03 -** Maintain the skills and competencies of personnel	Menetapkan dan memantau kemampuan serta keterampilan yang diperlukan oleh staf.
R23	**APO03.01 -** Develop the enterprise architecture vision. **APO03.02 -** Define reference architecture. **APO07.03 -** Maintain the skills and competencies of personnel	Mengembangkan visi arsitektur perusahaan, menetapkan arsitektur referensi untuk mengikuti perkembangan teknologi, dan mempertahankan kompetensi staf melalui pelatihan serta pengembangan berkelanjutan.
R24	**APO07.02 -** Identify key IT personnel. **APO07.03 -** Maintain the skills and competencies of personnel	Mengidentifikasi karyawan TI menggunakan dokumentasi pengetahuan, berbagi pengetahuan, perencanaan suksesi, dan backup staf. Menetapkan serta mengawasi kemampuan yang dibutuhkan staf.
R25	**APO02.01** - Understand enterprise context and direction. **DSS06.01** - Align control activities embedded in business processes with enterprise objectives.	Memahami konteks perusahaan, termasuk penggerak industri, regulasi yang relevan, operasi saat ini, dan tingkat ambisi perusahaan dalam digitalisasi.
R54	**BAI07.05** - Perform acceptance tests. **APO14.10** - Manage data backup and restore arrangements.	Melakukan uji penerimaan untuk Melakukan uji penerimaan untuk memastikan versi baru berfungsi dengan baik sebelum diterapkan. Mengelola pencadangan dan pemulihan data untuk memungkinkan rollback jika diperlukan.
R55	**BAI07.01** - Establish an implementation plan.	Menyusun rencana implementasi yang mencakup langkah-langkah untuk mengurangi risiko
	BAI07.03 - Plan acceptance tests.	kerusakan data. Merencanakan uji penerimaan untuk memastikan perangkat lunak berfungsi dengan baik tanpa merusak data.
R56	**BAI03.10** - Maintain solutions.	Pemeliharaan solusi yang berkelanjutan diperlukan untuk mengatasi kerusakan perangkat lunak yang sering terjadi pada aplikasi penting guna memastikan keandalan dan kinerja optimal.
R57	**BAI09.03** - Manage the asset life cycle.	Aplikasi perangkat lunak yang sudah usang memerlukan manajemen siklus hidup aset untuk memastikan relevansinya dan dukungan terhadap operasional bisnis.
R58	**BAI07.08 -** Perform a post-implementation review (Development) **DSS01.03 -** Monitor I&T infrastructure. (Operasional)	Tinjauan pasca-implementasi dilakukan untuk menemukan kesimpulan akhir, pelajaran yang didapat, dan membuat rencana tindakan. Infrastruktur I&T dimonitor secara terus menerus dengan informasi kronologis yang cukup untuk peninjauan operasi.
R59	**BAI02.01 -**Define and maintain business functional and technical requirements **BAI03.03 -** Develop solution components. **BAI03.07 -** Prepare for solution testing.	Mendefinisikan dan pengawasan Menetapkan dan mengawasi persyaratan fungsional dan teknis bisnis. Mengembangkan komponen solusi yang mendukung perubahan model bisnis. Menguji elemen solusi dalam lingkungan yang sesuai untuk memastikan integrasi dan fungsionalitasnya.
R60	**BAI02.01 -**Define and maintain business functional and technical requirements. **BAI03.03 -** Develop solution components. **BAI03.07 -** Prepare for solution testing.	Menetapkan serta mengawasi persyaratan fungsional dan teknis bisnis untuk memastikan perangkat lunak sesuai kebutuhan perusahaan. Mengembangkan komponen solusi dan menguji elemen solusi yang terintegrasi.

V. KESIMPULAN

Bedasarkan hasil dari penelitian yang telah dilakukan mengenai Risk Assesment pada PT XYZ peneliti mendapatkan hasil yakni Divisi IT PT XYZ memerlukan manajemen risiko yang menyeluruh untuk mengantisipasi berbagai ancaman dan kelemahan yang dapat mempengaruhi IT operasional dan keberlangsungan Perusahaan yang dibantu dengan framework COBIT 2019 Figure 2.7 – Risk Profile Design Factor *(IT Risk Categories*) dengan mengambil 4 risk profile yang sudah dilakukan penentuan oleh PT. XYZ yaitu: Data and Information Management, IT Cost and Oversight, IT Expertise, Skill, and Behavior, dan Software Failures dengan total 21 risiko yang telah diidentifikasi.

Dalam melakukan penilaian pada risiko yang telah diidentifikasi terdapat 1 risiko dengan level crisis, 5 risiko dengan level high, 12 risiko dengan level medium dan 3 risiko dengan level low. Berdasarkan hasil evaluasi, diputuskan untuk tidak menangani risiko yang berstatus low dikarenanakan dampaknya terhadap PT XYZ tidak terlalu signifikan. Dan untuk 18 risiko lainnya yang berstatus medium hingga crisis akan diberikan penanganan dan kontrol risiko yang sesuai tingkat level risiko yang telah ditetapkan sebelumnya.

Risiko tersebut diberi penanganan karena memiliki dampak yang signifikan, sehingga perlu dilakukan pengelolaan kontrol untuk mengurangi dampak yang mungkin terjadi. Risiko yang telah dievaluasi kemudian diberikan kontrol berdasarkan standar COBIT 2019. Kontrol yang digunakan adalah APO02.01 - *Understand enterprise context and direction,* DSS06.01 - *Align control activities embedded in business processes with enterprise objectives.* APO07.02 - *Identify key IT personnel,* APO07.03 - *Maintain the skills and competencies of personnel,* APO06.05 - *Manage costs,* BAI03.10 - *Maintain solutions,* BAI09.03 - *Manage the asset life cycle,* DSS05.04 - *Manage user identity and logical access,* APO13.02 - *Define and manage an information security and privacy risk treatment plan,* APO07.06 - *Manage contract staff.* APO08.01 - *Understand business expectations,* APO08.02 - *Align I&T strategy with business expectations and identify opportunities for IT to enhance the business,* DSS05.06 - *Manage sensitive documents and output devices,* DSS05.02 - *Manage network and connectivity security,* APO03.01 - *Develop the enterprise architecture vision,* APO03.02 - *Define reference architecture,* BAI07.05 - *Perform acceptance tests,* APO14.10 - *Manage data backup and restore arrangements.* BAI07.01 - *Establish an implementation plan,* BAI07.03 - *Plan acceptance tests,* BAI07.08 - *Perform a post-implementation review (Development)* DSS01.03 - *Monitor I&T infrastructure. (Operasional),* BAI02.01 - *Define and maintain business functional and technical requirements,* BAI03.03 - *Develop solution components,* BAI03.07 - *Prepare for solution testing,* APO06.02 - *Prioritize resource allocation,* APO09.02 - *Catalog I&T-enabled services,* APO09.03 - *Define and prepare service agreements.*

REFERENSI

[1] A. P. Aisyah and L. Dahlia, "Jurnal Akuntansi dan Manajemen (JAM) Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti," *BPJP) Sekolah Tinggi Ilmu Ekonomi Indonesia Jakarta*, vol. 19, no. 02, 2022, doi: 10.36406/jam.v19i01.483.

[2] S. M. Mohammad, "Risk Management in Information Technology," *SSRN Electronic Journal*, Jun. 2020, doi: 10.2139/ssrn.3625242.

[3] N. M. Sirait and A. Susanty, "Analisis Risiko Operasional Berdasarkan Pendekatan Enterprise Risk Management (ERM) pada Perusahaan Pembuatan Kardus di CV Mitra Dunia Palletindo," 2016.

[4] A. Lokobal, A. Pascasarjana, U. Sam, R. Marthin, D. J. Sumajouw, and B. F. Sompie, "Manajemen Risiko pada Perusahaan Jasa Pelaksana Konstruksi di Provinsi Papua (Studi Kasus di Kabupaten Sarmi)," *Jurnal Ilmiah Media Engineering*, vol. 4, no. 2, pp. 109–118, 2014.

[5] I. Putu, A. Eka, P. #1, and T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *Jurnal Telematika*, vol. 15, no. 2.

[6] C. Septiawan, E. Sujana, S. Tinggi, I. Kesehatan, and I. Maju, "Model Sistem Manajemen Risiko pada Perguruan Tinggi Kesehatan Swasta di Indonesia (Studi Kasus di STIKES Indonesia Maju)".

[7] R. Yasirandi, A. Rakhmatsyah, and F. Kurniawan, "IT Risk Management dalam Operasional untuk Peningkatan Layanan Informasi Pesanan," *Krea-TIF*, vol. 9, no. 2, p. 21, Nov. 2021, doi: 10.32832/kreatif.v9i2.5982.

[8] J. Sirajuddin, A. Rajjani, B. T. Hanggara, and Y. T. Musityo, "Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12," 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[9] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2018.

[10] V. Agrawal, "A framework for the information classification in ISO 27005 standard."

[11] ISO/IEC 31000, "Risk management-Guidelines INTERNATIONAL STANDARD ISO 31000 ISO 31000:2018(E) ii COPYRIGHT PROTECTED DOCUMENT Published in Switzerland," 2018.