AUDIT MANAJEMEN RISIKO DENGAN MENGGUNAKAN FRAMEWORK ISO 31000:2018 DAN COBIT 2019 PADA UPA TIK POLITEKNIK NEGERI LAMPUNG

Tesis

Oleh

Pradana Marlando

NPM 2125031004

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2025

AUDIT MANAJEMEN RISIKO DENGAN MENGGUNAKAN FRAMEWORK ISO 31000:2018 DAN COBIT 2019 PADA UPA TIK POLITEKNIK NEGERI LAMPUNG

Oleh

PRADANA MARLANDO

TESIS

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
MAGISTER TEKNIK

Pada

Jurusan Teknik Elektro
Fakultas Teknik Universitas Lampung

FAKULTAS TEKNIK
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2025

ABSTRACT

AUDIT INFORMATION TECHNOLOGY BY USING ISO 31000:2018 AND COBIT 2019 AS A FRAMEWORK ON UPA TIK POLITEKNIK NEGERI LAMPUNG

By

PRADANA MARLANDO

Nowdays, the use of information technology is a common thing for an organization including at the Lampung State Polytechnic. In addition to providing benefits, information technology also has new things to consider, namely information technology risks that need to be managed by implementing risk management. A good risk management can minimize or as a preventive action against risks. An audit of risk management is necessary in order to provide an overview of the risks and their preventive measures, as well as an evaluation of risk management with an assessment of the current level of capability. This study use the ISO 31000:2018 framework as a standard and COBIT 2019 as a best practice framework in the field in implementing the audit. ISO 31000:2018 will provide a complete overview of existing technology risks, while COBIT 2019 will provide an assessment of the level of capability, both of which will serve as a guide to provide recommendations for improving the technology risk management that has been carried out. Based on the results of the audit, 68 risks were found, consisting of 8 high-level risks, 35 medium-level risks, and 25 low-level risks. These risks are given suggestions for prevention or reducing the impact of the risk. Evaluation of the capability level on the objective APO12 state the current condition at level 2, where the expected condition based on the factor design analysis is at level 4 where there is a gap of 2 levels. There are 20 recommendations proposed to achieve level 4 and recommendations for risks in general in order to reduce the level of risk.

Keywords: Information Technology Risk Management, ISO 31000:2018, COBIT 2019.

ABSTRAK

AUDIT MANAJEMEN RISIKO DENGAN MENGGUNAKAN FRAMEWORK ISO 31000:2018 DAN COBIT 2019 PADA UPA TIK POLITEKNIK NEGERI LAMPUNG

Oleh

PRADANA MARLANDO

Pada era saat ini, penggunaan teknologi informasi merupakan hal yang sangat umum digunakan untuk sebuah organisasi termasuk di Politeknik Negeri Lampung. Teknologi informasi selain akan memberikan keuntungan, terdapat juga hal baru yang perlu diperhatikan yaitu risiko teknologi informasi yang perlu dikelola dengan dilakukannya manajemen risiko. Manajemen risiko yang baik dapat meminimalisir atau tindakan pencegahan terhadap risiko. Audit terhadap manajemen risiko dirasa perlu dilakukan agar dapat memberikan gambaran terkait risiko dan tindakan pencegahannya selain itu juga evaluasi terhadap manajemen risiko dengan penilaian tingkat kapabilitas saat ini. Penelitian ini menggunakan kerangka kerja ISO 31000:2018 sebagai standar dan COBIT 2019 sebagai *best practice* di lapangan pada pelaksanaan auditnya. ISO 31000:2018 akan memberikan gambaran lengkap terkait dengan risiko teknologi yang ada, sedangkan COBIT 2019 akan memberikan penilaian tingkat kapabilitas yang keduanya akan menjadikan panduan untuk diberikan sebuah rekomendasi perbaikan dari manajemen risiko teknologi yang telah dilakukan. Berdasarkan hasil pelaksanaan audit ditemukan 68 Risiko yang terdiri dari 8 risiko tingkat tinggi, 35 risiko tingkat menengah, dan 25 risiko tingkat rendah. Risiko-risiko tersebut diberikan saran untuk pencegahan atau mengurangi dampak dari risiko tersebut. Evaluasi dari tingkat kapabilitas pada obyek APO12 menyatakan kondisi terkini pada level 2, dimana kondisi yang diharapkan berdasarkan analisis desain faktor ada pada level 4 yang mana terdapat kesenjangan sebanyak 2 level. Terdapat 20 rekomendasi yang diusulkan untuk dapat mencapai level 4 dan rekomendasi terhadap risiko secara keseluruhan agar dapat mengurangi tingkat risiko.

Kata kunci : Manajemen Risiko Teknologi Informasi, ISO 31000: 2018, COBIT 2019.

Judul Tesis	: AUDIT MANAJEMEN RISIKO DENGAN MENGGUNAKAN FRAMEWORK ISO 31000:2018 DAN COBIT 2019 PADA UPA TIK POLITEKNIK NEGERI LAMPUNG
Nama Mahasiswa	: *Pradana Marlando*
Nomor Pokok Mahasiswa	: 2125031004
Jurusan	: Magister Teknik Elektro
Fakultas	: Teknik

MENYETUJUI

1. Komisi Pembimbing

Dr. Eng. Ir. Mardiana, S.T., M.T., IPM.
NIP 197203161999032002

Misfa Susanto, S.T., M.Sc., Ph.D.
NIP 197105251999031001

2. Ketua Program Studi Magister Teknik Elektro

Dr. Ir. Sri Ratna Sulistiyanti, M.T.
NIP 196510211995122001

MENGESAHKAN

1. Tim Penguji

   Ketua : **Dr. Eng. Ir. Mardiana, S.T., M.T., IPM**

   Sekretaris : **Misfa Susanto, S.T., M.Sc., Ph.D.**

   Anggota : **Dr. Eng. Helmy Fitriawan, S.T., M.Sc.**

   Anggota : **Dr. Eng. F.X. Arinto Setyawan, S.T.,M.T.**

2. Dekan Fakultas Teknik

   Dr. Eng. Helmy Fitriawan, S.T., M.Sc.
   NIP 197509282001121002

3. Direktur Program Pascasarjana

   Prof. Dr. Ir. Murhadi, M.Si.
   NIP 196403261989021001

Tanggal Lulus Ujian Tesis : **12 Juni 2025**

LEMBAR PERNYATAAN

Dengan ini Saya Menyatakan bahwa sesungguhnya tesis yang saya susun sebagai syarat untuk mendapatkan gelar Magister Teknik pada Program Pascasarjana Magister Teknik Elektro seluruhnya adalah benar merupakan hasil karya sendiri.

Adapun bagian-bagian tertentu dalam penulisan tesis ini, saya kutip dari hasil penulisan orang lain yang sumbernya dituliskan dengan jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah.

Tesis berjudul "Audit Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 DAN COBIT 2019 Pada UPA TIK Politeknik Negeri Lampung" dapat diselesaikan dengan bimbingan dari dosen pembimbing dan semua pihak yang terlibat. Saya ucapkan terimakasih yang sebesar besarnya kepada Ibu Dr. Eng. Ir. Mardiana, S.T., M.T., IPM. Dan Bapak Misfa Susanto, S.T., M.T., Ph.D selaku dosen pembimbing dan semua pihak yang telah membantu perjalanan saya dalam menyelesaikan Program Magister ini.

Apabila di kemudian hari terbukti bahwa tesis saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi akademik sesuai dengan peraturan perundangan yang berlaku.

Bandar Lampung, 12 Juni 2025

Pradana Marlando
NPM 2125031004

RIWAYAT HIDUP

Penulis lahir di Bandar Lampung pada tanggal 4 Desember 1993 anak pertama dari pasangan Ayah Yatim Rahayu Widodo dan Mama Anna Maria. Penulis pertama kali mengenyam pendidikan formal di SD Kartika II-5 Bandar Lampung dan lulus pada tahun 2005, kemudian melanjutkan pendidikan Sekolah Menengah Pertama di SMPN 2 Bandar Lampung dan lulus pada tahun 2008. Selanjutnya, penulis melanjutkan pendidikan Sekolah Menengah Atas di SMAN 2 Bandar Lampung dan lulus pada tahun 2011. Tahun tersebut juga, penulis melanjutkan pendidikan di perguruan tinggi negeri Universitas Lampung sebagai mahasiswa Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam. Penulis berhasil menyelesaikan program S1 pada tahun 2015. Penulis saat ini bekerja di Politeknik Negeri Lampung sejak tahun 2017. Merasa perlu mengembangkan diri dan ilmu sehingga penulis melanjutkan studi program S2 pada tahun 2021 dengan mengambil Program Studi Magister Teknik Elektro dengan fokus bidang Telekomunikasi dan Teknologi Informasi.

PERSEMBAHAN

Kupersembahkan karya ini untuk :

Ayah dan mama yang telah merawat, mendidik, memotivasi, dan selalu memberikan doa yang terbaik.

Adikku yang aku sayangi.

Serta Keluarga Kecilku yang tersayang dan tercinta,

Istriku Rifka Faridah Adhima,

Anakku Rayzen Ammar Malik Keenandra.

Terima Kasih untuk semua yang kalian berikan.

MOTTO

Do It Now, or Regret Later

"Sesungguhnya Allah tidak merubah keadaan sesuatu kaum sehingga mereka merubah keadaan yang ada pada diri mereka sendiri."(QS Ar-Ra'd: 11)

Give the best for someone who have faith in you

"Berencanalah kalian, Allah membuat rencana. Dan Allah sebaik-baik perencana." (QS. Ali Imran : 54)

UCAPAN TERIMAKASIH

Puji syukur penulis panjatkan kehadirat Allah SWT atas berkat rahmat, hidayah, dan kesehatan yang diberikan sehingga penulis dapat menyelesaikan penulisan tesis ini.

Tesis ini disusun sebagai syarat untuk memperoleh gelar Magister Teknik Elektro di Jurusan Teknik Elektro Universitas Lampung. Judul dari tesis ini adalah "Audit Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Dan COBIT 2019 Pada UPA TIK Politeknik Negeri Lampung".

Dalam penyusunan tesis ini, penulis banyak menghadapi kesulitan. Namun, berkat bantuan dan motivasi dari berbagai pihak, akhirnya penulis dapat menyelesaikan tesis ini. Untuk itu pada kesempatan ini, penulis mengucapkan terimakasih kepada:

1. Ayah dan Mama yang telah memberikan doa dan motivasi serta memfasilitasi kebutuhan untuk menyelesaikan tesis ini.
2. Keluarga kecilku yang selalu menjadi motivasi untuk menyelesaikan tesis ini.
3. Keluarga Alm. Papah Drs. Denden Kurnia Drajat, M.Si. yang selalu memberikan motivasi dan dukungannya untuk penyelesaian tesis ini.
4. Ibu Prof. Dr. Ir. Lusmeilia Afriana, D.E.A., IPM., selaku Rektor Universitas Lampung.
5. Bapak Prof. Dr. Murhadi, M.Si. selaku Direktur Program Pascasarjana Universitas Lampung.
6. Ibu Dr. Eng. Ir. Mardiana, S.T., M.T., IPM sebagai pembimbing I sekaligus pembimbing akademik penulis yang telah memberikan ide dan masukan dalam pengerjaan tesis serta dengan sabar membimbing hingga tesis ini selesai.
7. Bapak Misfa Susanto, S.T., M.Sc., Ph.D. sebagai pembimbing II penulis, yang tidak pernah bosan memotivasi dan membantu penulis untuk dapat menyelesaikan tesis, tanpa beliau mungkin tesis ini tidak akan pernah ada.

8. Bapak Dr. Eng. Helmy Fitriawan, S.T., M.Sc. sebagai penguji utama yang telah memberikan masukan-masukan dan saran yang bermanfaat dalam tesis ini serta telah sedia memberikan waktunya ditengah kesibukannya sebagai Dekan Fakultas Teknik.
9. Bapak Dr. Eng. F.X. Arinto Setyawan, S.T.,M.T sebagai penguji yang telah memberikan masukan-masukan dan saran yang bermanfaat dalam tesis ini serta selalu mendukung penyelesaian tesis ini.
10. Ibu Dr. Ir. Sri Ratna Sulistiyanti, M.T. selaku Ketua Program Studi Magister Teknik Elektro saat ini dan juga yang telah memberikan daftar Matakuliah Kurikulum sehingga meyakinkan untuk melanjutkan studi.
11. Bapak Dr. Septafiansyah Dwi Putra, S.T., M.T. selaku pembimbing di tempat bekerja dan Bapak Halim Fathoni, Ph.D. selaku Kepala UPA TIK Politeknik Negeri Lampung.
12. Bapak dan Ibu Dosen Magister Teknik Elektro yang telah memberikan ilmu pengetahuan yang bermanfaat bagi penulis.
13. Tim PPMPP dan keluarga Politeknik Negeri Lampung yang telah mengizinkan untuk melanjutkan pendidikan.
14. Mba Nurul dan Mba Yeni yang selalu bersedia direpotkan ketika bimbingan maupun administrasi.
15. Rekan-rekan seperjuangan Magister Teknik Elektro Angkatan 2021, khususnya Wahyu dan Sora.
16. Dan semua pihak yang telah membantu menyelesaikan tesis ini yang tidak bisa disebutkan satu per satu.

Penulis menyadari bahwa tesis ini masih jauh dari kesempurnaan, akan tetapi sedikit harapan semoga tesis ini bermanfaat bagi perkembangan ilmu Manajemen Teknologi saat ini.

Bandar Lampung, 12 Juni 2025

Pradana Marlando

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Pada era modern saat ini, penggunaan teknologi informasi merupakan hal yang sangat umum digunakan untuk sebuah organisasi kecil hingga besar. Penggunaan teknologi informasi ini digunakan untuk mempermudah pekerjaan manusia. Teknologi informasi yang baik akan dapat memberikan informasi yang relevan yang dapat digunakan manajerial untuk mengambil keputusan yang terbaik. Dengan teknologi informasi pula fungsi-fungsi manajemen seperti *Planning – Organizing – Actuating – Controlling* dapat berjalan dengan efektif dan efisien [1]. Proses yang *real time* dan *reliable* dapat dimanfaatkan untuk menunjang kebutuhan mendesak dan cepat. Pada perguruan tinggi hal ini tentu berperan penting dalam menjalankan fungsi dan tugas perguruan tinggi serta memaksimalkan potensi yang tersedia pada perguruan tinggi.

Perguruan tinggi secara umum dipimpin oleh seorang dosen yang diberikan tugas tambahan. Hal ini membuat seorang pimpinan perguruan tinggi membutuhkan sebuah teknologi informasi yang dapat digunakan secara efektif dan efisien sebagai penyedia informasi. Namun apakah teknologi informasi yang digunakan sudah dapat menyediakan informasi yang tepat dan sesuai dengan kebutuhan. Jika tidak maka teknologi informasi yang digunakan dapat dikatakan tidak baik karena investasi teknologi informasi yang tepat pada saat ini adalah sesuatu yang sangat berharga. Karenanya tata kelola teknologi informasi dibutuhkan untuk menjamin bahwa teknologi informasi tersebut mendukung perguruan tinggi untuk mencapai tujuan atau *goal* dari pimpinan yang telah ditentukan [2]. Hal ini akan menjadi fokus utama dari teknologi informasi di perguruan tinggi.

Politeknik Negeri Lampung merupakan salah satu perguruan tinggi negeri yang bertempat di Kota Bandar Lampung [3]. Saat ini Politeknik Negeri Lampung telah

menjalankan proses bisnisnya dengan menggunakan bantuan dari teknologi informasi sebagai penyimpanan data dan penyedia informasi. Teknologi informasi merupakan alat bantu yang vital, karena jika salah satu teknologi informasi bermasalah atau tidak dapat digunakan akan berdampak untuk keseluruhan proses yang ada. Politeknik Negeri Lampung memiliki *server* tersendiri untuk mengelola data dan juga menggunakan *server* pihak luar untuk beberapa teknologi informasinya. Tentunya hal tersebut akan memberikan keuntungan tersendiri untuk Politeknik Negeri Lampung, namun hal tersebut juga memiliki kelemahan. Karenanya sebuah manajemen risiko perlu dilakukan.

Manajemen risiko merupakan hal yang wajib dimiliki atau dilakukan oleh sebuah organisasi dalam menghadapi proses bisnis. Manajemen risiko dapat mengurangi dampak yang diakibatkan sebuah risko dari suatu sistem [4]. Dengan manajemen risiko seluruh Sumber Daya Manusia yang ada di organisasi dapat melakukan pencegahan sesuai dengan prosedur yang tepat. Prosedur itu umumnya didokumentasikan agar seluruh Sumber Daya Manusia dapat memahami dan mengaplikasikannya. Risiko-risiko tersebut juga dapat terjadi pada kasus perguruan tinggi khususnya di bagian teknologi informasi. Pada perguruan tinggi, *database* merupakan hal yang sangat vital, karena *database* perlu dilindungi pada *server* yang aman dan *reliable*. Tidak hanya sekedar data, *database* pada perguruan tinggi dapat mencakup hal yang bersifat pribadi. Namun apakah *server* yang telah dilindungi dapat dikatakan aman dan *reliable*? Tentu tidak, kesalahan atau kegagalan tidak hanya terjadi pada internal organisasi namun juga eksternal yang diluar kendali kita. Karenanya sebuah manajemen risiko yang tepat akan dapat melindungi *server* dari kegagalan atau kesalahan dengan dampak seminimal mungkin karena kemungkinan untuk mencegah akan sulit. Manajemen risiko mengambil peranan besar dalam melindungi *server* agar seluruh Sumber Daya Manusia dapat secara langsung mengurangi dampak tersebut. Sebuah manajemen risiko perlu dilakukan secara terstruktur dan terkendali, karenanya sebuah *framework* manajemen risiko diperlukan dalam pembuatan dokumentasi. Salah satu *framework* manajemen risiko terkait dengan teknologi informasi adalah *Control Objective for Information and Related Technology* (COBIT) dan *International Organization for Standardization* (ISO) yang akan menjadi fokus penelitian kali ini.

Control Objective for Information and Related Technology (COBIT) merupakan *Framework Best Practice* yang dikembangkan oleh ISACA untuk membantu dalam proses, mendesain dan mengimplementasikan teknologi informasi yang sesuai dengan kebutuhan [5]. *Framework Control Objective for Information and Related Technology* (COBIT) menjamin sebuah manajemen risiko tersebut terkendali dan sesuai dengan harapan yang dinginkan dari pemangku organisasi [6]. COBIT 2019 mengintegrasikan tata kelola risiko dan manajemen dengan keseluruhan tatakelola dan Manajemen TI yang terdefinisi dalam COBIT proses EDM03-*Ensured Risk Optimisation* dan APO12-*Managed Risk* [7]. Sedangkan *framework International Organization for Standardization* (ISO) adalah sebuah standar pelaksanaan dari sebuah manajemen risiko tersebut. ISO 31000:2018 dikembangkan untuk organisasi menciptakan dan menjaga nilai dari tujuan yang diharapkan dengan cara melakukan manajemen risiko, membuat keputusan atau kebijakan dari risiko tersebut dan menentukan *objective* dan peningkatan yang dibutuhkan [8]. Dengan menggabungkan kedua *framework* tersebut diharapkan penelitian ini mampu memberikan sebuah standar kelayakan dan masukan untuk mendapatkan sebuah keinginan dari pemangku organisasi dalam kasus manajemen risiko di perguruan tinggi. *Framework Control Objective for Information and Related Technology* (COBIT) yang akan digunakan adalah COBIT 2019 yang mana versi terbaru dari COBIT tersebut dan memiliki beberapa perubahan dari versi COBIT 5 terdahulunya. Sedangkan untuk ISO yang digunakan adalah 31000 yang mana digunakan saat ini sebagai standar untuk manajemen risiko [9].

Berdasarkan permasalahan di atas, maka diperlukan sebuah penilaian manajemen risiko untuk teknologi informasi yang saat ini digunakan di Politeknik Negeri Lampung. Dalam hal ini, akan dilakukan audit berbasis standar ISO 31000:2018 dengan menggunakan proses *assessment* dengan *framework* COBIT 2019. Diharapkan dengan menggunakan keduanya didapatkan sebuah penilaian risiko teknologi informasi yang ada di Politeknik Negeri Lampung dengan standar 31000 yang digunakan untuk memastikan berjalan sesuai dengan standar dan COBIT yang digunakan untuk melakukan tata kelola agar hasil luaran dari teknologi informasi yang dilakukan telah sesuai dengan yang diharapkan.

1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah sebagai berikut:

1 Bagaimana hasil identifikasi, analisis, dan penilaian manajemen risiko dengan menggunakan standar ISO 31000:2018 dan COBIT 2019 sebagai *best practice* untuk teknologi informasi yang ada di Politeknik Negeri Lampung?

2 Apa rekomendasi terkait manajemen risiko untuk teknologi informasi yang digunakan di Politeknik Negeri Lampung dengan menggunakan *capability level*?

3 Bagaimana *gap* antara kondisi terkini dan kondisi yang diharapkan di Politeknik Negeri Lampung?

1.3 Batasan Masalah

Adapun Batasan masalah untuk penelitian ini adalah sebagai berikut:

1 Studi kasus penelitian pada Politeknik Negeri Lampung.

2 Penelitian ini dilakukan untuk meneliti Manajemen Risiko berbasis standar ISO 31000:2018 dan COBIT 2019 dengan domain EDM03 dan APO12.

3 Manajemen risiko yang dilakukan adalah terkait Teknologi Informasi yang diterapkan di Politeknik Negeri Lampung yang terpusat pada Unit Pelayanan Akademik (UPA) Teknologi Informasi dan Komunikasi (TIK).

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1 Memberikan Gambaran terkait risiko TI pada UPA TIK Politeknik Negeri Lampung.

2 Menilai *capability level* dari teknologi informasi yang diterapkan di Politeknik Negeri Lampung.

3 Mengevaluasi dan memberikan rekomendasi untuk perbaikan teknologi informasi yang diterapkan di Politeknik Negeri Lampung.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1 Manfaat bagi peneliti adalah untuk mendapatkan pemahaman dan praktik lapang terkait dengan pelaksanaan audit teknologi informasi, serta memenuhi syarat menyelesaikan studi.
2 Manfaat bagi institusi adalah untuk memberikan gambaran dan rekomendasi perbaikan terkait teknologi informasi yang berjalan di Politeknik Negeri Lampung.
3 Manfaat bagi penelitian selanjutnya adalah untuk membuka wawasan dan rekomendasi terhadap audit teknologi informasi dan *framework* ISO 31000:2018 dan *framework* COBIT 2019.

1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini akan dibagi dalam 5 bab, sebagaimana dijelaskan berikut ini:

BAB I Pendahuluan

Di dalam bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Di dalam bab ini akan diterangkan mengenai teori-teori yang mendasari penelitian.

BAB III Metodologi Penelitian

Di dalam bab ini akan dijabarkan terkait metodologi yang digunakan selama penelitian.

BAB IV Hasil dan Pembahasan

Di dalam bab ini akan dijabarkan terkait hasil dari penelitian ini serta evaluasi terhadap penelitian yang telah dilakukan.

BAB V Penutup

Di dalam bab ini berisi kesimpulan dari penelitian yang telah dilakukan.

BAB II. TINJAUAN PUSTAKA

2.1 Penelitian Sejenis

Penelitian yang diteliti oleh Prof. Dr. Osama Abdel Munem Ali dengan judul *Impact of* COSO and COBIT5 *Regulatory Integrasion in the Correct Aplication of Cyber Governance in Jordanian Commercial Banks* tahun 2021 membahas terkait efek dari pengaplikasian dua *framework* Audit untuk manajemen risiko antara COSO dan COBIT5 yang mengambil obyek bank komersial di Jordania. Pada penelitian ini, peneliti menggunakan dua *framework* berbeda dan tidak diintegrasikan untuk membuktikan hipotesa terkait pengambilan keputusan supervisor dalam pengaplikasian tata kelola siber terhadap kerangka kerja yang dilakukan. Berdasarkan penelitian ini diambil kesimpulkan terdapat hasil yang signifikan terkait tata kelola yang diimplementasikan dengan COBIT 5 dan COSO [10].

Penelitian terkait ISO 31000 dan COBIT yang diteliti oleh Khrisna Aprianto, dkk tahun 2021 yang berjudul Analisis Manajemen Risiko SPBE menggunakan COBIT 5 *For Risk* dan ISO 31000:2018 di Kabupaten Magetan mendapatkan identifikasi risiko dan rekomendasi terkait manajemen risiko SPBE tersebut. Peneliti menuliskan ego sektoral antar intitusi penerapan TI tidak optimal, karenanya perlu dilakukan manajemen risiko TI. Peneliti melakukan analisis dari manajemen risiko SPBE itu dan memberikan rekomendasi terkait risiko yang ada berdasarkan framework COBIT 5 dan ISO 31000:2018 [11].

Penelitian lainnya terkait ISO 31000 dan COBIT tahun 2023 adalah Audit Manajemen Risiko Sistem Informasi pada *Website* Digo.id dengan *framework* COBIT 5 dan ISO 31000. Pada penelitian yang dilakukan oleh Putra Pamungkas Sukmana, dkk melakukan identifikasi, analisis dan audit manajemen risiko pada web Digo.id dengan *framework* COBIT 5 dan ISO 31000 untuk mendapatkan

gambaran yang jelas terkait manajemen risiko yang dilaksanakan oleh perusahaan. Berdasarkan hasil audit peneliti terdapat gap sejumlah 2 terkait *capability level existi*ng dan target. Peneliti memberikan rekomendasi terkait kegiatan yang dapat dilakukan untuk mencapai target tersebut [12].

Penelitian berjudul Penerapan Manajemen Risiko IT pada Bank X dengan Menggunakan *Framework* COBIT 2019 yang diteliti oleh Willian Jordy, dkk tahun 2022, meneliti permasalahan proses bisnis pada Bank X yang melibatkan IT. Menurut Peneliti, permasalahan yang umum terjadi seperti *server* yang tidak stabil pada penginputan data. Penelitian ini bertujuan pada faktor apa saja yang paling berpengaruh pada proses bisnis yang berkaitan dengan penggunaan IT dengan menggunakan COBIT 2019 pada *domain* APO 11 *Managed Quality dan* APO 12 *Managed Risk.* Peneliti akan meneliti hasil *capability level* dan penilaian risiko menggunakan standar OWASP pada domain APO 11 dan APO 12. Berdasarkan hasil penelitian dituliskan beberapa solusi untuk menghindari risiko [13].

Penelitian lainnya berjudul Evaluasi Manajemen Risiko Teknologi Informasi pada *Department of ICT* PT Semen Indoensia (Persero) Tbk yang diteliti oleh Jauhar Sirajuddin, dkk pada tahun 2021 dengan menggunakan *Framework* COBIT 2019 dengan Domain EDM03 dan APO12. PT Semen Indonesia membutuhkan teknologi informasi sebagai penunjang kegiatan operasionalnya. Peneliti berasumsi jika tidak memiliki tingkat penanganan yang tepat, teknologi informasi seperti itu memiliki risiko-risiko yang tidak dapat dihindari. Karenanya diperlukan penilaian tingkat kematangan atau *capability level* pada manajemen risiko sistem informasi. Peneliti menggunakan kerangka kerja COBIT 2019 dengan domain EDM03 dan APO12. Hasil dari penelitian ini adalah dokumen standar dan kebijakan serta implementasi proses optimasi risiko teknologi informasi [14].

Penelitian terkait lainnya berjudul Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO12 yang diteliti oleh Rifqi Anugrah,dkk pada tahun 2022. Menurut Peneliti setiap sistem teknologi informasi yang mendukung keberlangsungan sektor pendidikan di Indonesia harus dimaksimalkan. Guna mencapai tingkat teknologi informasi yang baik di sektor pendidikan diperlukan adanya suatu analisis terkait

manajemen risiko dengan melalui audit tata kelola informasi teknologi. Penelitian ini berfokus menganalisis manajemen risiko dengan menggunakan *framework* COBIT 2019 pada domain APO12 untuk menghasilkan nilai *capability level* yang dijadikan acuan manajemen risiko pada perguruan tinggi [15].

Penelitian berjudul Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari *Departement Store* Cabang Malang *Town Square*) yang diteliti oleh Hana Talitha Iddo Driantami, dkk pada tahun 2018. Penelitiam ini merupakan penelitian sejenis lainnya. Untuk mewujudkan visi PT Matahari *Departement Store* diperlukan manajemen risiko terkait teknologi informasi. Peneliti menyampaikan belum memiliki dokumentasi terkait manajemen risiko teknologi informasi, maka dilakukanlah penelitian dengan berbasis ISO 31000 untuk manajemen risiko teknologi informasi [16].

Analisis Manajemen Risiko TI Pada Diskominfo Salatiga Menggunakan COBIT 5 Dengan Domain APO 12 merupakan penelitian terkait selanjutnya. Meskipun penelitian ini menggunakan COBIT 5 namun dapat dikaitkan terkait manajemen risiko teknologi informasi dan *domain* APO12 yang digunakan. Penelitian ini dilakukan oleh Hesti Ani Novita Sari dkk. Pada tahun 2021. Peneliti mengambil studi kasus di Diskominfo Salatiga yang mana merupakan perangkat kota yang memiliki tugas mengelola di bidang komunikasi dan informatika. Manajemen risiko teknologi informasi yang tepat sangat diperlukan. *Server down*, *virus*, kerusakan maupun kehilangan data merupakan risiko yang dapat terjadi di diskominfo, karenanya diperlukan analisis manajemen risiko teknologi informasi pada diskominfo pada *domain* APO12. Hasil penlitian memaparkan risiko-risiko yang berpotensi membahayakan dan memberikan rekomendasi sebagai solusi untuk menekan potensi kerugian yang dapat timbul [17].

Penelitian-penelitian diatas merupakan rujukan dalam melakukan penelitian terkait analisis manajemen risiko teknologi informasi di Politeknik Negeri Lampung berbasis ISO 31000:2018 dengan menggunakan *Framework* COBIT 2019.

2.2 Politeknik Negeri Lampung

Dalam rangka memenuhi kebutuhan tenaga terampil dan profesional di bidang pertanian, Pemerintah Indonesia membuka sistem pendidikan baru yang berbentuk Politeknik Pertanian. Politeknik Pertanian Negeri di Provinsi Lampung ini resmi terbentuk dengan diterbitkannya SK Dirjen Dikti Depdikbud No.14/Dikti/Kep/1984, tanggal 7 April 1984 tentang Pembentukan Politeknik Pertanian Universitas Lampung. Kemudian dalam rangka mempersiapkan pengembangan Politeknik Pertanian, yang meliputi pengembangan fisik kampus, tenaga pengajar, dan pengembangan kurikulum, maka pada tanggal 3 Desember 1985, melalui SK Dirjen Dikti Depdikbud No.79/Dikti/Kep/1985, dibentuk Penanggung Jawab Unit Pelaksana Proyek pada Proyek Pengembangan Pendidikan Politeknik Pertanian Universitas Lampung [18].

Pada tanggal 3 November 1988 Politeknik Pertanian Universitas Lampung menempati kampus baru di Jalan Soekarno-Hatta, Rajabasa, Bandar Lampung dan pada tanggal 15 Desember 1988 Penanggungjawab Pengembangan Politeknik Pertanian Negeri Lampung dilantik oleh Rektor Universitas Lampung pada tanggal 7 April 2001, berdasarkan SK. Mendiknas RI No. 036/O/2001 tentang Pendirian Politeknik Pertanian Negeri Bandar Lampung, Politeknik Pertanian Negeri Lampung resmi mandiri menjadi salah satu bentuk Perguruan Tinggi Negeri (PTN) di Provinsi Lampung dengan nama Politeknik Pertanian Negeri Bandar Lampung.

Berdasarkan rapat Senat Politeknik tanggal 19 Oktober 2002 telah ditetapkan perubahan nama Politeknik Pertanian Negeri Bandar Lampung menjadi Politeknik Negeri Lampung (Polinela). Pertimbangan perubahan nama tersebut merupakan rencana pengembangan Politeknik di masa mendatang agar memperluas bidang studi yang dapat dilaksanakan dan dibutuhkan masyarakat, misalnya bidang studi ekonomi secara umum, keteknikan, manajemen dan sebagainya.

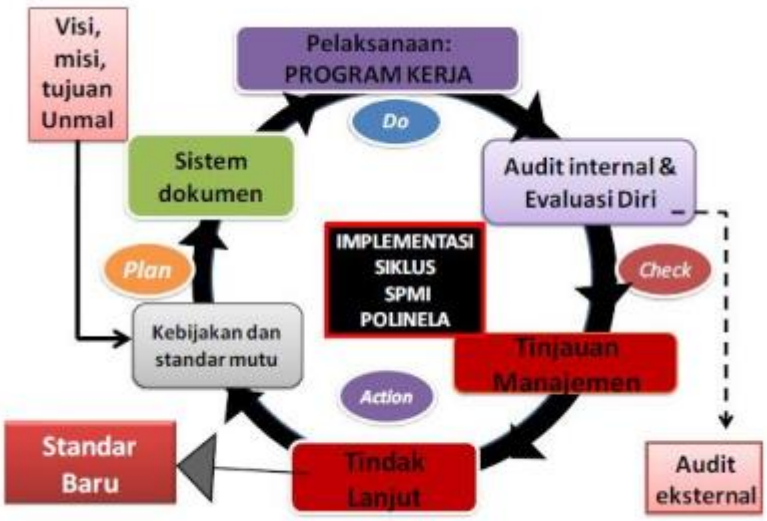
Berdasarkan statuta Polinela, Polinela memiliki visi menjadi Politeknik yang bermutu inovatif, dan unggul dalam ilmu pengetahuan dan teknologi terapan dengan misi antara lain:

1. Menyelenggarakan pendidikan vokasi yang berorientasi pada akhlak mulia, kompenten, kompetitif, disiplin, dan mandiri.

2. Melaksanakan kajian keilmuan dan penelitian terapan untuk menopang pendidikan dan pengajaran.
3. Melaksanakan pengabdian kepada masyarakat melalui transfer ilmu pengetahuan dan teknologi terapan.
4. Menguatkan budaya akademik, organisasi, dan kerja yang berkarakter dan beretika.
5. Menjalin kerjasama secara berkelanjutan dengan pihak lain.

Saat ini Polinela harus siap menyongsong masa depan dan berkembang sesuai dengan visi Indonesia Emas 204. Perubahan ilmu pengetahuan dan teknologi dengan akselarasi yang luar biasa cepat, seiring berubah, tak terduga, *unstructure*, dan belum pernah terbayangkan sebelumnya. Berbagai tantangan eksternal seperti era globalisasi abad XXI, revolusi industri 4.0, *society* 5.0, *disruption era*, bergesernya generasi dari milenial ke *Z generation* dan *Alpha* memaksa Polinela harus berkembang pesat mengikuti zaman agar tidak tersisihkan di era ini.

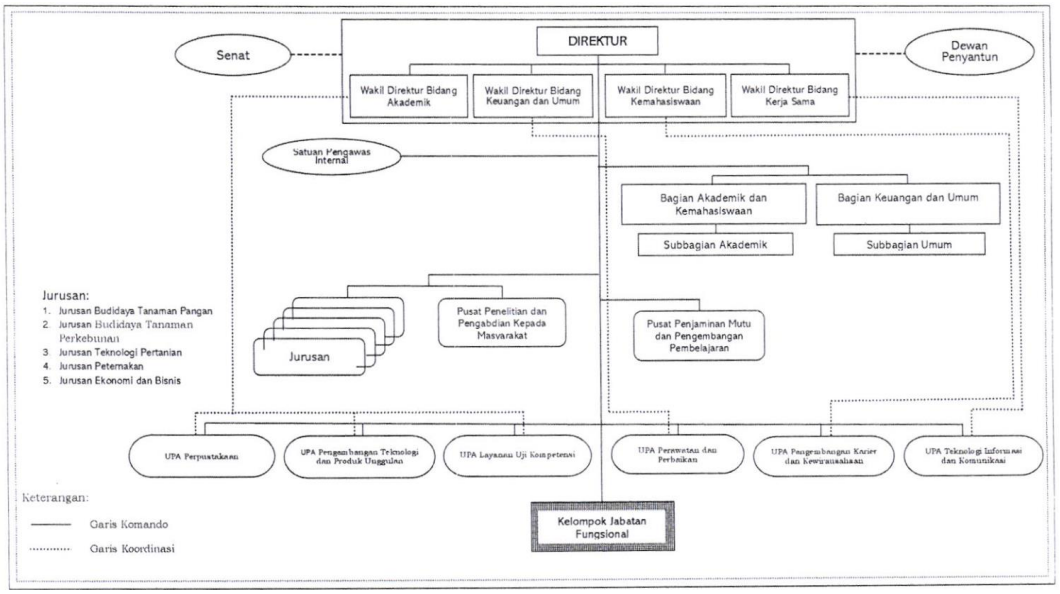
Revolusi industri 4.0 yang ditandai dengan pesatnya perkembangan di bidang *Internet Of Things, Artificial Inteleigent, New Material, Big Data, E-Learning*, dan lain-lainnya membutuhkan perubahan baik untuk lulusan maupun untuk manajemen tata kelola di Polinela sendiri. Untuk lulusan metode-metode pembelajaran yang dikembangkan seperti *Case-Method* dan *Project Based Learning* akan memiliki dampak pergeseran pembelajaran yang sebelumnya dilakukan *teacher center learning* menjadi *student center learning*, serta pembaharuan kurikulum berbasis Merdeka Belajar-Kampus Merdeka mengembangkan pengalaman dan pengetahuan mahasiswa di luar kampus/industri. Dengan semakin hebatnya perkembangan tersebut harus berbanding lurus dengan manajemen yang ada di tingkat perguruan tinggi. Polinela harus mampu mendigitalisasikan kegiatan manajemen, dimulai dari perencanaan hingga pelaksanaan evaluasi sebagaimana fungsi manajemen *Planning-Organizing-Actuating-Controlling.* Polinela selalu berupaya menerapakan *GUG (Good University Governance)* dengan menyusun standar penyelenggaraan pendidikan tinggi yang dapat digambar dengan siklus berikut:



Gambar 2. 1 Siklus Penyelenggaraan Standar Kebijakan Pendidikan Tinggi Polinela

2.2.1 Stuktur Organisasi Politeknik Negeri Lampung

Berdasarkan peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi nomor 59 Tahun 2022 Tentang Organisasi dan Tata Kerja Politeknik Negeri Lampung, unsur pengelola manajemen Politeknik Negeri Lampung Periode Tahun 2022 – 2026 adalah sebagai berikut:



Gambar 2. 2 Struktur Organisasi Politeknik Negeri Lampung Tahun 2022-2026

Organisasi Polinela Terdiri atas:

a) Senat;
b) Pemimpin;
c) Satuan Pengawas Internal; dan
d) Dewa Penyantun.

Pemimpin dan Unsur Organisasi yang terdapat di Polinela terdiri atas :

a) Direktur;
b) Wakil Direktur Akademik;
c) Wakil Direktur Bidang Keuangan dan Umum;
d) Wakil Direktur Bidang Kemahasiswaan;
e) Wakil Direktur Bidang Kerjasama dan Sistem Informasi
f) Kepala Bagian Akademik dan Kemahasiswa (BAK)
g) Kepala Bagian Keuangan dan Umum (BKU)
h) Ketua Jurusan
i) Kepala Pusat Penelitian dan Pengabdian Kepada Masyarakat (PPPM)
j) Kepala Pusat Penjaminan Mutu dan Pengembangan Pembelajaran (PPMPP)
k) UPA Perawatan dan Perbaikan
l) UPA Teknologi Informasi dan Komunikasi (TIK)
m) UPA Pengembangan Teknologi Produk Unggulan
n) UPA *Center For Career and Entrepreneurship Development (CCED)*
o) UPA Perpustakaan
p) Kepala Satuan Pengawas Internal
q) UPA Layanan Uji Kompetensi

Yang mana seluruh pemimpin dan unsur organisasi di atas mengemban tugas masing-masing pada pelaksanaan pendidikan di Polinela [3].

2.2.2 UPA Teknologi Informasi dan Komunikasi (TIK)

Unit Penunjang Akademik (UPA) Teknologi Informasi dan Komunikasi (TIK) yang dahulu dikenal sebagai Unit Pusat Komputer merupakan unit yang melaksanakan pengembangan, pengelolaan dan pemberian layanan teknologi

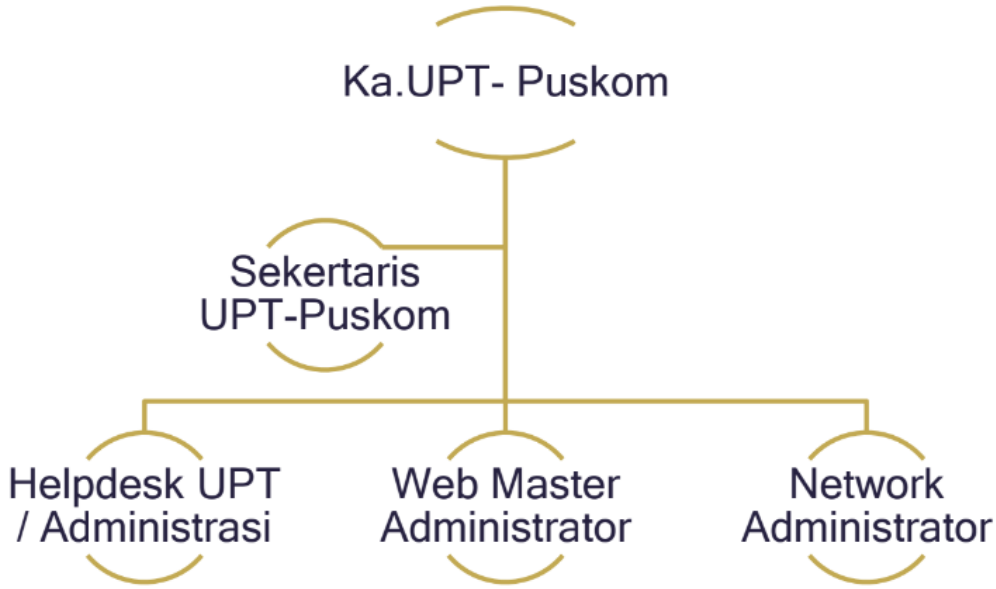
informasi dan komunikasi serta pengelolaan sistem informasi jaringan. UPA TIK merupakan unit perpanjangan tangan dari Wakil Direktur Bidang Kerjasama dan Sistem Informasi.

Adapun berikut Visi dan Misi dan UPA TIK antara lain:

Visi: menjadi pusat pengembangan teknologi informasi dan komputer dalam mendukung Politeknik yang bermutu, inovatif, dan unggul dalam ilmu pengetahuan dan teknologi terapan.

Misi: Merencanakan, mengembangan, mengimplementasikan, dan mensinergikan potensi Sumber Daya Teknologi Informasi dan Komputer guna menunjang kegiatan tridharma perguruan tinggi di Polinela.

Struktur organisasi UPA TIK digambarkan pada gambar berikut:



Gambar 2. 3 Stuktur Organiasi UPA TIK

UPA TIK memiliki satu kepala, sekretaris, dan tiga bidang administrator dalam pelaksanaannya sebagai Unit Penunjang Akademik [19].

2.3 Tata Kelola Teknologi Informasi

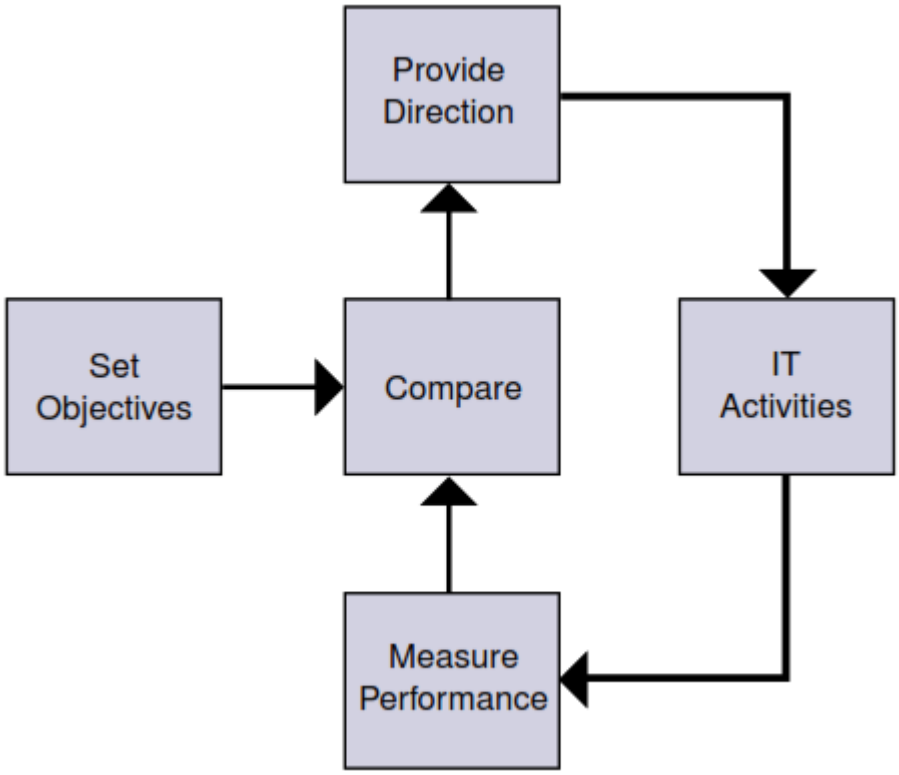
Tata kelola teknologi informasi adalah tanggung jawab dari direksi dan eksekutif manajemen. Hal tersebut merupakan turunan dari tujuan organisasi dan proses organisasi untuk memastikan teknologi informasi bertahan dan memperluas strategi serta tujuan organisasi. Hal yang penting bagi keberhasilan struktur dan proses ini adalah komunikasi yang efektif di antara semua pihak berdasarkan hubungan konstruktif, bahasa yang sama, dan komitmen bersama untuk mengatasi permasalahan. Tanggung jawab tata kelola TI merupakan bagian dari kerangka tata kelola perusahaan yang luas dan harus ditangani dengan serius. Sederhananya, untuk organisasi yang bergantung pada sistem TI, tata kelola harus efektif, transparan, dan akuntabel. Hal ini berarti bahwa direksi harus sangat jelas mengenai tanggung jawabnya sendiri dan tanggung jawab manajemen, dan harus memiliki sistem yang siap melaksanakan tanggung jawab tersebut. Tanggung jawab tersebut berkaitan dengan penyelarasan dan penggunaan TI dalam seluruh aktivitas perusahaan, pengelolaan risiko bisnis terkait teknologi, dan verifikasi nilai yang dihasilkan oleh penggunaan TI di seluruh perusahaan [20].

Tujuan tata kelola TI adalah mengarahkan upaya TI dan untuk memastikan bahwa kinerja TI memenuhi tujuan berikut:

a) Penyelarasan TI dengan perusahaan dan realisasi manfaat yang dijanjikan.
b) Penggunaan TI untuk memberdayakan perusahaan dengan memanfaatkan peluang dan memaksimalkan manfaat.
c) Penggunaan sumber daya TI secara bertanggung jawab.
d) Pengelolaan risiko terkait TI yang tepat.

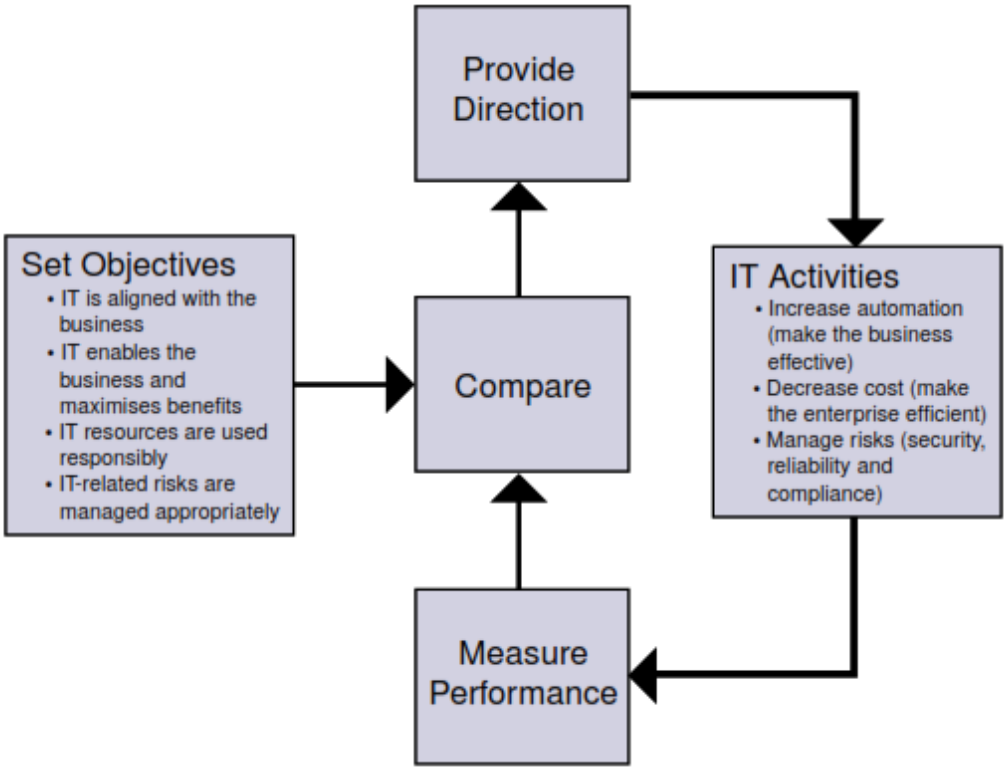
Tata kelola TI dilakukan tersendiri, dengan pemimpin tim melapor dan menerima arahan dari manajer mereka, dengan manajer melapor ke eksekutif, dan eksekutif ke direksi. Laporan yang menunjukkan penyimpangan dari target biasanya berisi rekomendasi tindakan yang harus didukung oleh pimpinan perusahaan. Jelasnya, pendekatan ini tidak akan efektif kecuali strategi dan tujuan telah diturunkan ke dalam organisasi terlebih dahulu. Ilustrasi pada gambar menyajikan secara konseptual interaksi tujuan dan aktivitas TI dari perspektif tata

kelola TI dan dapat diterapkan di antara berbagai lapisan dalam perusahaan. Adapun siklus tata kelola digambarkan pada gambar berikut:



Gambar 2. 4 Interaksi Objektif dan Aktivitas TI

Proses tata kelola dimulai dengan menetapkan tujuan TI perusahaan, memberikan arahan awal. Selanjutnya, siklus berkelanjutan dibentuk untuk mengukur kinerja, membandingkannya dengan tujuan, dan menghasilkan arahan direksi jika diperlukan dan perubahan tujuan jika diperlukan. Meskipun tujuan pada dasarnya merupakan tanggung jawab direksi dan mengukur kinerja adalah tanggung jawab manajemen, jelas bahwa tujuan tersebut harus dikembangkan secara bersamaan sehingga tujuan dapat dicapai dan ukuran tersebut mewakili tujuan dengan benar. Menanggapi arahan yang diterima, fungsi TI perlu fokus pada: mewujudkan manfaat dengan meningkatkan otomatisasi dan menjadikan perusahaan lebih efektif, dan dengan mengurangi biaya dan menjadikan seluruh perusahaan lebih efisien; dan dalam mengelola risiko (keamanan, keandalan, dan kepatuhan). Kerangka tata kelola TI kemudian dapat diselesaikan seperti yang ditunjukkan pada gambar berikut:



Gambar 2. 5 Siklus Tata Kelola TI

Meskipun TI sudah sangat penting bagi keberhasilan perusahaan, memberikan peluang untuk memperoleh keunggulan kompetitif dan menawarkan sarana untuk meningkatkan produktivitas, TI akan melakukan hal tersebut lebih jauh lagi di masa depan. Memanfaatkan TI secara optimal untuk mentransformasikan perusahaan dan menciptakan produk dan layanan bernilai tambah telah menjadi kompetensi bisnis. TI merupakan hal mendasar dalam mengelola sumber daya perusahaan, berhubungan dengan pemasok dan pelanggan, serta memungkinkan transaksi yang semakin global dan tidak berwujud. TI juga merupakan kunci untuk mencatat dan menyebarkan pengetahuan bisnis.

Persentase nilai pasar perusahaan yang semakin besar telah beralih dari nilai berwujud (persediaan, fasilitas, dll.) menjadi tidak berwujud (informasi, pengetahuan, keahlian, reputasi, kepercayaan, paten, dll.). Banyak dari aset ini berkisar pada penggunaan TI. Selain itu, suatu perusahaan pada dasarnya rapuh jika nilainya lebih berasal dari aset konseptual, bukan aset fisik. Oleh karena itu, tata kelola TI yang baik sangat penting dalam mendukung dan mewujudkan tujuan

perusahaan. TI juga membawa risiko. Jelas bahwa saat ini, dalam menjalankan bisnis dalam skala global sepanjang waktu, *downtime system* dan jaringan menjadi terlalu mahal untuk ditanggung oleh perusahaan mana pun. Di beberapa industri, TI merupakan sumber daya kompetitif yang diperlukan untuk membedakan dan memberikan keunggulan kompetitif, sementara di banyak industri lainnya, TI menentukan kelangsungan hidup, bukan hanya kemakmuran.

Dengan TI yang kini begitu melekat dan meresap dalam perusahaan, tata kelola perlu memberikan perhatian khusus terhadap TI, dengan meninjau seberapa kuat perusahaan bergantung pada TI dan betapa pentingnya TI untuk pelaksanaan strategi bisnis, karena:

a) TI sangat penting dalam mendukung dan mewujudkan tujuan perusahaan.
b) TI bersifat strategis bisnis (pertumbuhan dan inovasi).
c) Kebutuhan akan TI berdampak besar pada pendapatan dan pengolahan.

Meskipun direksi biasanya mempertimbangkan strategi bisnis dan risiko strategis, hanya sedikit direksi yang berfokus pada TI, meskipun faktanya hal tersebut melibatkan investasi besar dan risiko besar. Mengapa demikian? Diantara alasannya:

a) TI memerlukan lebih banyak wawasan teknis dibandingkan disiplin ilmu lain untuk memahami bagaimana TI memungkinkan perusahaan dan menciptakan risiko dan peluang.
b) TI secara tradisional diperlakukan sebagai entitas yang terpisah dari bisnis.
c) TI merupakan hal yang kompleks, terlebih lagi pada perusahaan besar yang beroperasi dalam ekonomi jaringan.

Alasan utama pentingnya tata kelola TI adalah karena harapan dan kenyataan sering kali tidak sesuai. Direksi biasanya mengharapkan manajemen untuk:

a) Memberikan solusi TI dengan kualitas yang tepat, tepat waktu dan sesuai anggaran

b) Memanfaatkan dan memanfaatkan TI untuk mengembalikan nilai bisnis
c) Memanfaatkan TI untuk meningkatkan efisiensi dan produktivitas sekaligus mengelola risiko TI

Tata kelola TI yang tidak efektif kemungkinan besar menjadi penyebab utama dari kegagalan proses bisnis, antara lain akan mengakibatkan:

a) Kerugian bisnis, rusaknya reputasi atau melemahnya posisi kompetitif.
b) Menghabiskan sumber daya seperti waktu, biaya, serta kualitas luaran lebih rendah dari perkiraan.
c) Efisiensi perusahaan.
d) Kegagalan TI dalam menghadirkan inovasi atau memberikan manfaat yang dijanjikan.

Meskipun tata kelola TI merupakan tanggung jawab eksekutif dan direksi, aktivitas tata kelola harus mengalir melalui berbagai tingkatan perusahaan. Peningkatan penekanan pada peran tata kelola perusahaan yang lebih luas bagi komite audit. Laporan tersebut meminta direksi untuk memastikan bahwa terdapat proses yang tepat dan efektif untuk memantau risiko dan bahwa sistem pengendalian internal efektif dalam mengurangi risiko tersebut ke tingkat yang dapat diterima. Tata kelola TI seperti sebagian besar aktivitas tata kelola lainnya, secara intensif melibatkan direksi dan manajemen eksekutif secara kooperatif. Namun, karena kompleksitas dan spesialisasinya, direksi dan eksekutif harus menentukan arah dan kendali, dan pada saat yang sama harus bergantung pada lapisan bawah dalam perusahaan untuk memberikan informasi yang diperlukan dalam pengambilan keputusan dan kegiatan evaluasi. Untuk memiliki tata kelola TI yang efektif di perusahaan, lapisan bawah perlu menerapkan prinsip yang sama dalam menetapkan tujuan, memberikan dan mendapatkan arahan, serta menyediakan dan mengevaluasi ukuran kinerja. Oleh karena itu, praktik tata kelola TI yang baik perlu diterapkan di seluruh perusahaan dan khususnya antara fungsi TI dan unit bisnis. Unit bisnis memiliki tanggung jawab untuk bekerja sama dengan

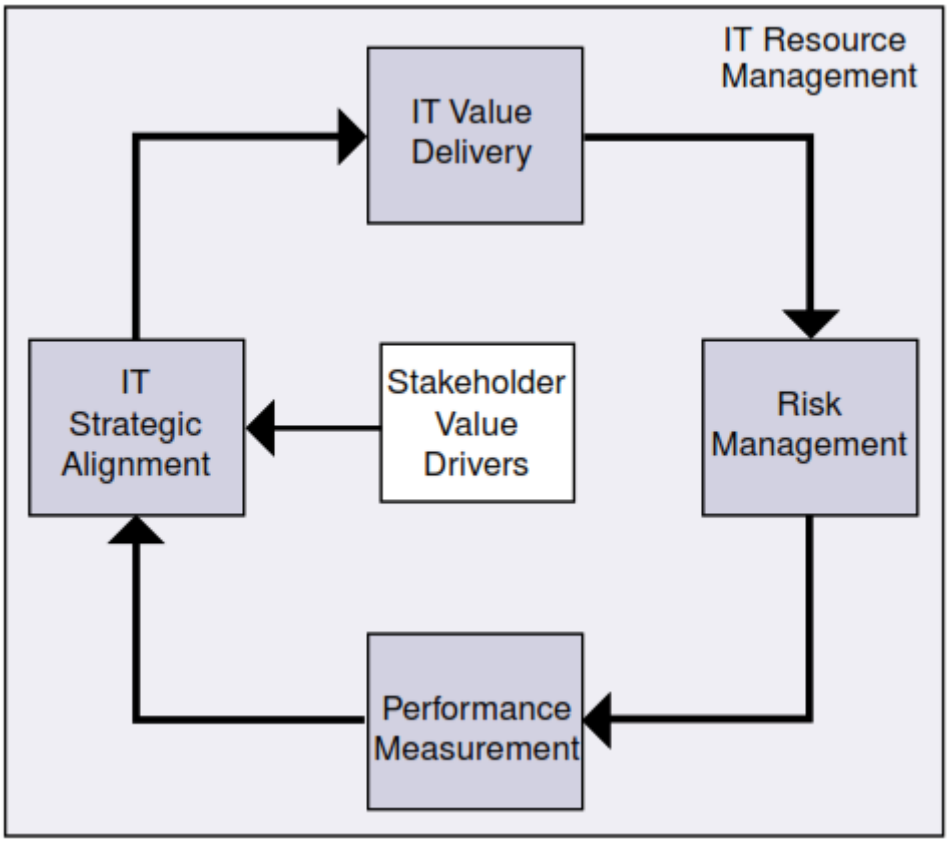
TI untuk memastikan bahwa kebutuhan bisnis mereka terpenuhi. Untuk membantu mengaktifkan ini:

a) Anggota direksi harus berperan aktif dalam strategi TI.
b) Manajer eksekutif harus menyediakan struktur organisasi untuk mendukung penerapan strategi TI.
c) Manajer TI harus berorientasi pada bisnis dan menjadi jembatan antara TI dan bisnis.
d) Semua manajer harus terlibat dalam pengarah TI.

Tanggung jawab tata kelola TI merupakan bagian dari kerangka tata kelola perusahaan yang luas. Kerangka kerja ini tercakup dalam Prinsip Tata Kelola Perusahaan yang berfokus pada hak, peran dan perlakuan adil terhadap pemegang saham, pengungkapan dan transparansi, dan tanggung jawab direksi. Laporan ini lebih lanjut menyerukan kerangka tata kelola untuk memastikan panduan strategis yang baik bagi perusahaan, untuk pemantauan manajemen yang efektif oleh direksi, dan agar direksi bertanggung jawab terhadap perusahaan dan *stakeholder*. Tanggung jawab direksi di antaranya adalah meninjau dan memandu strategi perusahaan, menetapkan dan memantau pencapaian tujuan kinerja manajemen, dan memastikan integritas sistem perusahaan. TI harus ditangani seperti agenda strategis lainnya, seperti sistem TI yang harus memiliki tata kelola yang efektif, transparan, dan akuntabel. Artinya, direksi harus sangat jelas mengenai tanggung jawabnya sendiri dan tanggung jawab manajemen. Perusahaan harus mempunyai sistem yang menerapkan tanggung jawab yang umumnya berkaitan dengan penyelarasan dan penggunaan TI dalam seluruh aktivitas perusahaan, pengelolaan risiko bisnis terkait teknologi, dan verifikasi nilai yang dihasilkan oleh penggunaan TI di seluruh perusahaan.

Pada dasarnya, tata kelola TI memperhatikan dua hal: penyampaian nilai TI bagi bisnis dan mitigasi risiko TI. Pertama didorong oleh keselarasan strategis TI dengan bisnis. Kedua didorong oleh penanaman akuntabilitas dalam perusahaan. Keduanya perlu didukung sumber daya yang memadai dan terukur untuk menjamin diperolehnya hasil. Hal ini mengarah pada lima area fokus utama tata kelola TI, yang semuanya didorong oleh nilai *stakeholder*. Dua di antaranya adalah hasil:

penyampaian nilai dan manajemen risiko. Tiga di antaranya adalah pendorong: penyelarasan strategis, pengelolaan sumber daya (yang mencakup semuanya) dan pengukuran kinerja.



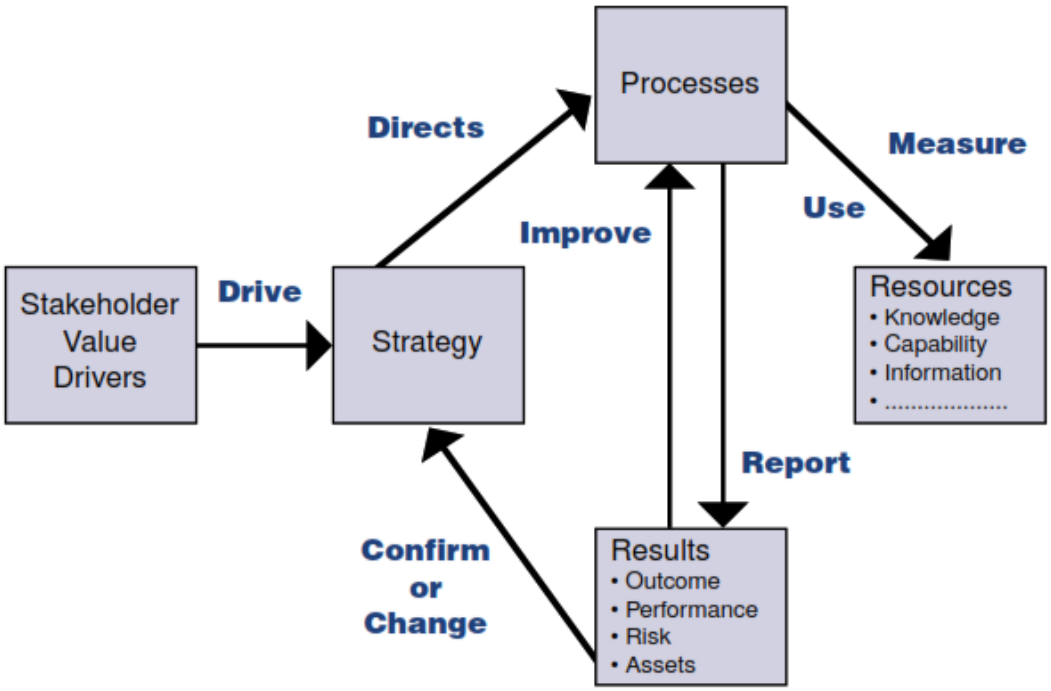
Gambar 2. 6 Fokus Area Tata Kelola TI

Tata kelola TI juga memiliki siklus hidup yang berkesinambungan, yang dapat dimasuki kapan saja. Biasanya seseorang memulai dengan strategi dan penyelarasannya di seluruh perusahaan. Kemudian implementasi dilakukan, memberikan nilai yang dijanjikan oleh strategi dan mengatasi risiko yang memerlukan mitigasi. Secara berkala (beberapa merekomendasikan secara terus menerus) strategi tersebut perlu dipantau dan hasilnya diukur, dilaporkan dan ditindaklanjuti. Umumnya setiap tahun, strategi dievaluasi ulang dan disesuaikan kembali, jika diperlukan. Siklus hidup ini tidak terjadi dalam ruang hampa. Setiap perusahaan beroperasi di lingkungan yang dipengaruhi oleh:

a) Nilai-nilai *stakeholder*.
b) Misi, visi dan nilai-nilai perusahaan.

c) Etika dan budaya masyarakat dan perusahaan.
d) Hukum, peraturan dan kebijakan yang berlaku.
e) Praktik industri.

Tata kelola TI juga merupakan proses di mana strategi TI menggerakkan proses TI, yang memperoleh sumber daya yang diperlukan untuk melaksanakan tanggung jawabnya. Proses TI melaporkan tanggung jawab ini mengenai hasil proses, kinerja, risiko yang dimitigasi dan diterima, serta sumber daya yang dikonsumsi. Laporan-laporan ini harus mengkonfirmasi bahwa strategi telah dilaksanakan dengan benar atau memberikan indikasi bahwa pengalihan strategis diperlukan.



Gambar 2. 7 Proses Tata Kelola TI

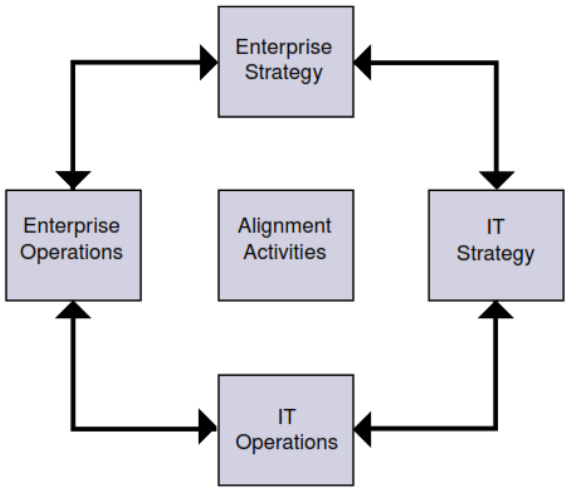
Tata kelola TI memerlukan sejumlah aktivitas bagi direksi dan manajer, seperti mendapatkan informasi tentang peran dan dampak TI pada perusahaan, menetapkan tanggung jawab, menentukan batasan dalam pengoperasian, mengukur kinerja, mengelola risiko, dan memperoleh jaminan. Subjek umum yang tercakup dalam kegiatan ini mencakup tujuan TI, peluang dan risiko teknologi baru, serta proses utama dan kompetensi inti. Isu-isu utama dalam manajemen TI telah berpindah dari

bidang teknologi ke bidang yang berhubungan dengan manajemen. Isu-isu ini jelas terlihat pada bidang tata kelola TI:

a) Penyelarasan strategis, dengan fokus pada penyelarasan bisnis dan solusi kolaboratif.

   Pertanyaan kuncinya adalah apakah investasi suatu perusahaan di bidang TI selaras dengan tujuan strategisnya (niat, strategi saat ini, dan tujuan perusahaan) dan dengan demikian membangun kemampuan yang diperlukan untuk memberikan nilai bisnis. Keadaan harmoni ini disebut sebagai "keselarasan". Hal ini rumit, memiliki banyak segi dan tidak pernah tercapai sepenuhnya. Ini tentang terus bergerak ke arah yang benar dan menjadi lebih selaras dibandingkan pesaing. Hal ini mungkin tidak dapat dicapai oleh banyak perusahaan karena tujuan perusahaan berubah terlalu cepat, namun hal ini tetap merupakan ambisi yang bermanfaat karena terdapat kekhawatiran nyata mengenai nilai investasi TI.

   Penyelarasan TI identik dengan strategi TI, yaitu apakah strategi TI mendukung strategi perusahaan? Untuk tata kelola TI, penyelarasan mencakup lebih dari sekedar integrasi strategis antara organisasi TI (masa depan) dan organisasi perusahaan (masa depan). Hal ini juga berkaitan dengan apakah operasional TI selaras dengan operasional perusahaan saat ini. Tentu saja, sulit untuk mencapai keselarasan TI ketika unit-unit perusahaan tidak selaras. Alur penyelarasaran TI perusahaan digambarkan pada gambar berkut:



Gambar 2. 8 Penyelarasaran TI Perusahaan

Oleh karena itu direksi, atau komite strategi TI yang berdedikasi, harus mendorong penyelarasan bisnis dengan:

- Memastikan bahwa strategi TI selaras dengan strategi bisnis dan strategi TI yang didistribusikan konsisten dan terintegrasi.
- Memastikan bahwa TI memberikan hasil yang sesuai dengan strategi (melaksanakan tepat waktu dan sesuai anggaran, dengan fungsionalitas yang sesuai dan manfaat yang diharapkan sebuah landasan mendasar dalam penyelarasan dan penyampaian nilai) melalui ekspektasi dan pengukuran yang jelas (misalnya, kartu skor bisnis yang seimbang).
- Menyeimbangkan investasi antar sistem yang mendukung perusahaan sebagaimana adanya, mentransformasikan perusahaan atau menciptakan infrastruktur yang memungkinkan bisnis untuk tumbuh dan bersaing di arena baru.
- Membuat keputusan yang dipertimbangkan mengenai fokus sumber daya TI, yaitu penggunaannya untuk memasuki pasar baru, mendorong strategi kompetitif, meningkatkan perolehan pendapatan secara keseluruhan, meningkatkan kepuasan pelanggan dan/atau menjamin retensi pelanggan.

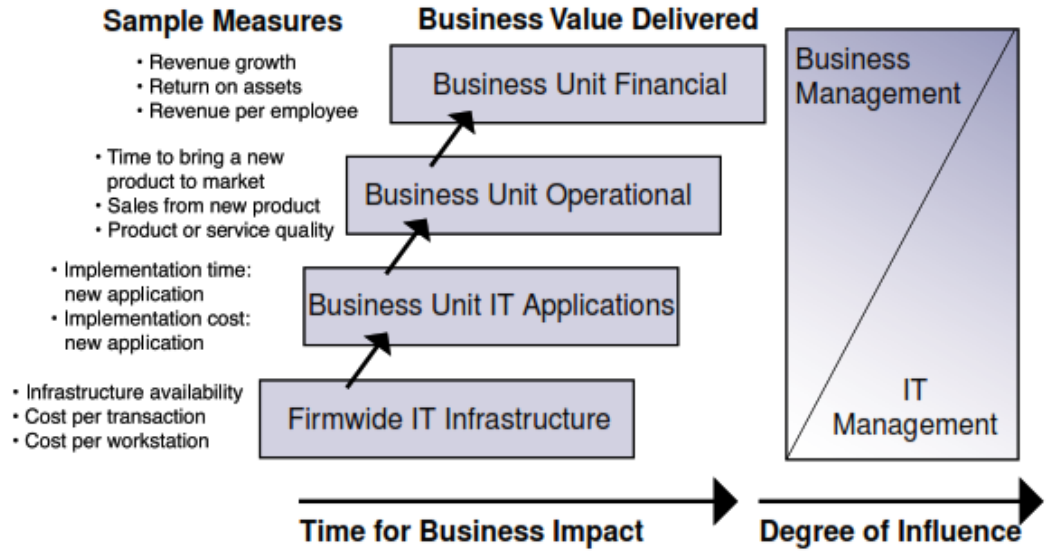
b) Penyampaian nilai, berkonsentrasi pada optimalisasi pengeluaran dan membuktikan nilai TI

Prinsip dasar nilai TI adalah penyampaian kualitas yang tepat waktu dan sesuai anggaran, sehingga mencapai manfaat yang dijanjikan. Dalam istilah bisnis, hal ini sering diterjemahkan menjadi: keunggulan kompetitif, waktu pemenuhan pesanan atau layanan, kepuasan pelanggan, waktu tunggu pelanggan, produktivitas karyawan, dan profitabilitas. Beberapa elemen di atas bersifat subjektif atau sulit diukur, dan hal ini perlu dipahami oleh semua *stakeholder*. Seringkali, manajemen puncak dan direksi takut untuk memulai investasi TI yang besar karena besarnya investasi dan ketidakpastian hasilnya. Agar penyampaian nilai TI yang efektif dapat dicapai, baik biaya aktual maupun laba atas investasi perlu dikelola. Nilai yang ditambahkan TI pada bisnis merupakan fungsi dari sejauh mana organisasi TI selaras dengan bisnis dan memenuhi harapan bisnis. Bisnis

harus menetapkan ekspektasi yang berhubungan dengan isi penyampaian TI:

- Sesuai dengan tujuan, memenuhi kebutuhan bisnis.
- Fleksibilitas untuk mengadopsi persyaratan di masa depan.
- *Throughput* dan waktu respons.
- Kemudahan penggunaan, ketahanan dan keamanan.
- Integritas, keakuratan dan kekinian informasi.

Tingkat manajemen dan pengguna yang berbeda memandang nilai TI secara berbeda, seperti yang diilustrasikan pada gambar. Gambar tersebut juga menunjukkan bahwa semakin tinggi hierarki pengukuran, semakin besar dilusi yang terjadi (yaitu, semakin kecil pengaruh yang dapat diterapkan oleh manajemen TI). Hal ini juga berarti bahwa mengukur dampak investasi TI jauh lebih mudah dilakukan pada hierarki terbawah dibandingkan pada hierarki teratas. Namun, investasi yang sukses di bidang TI mempunyai dampak positif pada keempat tingkat hierarki nilai bisnis. Selain itu, terdapat pemisahan yang semakin besar antara penciptaan nilai dan realisasi selanjutnya. Oleh karena itu, penting untuk tidak hanya berfokus pada pengukuran berdasarkan realisasi nilai (yaitu ukuran keuangan), namun juga memperhitungkan kinerja perusahaan dalam menciptakan nilai.



Gambar 2. 9 Pandangan Nilai TI

Agar berhasil, perusahaan perlu menyadari bahwa konteks strategis yang berbeda memerlukan indikator nilai yang berbeda pula. Ini berarti penting untuk menetapkan ukuran nilai yang selaras antara bisnis dan TI. Hal ini berarti, seperti yang direkomendasikan di bawah ini, bahwa *Balanced Scorecard* TI harus mencakup langkah-langkah ini dan dikembangkan dengan masukan dan persetujuan dari manajemen bisnis. Perlu juga disebutkan bahwa sektor publik mempunyai pendorong atau indikator nilai yang berbeda dengan sektor swasta. Di sektor publik, ukuran-ukuran seperti kepatuhan dan uji tuntas lebih diutamakan dibandingkan ukuran-ukuran keuangan seperti profitabilitas.

c) Manajemen risiko, menangani pengamanan aset TI, pemulihan bencana dan kelangsungan operasi

Kebutuhan universal untuk menunjukkan tata kelola perusahaan yang baik kepada pemegang saham dan pelanggan merupakan pendorong peningkatan aktivitas manajemen risiko di organisasi besar. Risiko perusahaan mempunyai banyak variasi, tidak hanya risiko finansial. Regulator secara khusus menaruh perhatian pada risiko operasional dan sistem, yang mana risiko teknologi dan masalah keamanan informasi merupakan hal yang menonjol. BIS, misalnya, mendukung pandangan tersebut karena semua masalah risiko utama di masa lalu yang diteliti dalam industri keuangan disebabkan oleh kegagalan dalam pengendalian internal, pengawasan, dan TI. Inisiatif perlindungan infrastruktur di AS dan Inggris menunjukkan ketergantungan seluruh perusahaan terhadap infrastruktur TI dan kerentanan terhadap risiko teknologi baru. Rekomendasi pertama yang dibuat oleh inisiatif ini adalah kesadaran risiko bagi para pejabat senior perusahaan.

Oleh karena itu, Direksi harus mengelola risiko perusahaan dengan:

- Memastikan adanya transparansi mengenai risiko-risiko signifikan yang dihadapi perusahaan dan memperjelas kebijakan pengambilan risiko atau penghindaran risiko (yaitu, menentukan selera risiko perusahaan).

- Menyadari bahwa tanggung jawab akhir manajemen risiko berada di tangan Direksi, sehingga ketika mendelegasikannya kepada manajemen eksekutif, pastikan batasan delegasi tersebut dikomunikasikan dan dipahami dengan jelas.
- Menyadari bahwa sistem pengendalian internal yang diterapkan untuk mengelola risiko seringkali mempunyai kapasitas untuk menghasilkan efisiensi biaya.
- Mengingat pendekatan manajemen risiko yang transparan dan proaktif dapat menciptakan keunggulan kompetitif yang dapat dimanfaatkan.
- Mendesak agar manajemen risiko diterapkan dalam operasional perusahaan, merespons dengan cepat terhadap perubahan risiko dan segera melaporkannya ke tingkat manajemen yang tepat, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).

Manajemen risiko yang efektif dimulai dengan pemahaman yang jelas mengenai selera risiko perusahaan dan sesi *brainstorming* mengenai paparan risiko tingkat tinggi yang dimiliki perusahaan. Hal ini memfokuskan seluruh upaya manajemen risiko, dan dalam konteks TI, berdampak pada investasi teknologi di masa depan, sejauh mana aset TI dilindungi, dan tingkat jaminan yang diperlukan. Setelah menetapkan selera risiko dan mengidentifikasi eksposur risiko, strategi pengelolaan risiko dapat ditetapkan dan tanggung jawab diperjelas. Bergantung pada jenis risiko dan signifikansinya terhadap bisnis, manajemen dan Direksi dapat memilih untuk:

• Mitigasi, Menerapkan kontrol (misalnya, memperoleh dan menerapkan teknologi keamanan untuk melindungi infrastruktur TI)

• *Transfer*, Berbagi risiko dengan mitra atau *transfer* ke perlindungan asuransi

• Menerima, Mengakui secara resmi bahwa ada risiko dan memantaunya. Minimal, risiko setidaknya harus dianalisis, karena meskipun tidak ada

tindakan segera yang diambil, kesadaran akan risiko akan mempengaruhi keputusan strategis menjadi lebih baik. Seringkali, risiko TI yang paling merugikan adalah risiko yang tidak dipahami dengan baik.

d) Manajemen sumber daya, optimalisasi pengetahuan dan infrastruktur TI

Kunci keberhasilan kinerja TI adalah investasi optimal, penggunaan dan alokasi sumber daya TI (manusia, aplikasi, teknologi, fasilitas, data) dalam melayani kebutuhan perusahaan. Kebanyakan perusahaan gagal memaksimalkan efisiensi aset TI mereka dan mengoptimalkan biaya yang berkaitan dengan aset tersebut. Selain itu, tantangan terbesar dalam beberapa tahun terakhir adalah mengetahui di mana dan bagaimana melakukan *outsourcing* dan kemudian mengetahui bagaimana mengelola layanan *outsourcing* sedemikian rupa sehingga memberikan nilai yang dijanjikan dengan harga yang dapat diterima.

Direksi perlu melakukan investasi yang tepat dalam infrastruktur dan kemampuan dengan memastikan bahwa:

- Tanggung jawab sehubungan dengan sistem TI dan pengadaan layanan dipahami dan diterapkan
- Ada metode yang tepat dan keterampilan yang memadai untuk mengelola dan mendukung proyek dan sistem TI
- Peningkatan perencanaan tenaga kerja dan investasi dilakukan untuk memastikan rekrutmen dan, yang lebih penting, retensi staf TI yang terampil
- Kebutuhan pendidikan, pelatihan dan pengembangan TI sepenuhnya diidentifikasi dan ditangani untuk semua staf
- Fasilitas yang sesuai disediakan dan tersedia waktu bagi staf untuk mengembangkan keterampilan yang mereka perlukan

Direksi perlu memastikan bahwa sumber daya TI digunakan secara bijaksana dengan memastikan bahwa:

- Metode yang tepat dan keterampilan yang memadai tersedia dalam organisasi untuk mengelola proyek TI
- Manfaat yang diperoleh dari pengadaan jasa apa pun adalah nyata dan dapat dicapai

Aset TI rumit untuk dikelola dan terus berubah karena sifat teknologi dan perubahan kebutuhan bisnis. Manajemen yang efektif atas siklus hidup perangkat keras, lisensi perangkat lunak, kontrak layanan, dan sumber daya manusia permanen dan kontrak merupakan faktor penentu keberhasilan tidak hanya untuk mengoptimalkan basis biaya TI, namun juga untuk mengelola perubahan, meminimalkan insiden layanan, dan menjamin kualitas layanan yang dapat diandalkan. Dari seluruh aset TI, sumber daya manusia mewakili bagian terbesar dari basis biaya dan, secara unit, merupakan sumber daya yang paling mungkin mengalami peningkatan. Penting untuk mengidentifikasi dan mengantisipasi kompetensi inti yang dibutuhkan dalam angkatan kerja. Ketika hal ini dipahami, program rekrutmen, retensi dan pelatihan yang efektif diperlukan untuk memastikan bahwa organisasi memiliki keterampilan untuk memanfaatkan TI secara efektif untuk mencapai tujuan yang telah ditetapkan. Kemampuan untuk menyeimbangkan biaya aset infrastruktur dengan kualitas layanan yang dibutuhkan (termasuk layanan yang disediakan oleh penyedia layanan eksternal yang dialihdayakan) sangat penting untuk keberhasilan penyampaian nilai. Hal ini juga merupakan alasan yang kuat untuk mengadopsi sistem pengukuran kinerja yang baik seperti *Balanced Scorecard.*

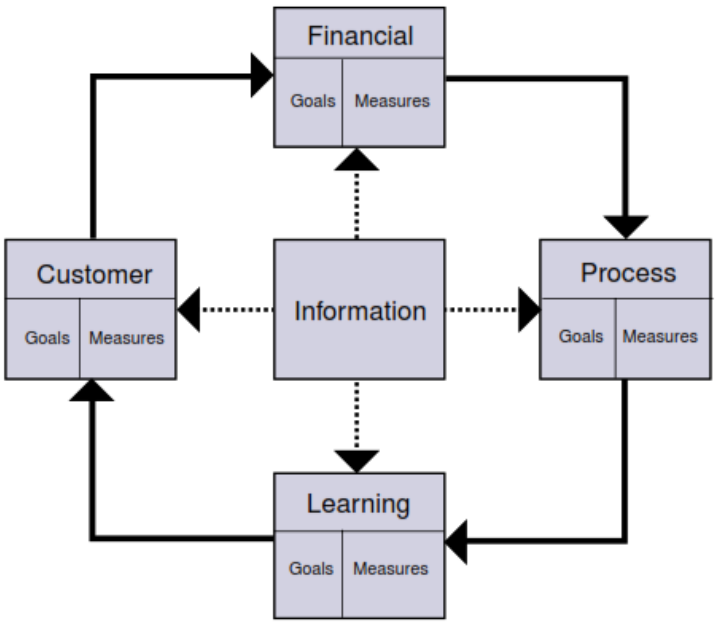
e) Pengukuran Kinerja, mengukur pancapaian *project* dan memantau layanan TI.

   Strategi kini menjadi semakin mendesak ketika perusahaan memobilisasi aset tak berwujud dan tersembunyi untuk bersaing dalam ekonomi global berbasis informasi. Sarana penciptaan nilai telah bergeser dari aset berwujud menjadi aset tidak berwujud, dan aset tidak berwujud pada umumnya tidak dapat diukur melalui sarana keuangan tradisional. *Balanced scorecard* menerjemahkan strategi menjadi tindakan untuk mencapai tujuan dengan sistem pengukuran kinerja yang melampaui akuntansi konvensional, mengukur hubungan dan aset berbasis pengetahuan yang diperlukan untuk bersaing di era informasi: fokus pelanggan, efisiensi proses, dan kemampuan untuk belajar dan berkembang.

Setiap perspektif dirancang untuk menjawab satu pertanyaan tentang cara perusahaan menjalankan bisnis:

- Perspektif finansial, untuk memuaskan *stakeholder*, tujuan finansial apa yang harus kita capai?
- Perspektif pelanggan, untuk mencapai tujuan keuangan kita, kebutuhan pelanggan apa yang harus kita layani?
- Perspektif proses internal, untuk memuaskan pelanggan dan *stakeholder*, proses bisnis internal manakah yang harus kita unggulkan?
- Perspektif pembelajaran, untuk mencapai tujuan kita, bagaimana organisasi kita harus belajar dan berinovasi?

Dengan menggunakan *Balanced Scorecard*, manajer tidak hanya mengandalkan ukuran keuangan jangka pendek sebagai indikator kinerja perusahaan. Mereka juga memperhitungkan hal-hal yang tidak berwujud seperti tingkat kepuasan pelanggan, perampingan fungsi internal, penciptaan efisiensi operasional dan pengembangan keterampilan staf. Pandangan operasi bisnis yang unik dan lebih holistik ini berkontribusi dalam menghubungkan tujuan strategis jangka panjang dengan tindakan jangka pendek.



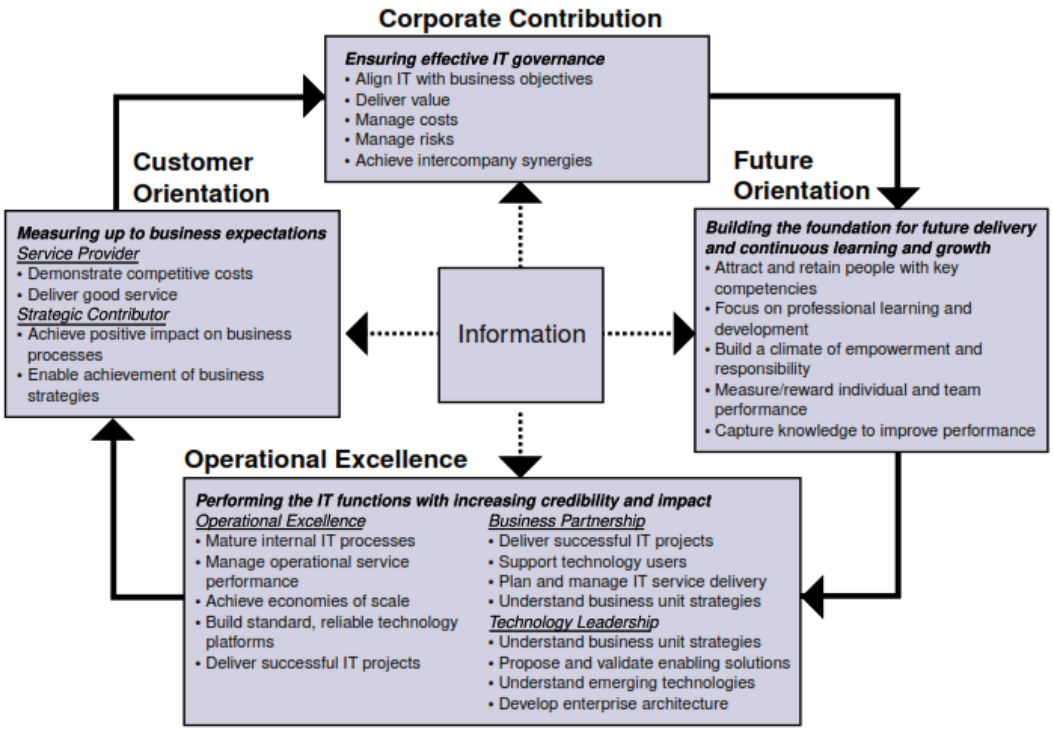
Gambar 2. 10 *Balanced Scorecard Dimension*

TI juga memungkinkan dan mempertahankan solusi untuk tujuan aktual yang ditetapkan dalam dimensi keuangan (manajemen sumber daya perusahaan), pelanggan (manajemen hubungan pelanggan), proses (intranet dan alur kerja) dan pembelajaran (manajemen pengetahuan) pada kartu skor.

TI tidak hanya menyumbangkan informasi ke dalam kartu skor bisnis dan alat-alat untuk berbagai dimensi yang diukur, namun juga karena pentingnya TI itu sendiri membutuhkan kartu skornya sendiri. Mendefinisikan tujuan yang jelas dan langkah-langkah yang baik yang secara jelas mencerminkan dampak bisnis dari tujuan TI merupakan sebuah tantangan dan perlu diselesaikan melalui kerjasama antar lapisan tata kelola yang berbeda dalam perusahaan.

Penggunaan *Balanced Scorecard* TI (IT BSC) adalah salah satu cara paling efektif untuk membantu Direksi dan manajemen mencapai keselarasan TI dan bisnis. Tujuannya adalah untuk membangun sarana pelaporan manajemen kepada Direksi, untuk menumbuhkan konsensus di antara para *stakeholder* utama mengenai tujuan strategis TI, untuk menunjukkan efektivitas dan nilai tambah TI dan untuk mengkomunikasikan kinerja, risiko, dan kemampuan TI. Untuk menerapkan konsep *Balanced Scorecard* pada fungsi TI, keempat perspektif tersebut perlu didefinisikan ulang. *Template IT* BSC dapat dikembangkan dengan mempertimbangkan pertanyaan-pertanyaan berikut:

- Kontribusi perusahaan, Bagaimana pandangan eksekutif bisnis terhadap departemen TI?
- Orientasi pengguna, Bagaimana pandangan pengguna terhadap departemen TI?
- Keunggulan operasional, Seberapa efektif dan efisien proses TI?
- Orientasi masa depan, Seberapa baik posisi TI untuk memenuhi kebutuhan masa depan?



Gambar 2. 11 Contoh Pengukuran IT *Fbag*

Gambar diatas merangkum tujuan masing-masing bidang spesifik yang menjadi dasar pengukuran, dan bagian 7 memberikan beberapa contoh pengukuran untuk manajemen dan mereka yang bertanggung jawab atas tata kelola TI.

2.4 Manajemen Risiko Teknologi Informasi

Risiko merupakan peluang terjadinya sesuatu yang memiliki dampak pada suatu proses bisnis [4]. Dampak yang dihasilkan dari sebuah risiko tersebut berupa hal negatif yang merugikan. Karena risiko bersifat memiliki suatu dampak dan probabilitas yang apabila dapat kita proses dengan baik akan dapat menghasilkan pembelajaran baru. Karenanya risiko perlu diidentifikasi dan diantisipasi dengan menggunakan suatu proses manajemen risiko.

Manajemen risiko adalah segala proses kegiatan yang dilakukan untuk meminimalkan bahkan mencegah terjadinya risiko perusahaan [21]. Atau berikut beberapa pengertian manajemen risiko lainnya:

1. Manajemen risiko adalah aktivitas manajemen yang dilakukan berdasarkan tingkatan pada tingkat pimpinan pelaksana. Kegiatan penemuan serta analisis sistematis terhadap kerugian yang mungkin dihadapi oleh perusahaan atau organisasi [22].
2. Manajemen risiko adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi berkenaan dengan risiko sehingga risiko yang ditimbulkan tidak memberikan dampak yang signifikan dan merugikan organisasi [23].

Suksesnya manajemen risiko akan tergantung pada efektifitas kerangka kerja manajemen yang menyediakan dasar dan pengaturan yang akan melekat pada keseluruhan organisasi pada semua tingkatan. Kerangka kerja tersebut membantu dalam pengelolaan risiko secara efektif melalui pengaplikasian dari proses manajemen risiko pada beragam tingkatan dan dalam konteks khusus organisasi [24]. Kerangka kerja tersebut memastikan bahwa informasi mengenai risiko yang berasal dari proses manajemen risiko dilaporkan secara memadai serta digunakan sebagai dasar pengambilan keputusan dan akuntabilitas pada semua tingkatan organisasi secara relevan.

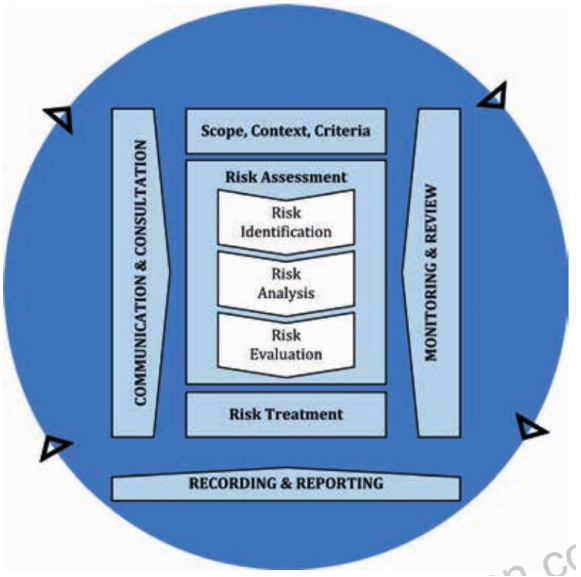
Gambar 2. 12 Komponen Kerangka Kerja

Kerangka kerja ini tidak dimaksudkan untuk menjelaskan sebuah sistem manajemen, namun lebih untuk membantu organisasi untuk mengintegrasikan manajemen risiko ke dalam keseluruhan sistem manajemen. Oleh karena itu,

organisasi sebaiknya mengadaptasi komponen-komponen dari kerangka kerja yang sesuai kebutuhan spesifi organisasi [8].

2.5 ISO 31000:2018

Proses manajamen risiko sebaiknya merupakan bagian yang terpadu dari manajemen, menyatu dalam budaya dan praktik, dan disesuaikan penggunaannya dengan proses bisnis organiasi. Proses manajemen risiko dijelaskan pada gambar dibawah ini [8].



Gambar 2. 13 Proses Manajemen Risiko

2.5.1 Komunikasi dan Konsultasi

Komunikasi dan konsultasi dengan *stakeholder* eksternal dan internal sebaikanya dilaksanakan selama proses manajemen risiko di semua tahapan. Oleh karena itu rencana komunikasi dan konsultasi sebaiknya dikembangkan sejak tahap awal. Dengan ini sebaiknya membahas isu yang berkaitan dengan risiko itu sendiri, penyebabnya, konsekuensinya (jika diketahui), dan tindakan yang perlu diambil untuk mengatasinya. Komunikasi dan konsultasi pada *stakeholder* ini penting karena memberikan penilaian tentang risiko berdasarkan persepsi setiap *stakeholder*.

2.5.2. Penetapan Suatu Ruang Lingkup, Konteks, dan Kriteria

Dengan penetapan suatu konteks, organisasi mengartikulasikan sasarannya, mendefinisikan parameter internal dan eksternal yang diperhitungkan pada saat pengelolaan risiko, serta menetapkan lingkup kerja dan kriteria risiko untuk proses yang masih ada. Pada konteks eksternal didefinisikan sebagai lingkungan eksternal di mana organisasi berusaha untuk mencapai sasarannya, contohnya budaya, sosial, politik, hukum, peraturan, teknologi dan lain-lain. Sedangkan pada konteks internal didefinisikan sebagai lingkungan internal di mana organisasi berusaha untuk mencapai sasarannya. Konteks internal ini harus selaras dengan konteks eksternal. Contoh dari konteks internal ini adalah tata kelola, kebijakan, sasaran, dan strategi, kemampuan, hubungan terakait, sistem informasi dan lain-lain.

Sasaran, strategi, ruang lingkup, dan parameter dari kegiatan organisai atau bagian lain dari organiasasi di mana proses manajemen risiko diterapkan, sebaiknya ditetapkan. Pengelolaan risiko sebaiknya dilakukan dengan penuh pertimbangan atas kebutuhan guna menjustifikasi penggunaan sumber daya dalam penyelenggaraan manajemen risiko. Sumber daya yang diperlukan, tanggung jawab dan wewenang, serta rekaman yang akan disimpan sebaiknya juga terperinci. Penetapan konteks ini meliputi:

- Pendefinisian tujuan dan sasaran dari kegiatan manajemen risiko.
- Pendifinisian tanggung jawab untuk dan dalam proses manajemen risiko.
- Pendefinisian ruang lingkup, serta kedalaman dan keluasan dari aktivitas manajemen risiko.
- Pendifinisian kegiatan, proses, fungsi, proyek, produk, jasa, atau aset dalam kaitannya lokasi dan waktu.
- Pendefinisian hubungan antara proyek proses, atau aktivitas tertentu dengan proyek proses, atau aktivitas lain dari organisasi.
- Pendefinisian metodologi penilaian risiko.
- Pendefinisian cara kerja dan efektivitas manajemen risiko di evaluasi.
- Pengidentifikasian dan spesifikasi keputusan-keputusan yang sebaiknya diambil.

- Pengidentifikasian, pelingkupan, ataupun pengerangkaan studi yang diperlukan cakupan dan sasarannya, serta sumber daya yang diperlukan untuk melakukan studi tersebut.

Pada penetapan konteks juga perlu didefinisikan suatu kriteria risiko yang akan digunakan untuk mengevaluasi signifikansi risiko. Kriteria tersebut sebaiknya merefleksi nilai, sasaran serta sumber daya organisasi. Kriteria risiko sebaiknya konsisten dengan kebijakan manajemen risiko, didefinisikan pada awal di setiap proses manajemen risiko, dan ditinjau secara berkesinambungan. Beberapa faktor yang perlu diperhatikan sebaiknya mencakupi

- Sifat dan jenis penyebab dan konsekuensi yang dapat terjadi dan bagaimana hal tersebut akan diukur.
- Bagaimana kemungkinan-kejadian akan didefinisikan.
- Kerangka waktu dari kemungkinan-kejadian dan/atau konsekuensinya.
- Bagaimana tingkat risiko akan ditentukan.
- Pandangan dari para *stakeholder*.
- Tingkat risiko yang dapat diterima atau dapat ditolerir.
- Apakah kombinasi risiko berganda sebaiknya diperhitungkan dan jika demikian, bagaimana dan kombinasi mana yang sebaiknya dipertimbangkan.

2.5.3 Penilaian Risiko

Penilaian risiko adalah keseluruhan proses dari identifikasi risiko, analisis risiko serta evaluasi risiko. Pada penilaiannya ini terbagi menjadi tiga proses antara lain:

2.5.3.1 Identifikasi Risiko

Tujuan dari identifikasi risiko adalah untuk menemukan, memahami, dan mendeskripsikan risiko yang dapat membantu atau mencegah objektif dari pencapaian suatu tujuan organisasi. Informasi yang relevan, sesuai dan up-to-date merupakan hal yang penting pada saat identifikasi risiko.

Organisasi dapat menggunakan berbagai macam teknik untuk mengidentifikasi ketidakpastian yang mungkin dapat mempengaruhi satu atau lebih objektif. Berikut

adalah beberapa faktor dan hubungan antara faktor berikut yang dapat dipertimbangkan

- Sumber risiko yang nyata dan tidak nyata
- Akibat dan *event*
- Ancaman dan peluang
- Ketidakmampuan dan kemampuan
- Perubahan external dan internal konteks
- Indikator risiko yang muncul
- Asal dan nilai dari asset dan *resource*
- Konsekuensi dan dampak terhadap objektif
- Keterbatasan pengetahuan dan dan informasi yang diyakini
- Faktor waktu
- Bias, asumsi dan kepercayaan terhadap yang terlibat

2.5.3.2. Analisis Risiko

Analisis risiko melibatkan pengembangan suatu pemahaman atas risiko. Analisis risiko menyediakan suatu masukan dalam evaluasi risiko dan dalam membuat keputusan apakah risiko membutuhkan perlakuan atau tidak, serta keputusan dalam penentuan metodologi dan strategi perlakuan risiko yang paling layak. Analisis risiko juga dapat menyediakan suatu masukan dalam pengambilan keputusan di mana ada beberapa pilihan harus dibuat dan berbagai opsi yang melibatkan jenis dan tingkatan risiko yang berbeda-beda. Analisis risiko melibatkan pertimbangan atas penyebab dan sumber risiko, konsekuensi positif negatif, serta kemungkinan-kejadian konsekuensi tesebut dapat terjadi Risiko yang dianalisis dapat digambarkan dalam sebuah matrik risiko yang biasanya digambarkan dengan perbandingan antara dampak dan tingkat kemungkinan terjadinya sehingga menghasilkan penilaian terhadap risiko tersebut. Adapun penilaian terhadap risiko tersebut wajib dikomunikasikan terhadap *stakholder* dan diberikan pertimbangan terhadap risiko tersebut. Adapun matrik risiko biasanya digambarkan sebagai berikut:

Tabel 2. 1 Matrik Risiko

Tingkat Kemungkinan/ Dampak	SR	R	S	B	E
SK	R	R	R	R	M
K	R	M	M	M	T
S	R	M	M	M	T
B	R	M	M	T	T
SB	M	M	T	T	T

Dengan tingkat kemungkinan dikategorikan sebagai berikut:

- Sangat Besar (SB)
- Besar (B)
- Sedang (S)
- Kecil (K)
- Sangat Kecil (SK)

Sedangkan untuk dampak yang dihasilkan dikategorikan sebagai berikut:

- Ekstrem (E)
- Besar (B)
- Sedang (S)
- Rendah (R)
- Sangat Rendah (SR)

Dan menghasilkan risiko dengan tingkat

- Rendah (R)
- Menengah (M)
- Tinggi (T)

Analisis risiko dapat dilaksanakan dengan tingkat kerincian yang bervariasi, tergantung pada risiko tersebut, tujuan dan analisis, serta informasi, data dan sumber daya yang tersedia. Analisis dapat berbentuk kualitatif, semi kualitatif, atau kuantitatif, ataupun kombinasinya.

2.5.3.3 Evaluasi Risiko

Tujuan dari evaluasi risiko adalah membantu pengambilan keputusan, berdasarkaan manfaat keluaran dari analisis risiko, tentang risiko mana yang membutuhkan perlakuan serta implementasi perlakuan. Evaluasi risiko melibatkan perbandingan tingkat risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan ketika konteks tersebut dipertimbangkan. Keputusan sebaiknya memperhitungkan konteks risiko yang lebih luas dan mencakupi pertimbangan toleransi risiko yang ditanggung oleh pihak di luar organisasi yang diuntungkan dari risiko, keputusan sebaiknya dibuat sesuai dengan hukum peraturan, dan ketentuan lainnya.

Dalam keadaan tertentu, evaluasi risiko tersebut dapat mengarah pada suatu keputusan untuk melakukan analisis lebih lanjut serta untuk tidak memperlakukan risiko selain mempertahankan pengendalian yang ada.

2.5.4 Perlakuan Risiko

Perlakuan risiko melibatkan pemilihan satu opsi atau lebih untuk pemodifikasian risiko dan pengimplementasian opsi tersebut. Begitu diimplementasikan, perlakuan risiko menyediakan atau memodifikasi pengendalian yang sudah ada. Perlakukan risiko melibatkan suatu siklus yang terdiri dari :

- Penialaian suatu perlakuan risiko.
- Pemutusan apakah tingkat risiko residu dapat ditoleransi.
- Jika tidak dapat ditoleransi, perlu dihasilkan suatu perlakuan risiko baru.
- Penilaian efektifitas dari perlakuan risiko tersebut.

Untuk pemilihan opsi perlakuan risiko akan menimbang kelayakan terkait biaya dan upaya implementasi dengan manfaat yang diperoleh. Dalam pemilihan opsi perlakuan risiko, suatu organisasi sebaiknya mempertimbangkan nilai-nilai dan persepsi para *stakeholder* serta cara yang paling layak. Ketika opsi perlakuan risiko dapat berdampak pada risiko di tempat lain dalam organisasi atau dengan

stakeholder, mereka sebaiknya diikutsertakan dalam pengambilan keputusan. Suatu rencana perlakuan risiko sebaiknya dapat mengidentifikasi secara jelas urutan prioritas dalam hal perlakuan risiko individual dan dapat diimplementasikan serta dapat juga menghadirkan risiko. Risiko yang signifikan dapat merupakan suatu kegagalan atau ketidakefektifan dari tindakan perlakuan risiko. Pemantauan merupakan hal yang penting dan terpadu dari rencana perlakuan risiko.

Tujuan dari rencana perlakuan risiko adalah mendokumentasikan bagaimana opsi perlakuan yang terpilih akan diimplementasikan. Informasi yang tersedia dalam rencana perlakuan risiko antara lain:

- Suatu alasan untuk memilih opsi perlakuan, termasuk manfaat yang diharapkan yang ini diperoleh.
- Pihak yang akuntabel untuk persetujuan suatu rencana dan pihak yang bertanggung jawab untuk pengimplementasian rencana tersebut.
- Tindakan yang diusulkan.
- Persyaratan sumber daya termasuk kontijensi.
- Pengukuran kinerja dan batasannya.
- Persyaratan pelaporan pemantauan.
- Waktu dan jadwal.

2.5.5 Pemantauan dan Tinjauan

Pemantauan dan tinjauan menjadi suatu bagian yang terencana dalam proses manajemen risiko serta melibatkan pemeriksaan reguler. Proses pemantauan dan tinjauan dalam suatu organisasi sebaiknya mencakup semua aspek dari suatu proses manajemen risiko untuk mencapai tujuan dari:

- Pemastian bahwa pengendalian efisien dan efektif baik rancangan maupun pelaksanaan.
- Pengumpulan informasi lebih lanjut untuk mengembangkan penilaian risiko.
- Pengumpulan informasi lebih lanjut untuk mengembangkan penilaian risiko.
- Analisis dan proses pembelajaran dari kejadian, perubahan, tren, keberhasilan dan kegagalan.

- Pendeteksian perubahan dalam konteks eksternal dan internal.
- Pengidentifikasian risiko baru yang muncul.

Hasil pemantauan dan tinjauan sebaiknya direkam, dan dilaporkan selayaknya kepada eksternal dan internal dan sebaiknya juga digunakan sebagai masukan untuk suatu tinjauan terhadap kerangka kerja manajemen risiko.

2.5.6 Pencatatan dan Pelaporan

Proses manajemen risiko dan keluarannya perlu di dokumentasikan dan dilaporkan dalam mekanisme yang sesuai. Pencatatan dan pelaporan ditujukan untuk:

- Mengkomunikasikan kegiatan manajemen risiko dan keluarannya di dalam organisasi
- Memberikan informasi untuk pengambilan keputusan
- Meningkatkan manajemen risiko
- Membantu interaksi dengan stakeholder, termasuk yang bertanggung jawa untuk manajemen risiko

Pengambilan keputusan memperhatikan suatu ciptaan, ingatan, dan penanganan dari dikomen yang perlu diperhatikan atau dibuat, namun tidak terbatas dari: kegunaannya, sensitifitas informasinya, dan eksternal dan internal konteks.

Pelaporan merupakan bagian yang tidak terpisahkan dari tata kelola organisasi dan meningkatkan kualitas dialog dengan *stakeholder* dan mendukung manajemen dan seluruh yang bagian dalam memenuhi tanggung jawab mereka. Faktor-faktor yang perlu dipertimbangkan dalam pelaporan mencakup:

- pemangku kepentingan yang berbeda serta kebutuhan dan persyaratan informasi spesifik mereka;
- biaya, frekuensi dan ketepatan waktu pelaporan;
- Metode pelaporan
- Hubungan antara informasi terhadap objektif dan pengambilan keputusan organisasi

2.6 COBIT 2019

Mengingat transformasi digital, informasi dan teknologi (TI) menjadi sangat penting dalam mendukung, keberlanjutan, dan pertumbuhan perusahaan. Sebelumnya, direksi dan manajemen senior dapat mendelegasikan, mengabaikan atau menghindari keputusan terkait TI. Sebagian besar sektor dan industri, sikap seperti ini kini tidak bijaksana. Penciptaan nilai *stakeholder* (yaitu mewujudkan manfaat dengan biaya sumber daya yang optimal sambil mengoptimalkan risiko) sering kali didorong oleh digitalisasi tingkat tinggi dalam model bisnis baru, proses yang efisien, inovasi yang sukses, dll. Perusahaan-perusahaan yang terdigitalisasi semakin bergantung pada TI untuk kelangsungan hidup dan pertumbuhan [5].

Mengingat pentingnya TI untuk manajemen risiko perusahaan dan penciptaan nilai, fokus khusus *pada governance of information and technology (EGIT)* telah muncul selama tiga dekade terakhir. EGIT merupakan bagian integral dari tata kelola perusahaan. Hal ini dilaksanakan oleh Direksi yang mengawasi definisi dan penerapan proses, struktur, dan mekanisme relasional dalam organisasi yang memungkinkan pelaku bisnis dan TI melaksanakan tanggung jawab mereka dalam mendukung penyelarasan bisnis atau TI dan penciptaan nilai bisnis dari dukungan TI; investasi bisnis.

Gambar 2. 14 Tata Kelola Perusahaan dari TI

Tata kelola informasi dan teknologi perusahaan bersifat kompleks dan beragam. Tidak ada solusi jitu (atau cara ideal) untuk merancang, menerapkan, dan memelihara EGIT yang efektif dalam suatu organisasi. Oleh karena itu, anggota direksi dan manajemen senior biasanya perlu menyesuaikan langkah-langkah dan implementasi EGIT mereka sesuai dengan konteks dan kebutuhan spesifik mereka. Mereka juga harus bersedia menerima akuntabilitas yang lebih besar terhadap TI dan mendorong pola pikir dan budaya yang berbeda untuk memberikan nilai dari TI [25].

COBIT sebagai kerangka kerja tata kelola TI sudah dikembangkan oleh EGIT selama 25 tahun lebih sebagai *best practices* di lapangan. Kerangka COBIT membuat perbedaan yang jelas antara tata kelola dan manajemen. Kedua disiplin ilmu ini mencakup aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda, dan memiliki tujuan yang berbeda. Tata kelola memastikan bahwa:

- Kebutuhan, kondisi dan pilihan *stakeholders* dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati.
- *Direction* ditentukan melalui penentuan prioritas dan pengambilan keputusan.
- *Performance dan Compliance* dipantau berdasarkan arah dan tujuan yang disepakati.

Di sebagian besar perusahaan, tata kelola secara keseluruhan merupakan tanggung jawab direksi. Tanggung jawab tata kelola yang spesifik dapat didelegasikan kepada struktur organisasi khusus pada tingkat yang sesuai, khususnya di perusahaan yang lebih besar dan kompleks. Manajemen merencanakan, membangun, menjalankan dan memantau aktivitas, sejalan dengan arahan yang ditetapkan oleh badan tata kelola, untuk mencapai tujuan perusahaan. COBIT mendefinisikan komponen untuk membangun dan mempertahankan sistem tata kelola: proses, struktur organisasi, kebijakan dan prosedur, arus informasi, budaya dan perilaku, keterampilan, dan infrastruktur. COBIT mendefinisikan faktor desain yang harus dipertimbangkan oleh perusahaan untuk membangun sistem tata kelola yang paling sesuai. COBIT mengatasi masalah tata kelola dengan mengelompokkan komponen tata kelola yang relevan ke dalam tujuan tata kelola dan manajemen yang dapat dikelola hingga tingkat kemampuan yang diperlukan. Target audiens COBIT adalah *stakeholder* EGIT dan lebih jauh lagi, *stakeholder* tata kelola perusahaan. Manfaat yang diperoleh *stakeholder* dari COBIT dapat dilihat pada gambar berikut

Tabel 2. 2 *Stakeholder* pada COBIT

Stakeholder	Manfaat dari COBIT
Internal	

Stakeholder	Manfaat dari COBIT
Direksi	Memberikan wawasan tentang cara mendapatkan manfaat dari penggunaan TI dan menjelaskan tanggung jawab direksi yang relevan.
Executive Management	Memberikan panduan tentang cara mengatur dan memantau kinerja TI di seluruh perusahaan.
Manajer Bisnis	Membantu memahami cara mendapatkan solusi TI yang dibutuhkan perusahaan dan cara terbaik memanfaatkan teknologi baru untuk peluang strategis baru.
Manajer TI	Memberikan panduan tentang cara terbaik untuk membangun dan menyusun departemen TI, mengelola kinerja TI, menjalankan operasi TI yang efisien dan efektif, mengendalikan biaya TI, menyelaraskan strategi TI dengan prioritas bisnis, dll.
Penyedia Asuransi	Membantu mengelola ketergantungan pada penyedia layanan eksternal, mendapatkan jaminan atas TI, dan memastikan keberadaan sistem pengendalian internal yang efektif dan efisien.
Manajemen Risiko	Membantu memastikan identifikasi dan pengelolaan semua risiko terkait TI.
Eksternal	
Pembuat Kebijakan	Membantu memastikan perusahaan mematuhi aturan dan regulasi yang berlaku serta memiliki sistem tata kelola yang tepat untuk mengelola dan mempertahankan kepatuhan.

Tabel 2. 2 Stakeholder pada COBIT (Lanjutan)

Partner Bisnis	Membantu memastikan bahwa operasional mitra bisnis aman, andal, dan mematuhi peraturan dan ketentuan yang berlaku.
Vendor TI	Membantu memastikan bahwa operasi *vendor* TI aman, andal, dan mematuhi aturan dan regulasi yang berlaku.

Tingkat pengalaman tertentu dan pemahaman menyeluruh tentang perusahaan diperlukan untuk mendapatkan manfaat dari kerangka COBIT. Pengalaman dan pemahaman tersebut memungkinkan pengguna untuk menyesuaikan panduan inti COBITyang bersifat umum menjadi panduan yang disesuaikan dan terfokus untuk perusahaan, dengan mempertimbangkan konteks perusahaan. Sasarannya mencakup mereka yang bertanggung jawab sepanjang siklus hidup solusi tata kelola, mulai dari perancangan, pelaksanaan, hingga penjaminan. Memang benar, penyedia jaminan dapat menerapkan logika dan alur kerja yang dikembangkan dalam publikasi ini untuk menciptakan program jaminan yang dapat dibuktikan dengan baik bagi perusahaan.

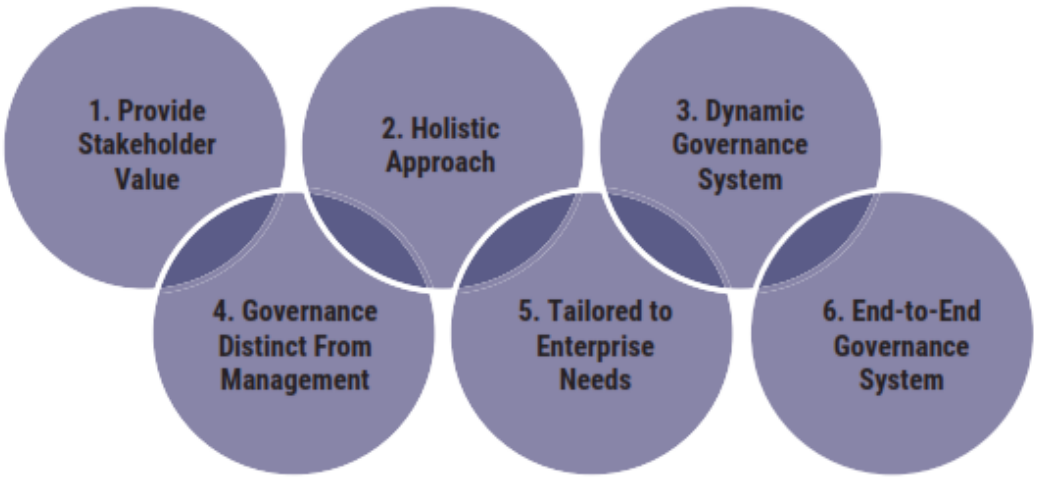
COBIT 2019 dikembangkan berdasarkan dua prinsip:

1 Prinsip yang menjelaskan persyaratan inti sistem tata kelola informasi dan teknologi perusahaan.
2 Prinsip-prinsip kerangka tata kelola yang dapat digunakan untuk membangun sistem tata kelola bagi perusahaan.

COBIT 2019 memiliki enam prinsip tata kelola antara lain:

1. Setiap perusahaan memerlukan sistem tata kelola untuk memenuhi kebutuhan *stakeholder* dan menghasilkan nilai dari penggunaan TI. Nilai mencerminkan keseimbangan antara manfaat, risiko, dan sumber daya, dan perusahaan memerlukan strategi dan sistem tata kelola yang dapat ditindaklanjuti untuk mewujudkan nilai ini.

2. Sistem tata kelola untuk TI perusahaan dibangun dari sejumlah komponen yang bisa berbeda jenisnya dan bekerja sama secara *holistic.*
3. Sistem pemerintahan harus bersifat dinamis. Artinya, setiap kali satu atau lebih faktor desain diubah (misalnya perubahan strategi atau teknologi), dampak perubahan tersebut terhadap sistem EGIT harus dipertimbangkan. Pandangan dinamis tentang EGIT akan mengarah pada sistem EGIT yang layak dan tahan masa depan.
4. Sistem tata kelola harus secara jelas membedakan antara aktivitas dan struktur tata kelola dan manajemen.
5. Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan, dengan menggunakan serangkaian faktor desain sebagai parameter untuk menyesuaikan dan memprioritaskan komponen sistem tata kelola.
6. Sistem tata kelola harus mencakup seluruh perusahaan, dengan fokus tidak hanya pada fungsi TI namun pada semua teknologi dan pemrosesan informasi yang diterapkan perusahaan untuk mencapai tujuannya, terlepas dari lokasi pemrosesan di perusahaan tersebut.



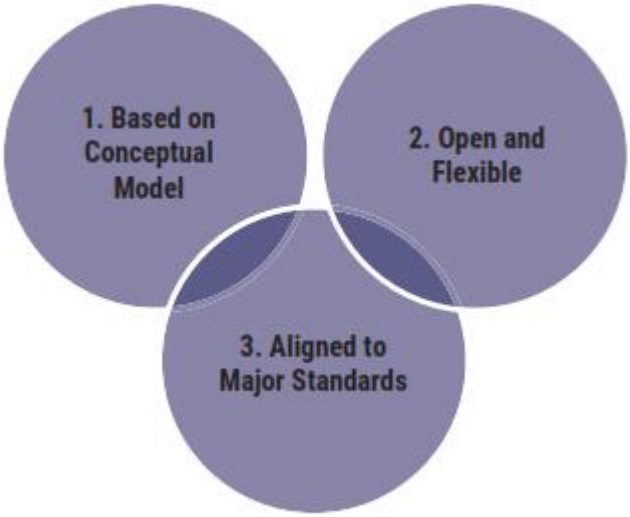
Gambar 2. 15 Enam Prinsip Tata Kelola

Tiga Prinsip Kerangka Kerja Tata Kelola COBIT 2019 antara lain:

1. Kerangka tata kelola harus didasarkan pada model konseptual, yang mengidentifikasi komponen-komponen utama dan hubungan antar

komponen, untuk memaksimalkan konsistensi dan memungkinkan otomatisasi.

2. Kerangka tata kelola harus terbuka dan fleksibel. Hal ini harus memungkinkan penambahan konten baru dan kemampuan untuk mengatasi masalah baru dengan cara yang paling fleksibel, dengan tetap menjaga integritas dan konsistensi.
3. Kerangka tata kelola harus selaras dengan standar, kerangka kerja, dan peraturan terkait yang relevan.



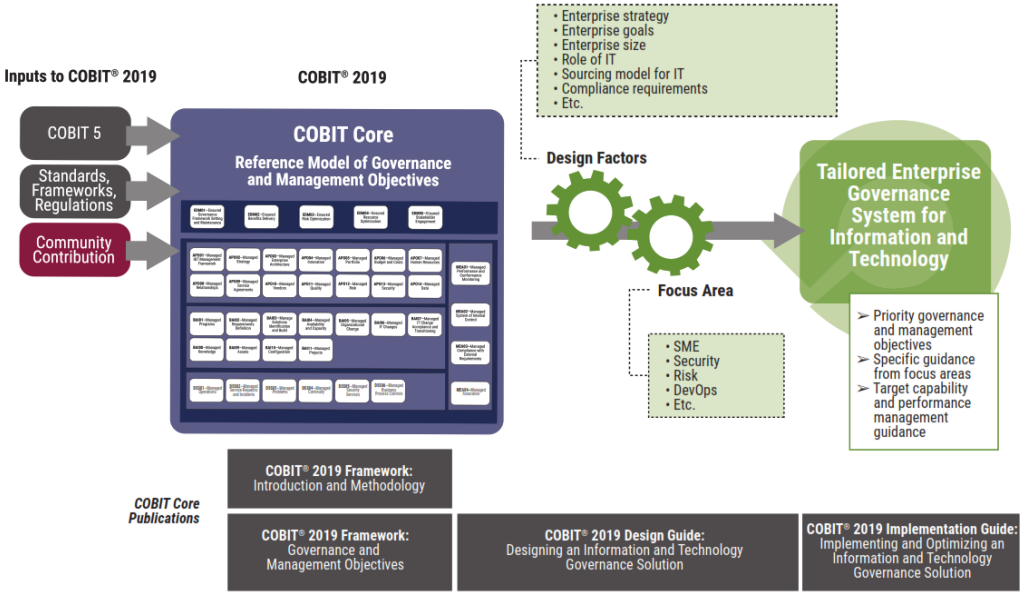
Gambar 2. 16 Tiga Prinsip Kerangka Kerja Tata Kelola COBIT 2019

Pada COBIT 2019 ini memiliki pengembangan diarea-area berikut:

1. fleksibilitas dan keterbukaan, definisi dan penggunaan faktor desain memungkinkan COBIT disesuaikan agar lebih selaras dengan konteks khusus pengguna. Arsitektur terbuka COBIT memungkinkan penambahan area fokus baru atau memodifikasi area fokus yang sudah ada, tanpa implikasi langsung terhadap struktur dan konten model inti COBIT.
2. Mata uang dan relevansi, model COBIT mendukung referensi dan penyelarasan konsep yang berasal dari sumber lain (misalnya, standar TI terbaru dan peraturan kepatuhan).
3. Penerapan preskriptif, model seperti COBIT dapat bersifat deskriptif dan preskriptif. Model konseptual COBIT dibangun dan disajikan sedemikian

rupa sehingga instantiasinya (yaitu penerapan komponen tata kelola COBIT yang disesuaikan) dianggap sebagai resep untuk sistem tata kelola TI yang disesuaikan.

4. Manajemen kinerja TI, struktur model manajemen kinerja COBIT diintegrasikan ke dalam model konseptual. Konsep kematangan dan kemampuan diperkenalkan untuk penyelarasan yang lebih baik dengan CMMI.



Gambar 2. 17 Gambaran Umum COBIT 2019

Konsep dasar yang berkaitan dengan tujuan tata kelola dan pengelolaan adalah:

- Tujuan tata kelola atau pengelolaan selalu berkaitan dengan satu proses (dengan nama yang identik atau mirip) dan serangkaian komponen terkait lainnya untuk membantu mencapai tujuan.
- Tujuan tata kelola berkaitan dengan proses tata kelola, sedangkan tujuan pengelolaan berkaitan dengan proses pengelolaan. Direksi dan manajemen eksekutif biasanya bertanggung jawab atas proses tata kelola, sedangkan proses manajemen merupakan *domain* manajemen senior dan menengah.
- Tujuan tata kelola dan manajemen dalam COBIT dikelompokkan menjadi lima *domain*. *Domain* memiliki nama dengan kata kerja yang

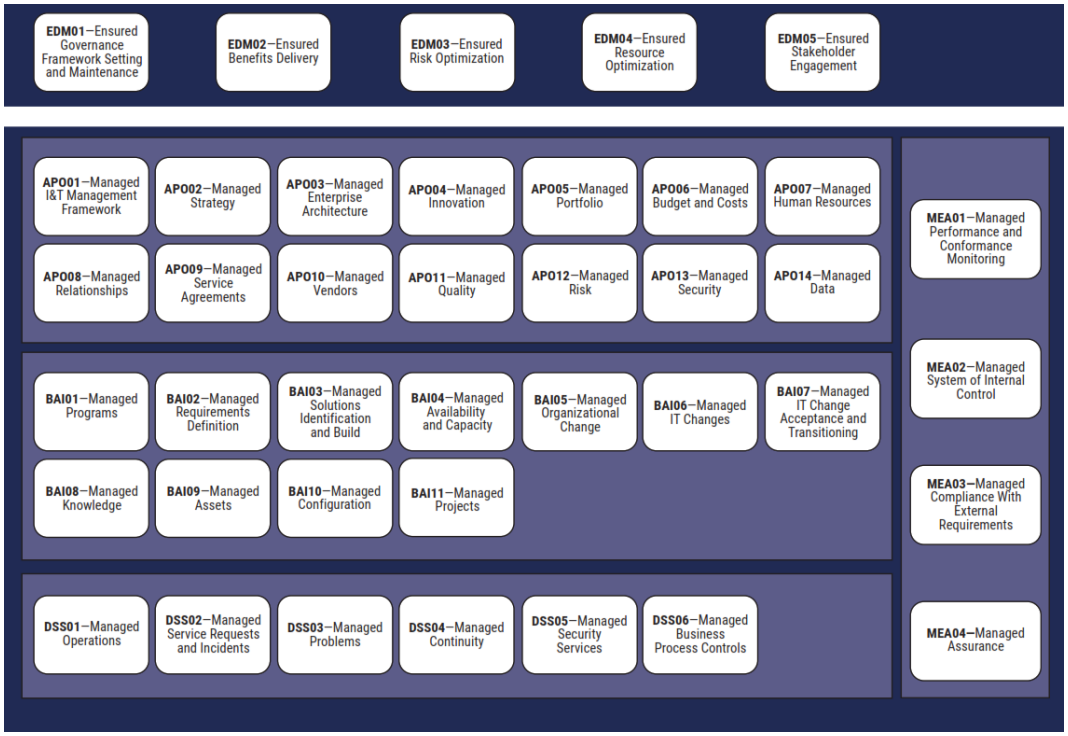
mengungkapkan maksud utama dan bidang kegiatan dari tujuan yang terkandung di dalamnya:

Proses tata kelola diatur pada *domain Evaluate, Direct and Monitor (EDM).* Dalam *domain* ini membahas direksi mengevaluasi pilihan-pilihan strategis, mengarahkan manajemen pada pilihan-pilihan strategis yang dipilih dan memantau pencapaian strategi.

Sedangkan proses manajemen diatur dalam empat *domain*:

- *Align, Plan, and Organize (APO)* membahas keseluruhan organisasi, strategi dan kegiatan pendukung TI.
- *Build, Acquire, and Implement (BAI)* membahas definisi, akuisisi dan implementasi solusi TI dan integrasinya dalam proses bisnis.
- *Deliver, Service, and Support (DSS)* membahas penyampaian operasional dan dukungan layanan TI, termasuk keamanan.
- *Monitor, Evaluate, and Assess (MEA)* membahas pemantauan kinerja dan kesesuaian TI dengan target kinerja internal, tujuan pengendalian internal, dan persyaratan eksternal.

Untuk lebih lengkapnya, *objectives* dari COBIT 2019 digambarkan pada gambar COBIT *Core Model* di bawah.



Gambar 2. 18 COBIT *Core Model*

Komponen dari sistem tata kelola :

- Untuk memenuhi tujuan tata kelola dan manajemen, setiap perusahaan perlu membangun, menyesuaikan dan mempertahankan sistem tata kelola yang dibangun dari sejumlah komponen.
- Komponen adalah faktor-faktor yang secara individu dan kolektif, berkontribusi terhadap berjalannya sistem tata kelola perusahaan atas TI dengan baik.
- Komponen berinteraksi satu sama lain, menghasilkan sistem tata kelola TI yang *holistic.*
- Komponen dapat terdiri dari berbagai jenis, yang paling familiar adalah proses. Namun, komponen sistem tata kelola juga mencakup struktur organisasi; kebijakan dan prosedur; item informasi; budaya dan perilaku; keterampilan dan kompetensi; dan layanan, infrastruktur dan aplikasi

Processes, menggambarkan serangkaian praktik dan aktivitas terorganisir untuk mencapai tujuan tertentu dan menghasilkan serangkaian keluaran yang mendukung pencapaian tujuan terkait TI secara keseluruhan.

Organizational structures, adalah entitas pengambil keputusan utama dalam suatu perusahaan.

Principles, policies and frameworks, menerjemahkan perilaku yang diinginkan menjadi panduan praktis untuk manajemen sehari-hari.

Information, tersebar luas di seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. COBIT berfokus pada informasi yang diperlukan untuk berfungsinya sistem tata kelola perusahaan secara efektif.

Culture, ethics and behavior, individu dan perusahaan sering diremehkan sebagai faktor keberhasilan kegiatan tata kelola dan manajemen.

People, skills and competencies, Diperlukan untuk pengambilan keputusan yang baik, pelaksanaan tindakan perbaikan dan keberhasilan penyelesaian semua kegiatan.

Services, infrastructure and applications, mencakup infrastruktur, teknologi, dan aplikasi yang menyediakan sistem tata kelola bagi pemrosesan TI bagi perusahaan.

Gambar 2. 19 Komponen COBIT dari sistem tata kelola

Semua jenis komponen dapat bersifat generik atau dapat berupa varian. Komponen generik dijelaskan dalam model inti COBIT dan pada prinsipnya berlaku untuk situasi apa pun. Namun, hal tersebut bersifat umum dan umumnya memerlukan penyesuaian sebelum diterapkan secara praktis. Varian didasarkan pada komponen umum namun disesuaikan untuk tujuan atau konteks tertentu dalam area fokus (misalnya, untuk keamanan informasi, DevOps, peraturan tertentu).

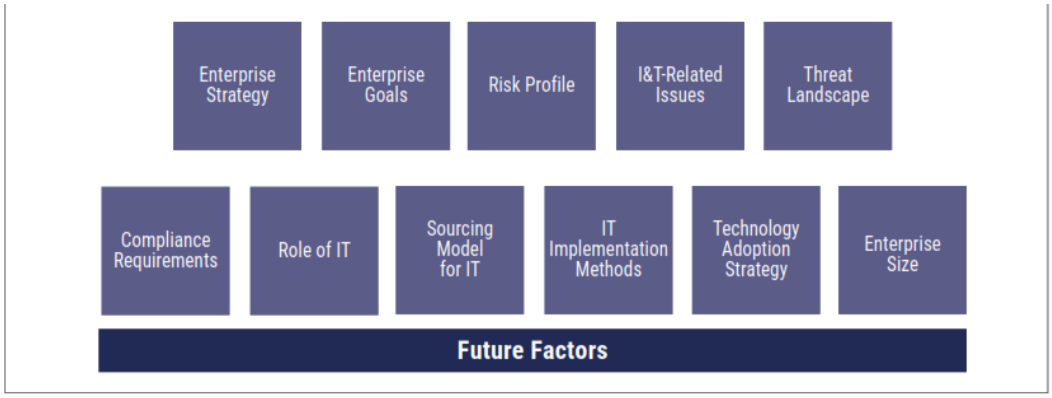
Di dalam COBIT juga dikenal istilah yang disebut *focus area* yaitu menggambarkan topik, *domain*, atau isu tata kelola tertentu yang dapat diatasi melalui kumpulan tujuan tata kelola dan pengelolaan serta komponennya. Contoh *focus area* meliputi: usaha kecil dan menengah, keamanan siber, transformasi digital, *cloud computing*, privasi, dan DevOps. *Focus area* mungkin berisi kombinasi komponen dan varian tata kelola yang umum. Jumlah *focus area* sebenarnya tidak terbatas. Hal inilah yang membuat COBIT bersifat terbuka. *Focus area* baru dapat ditambahkan sesuai kebutuhan atau seiring dengan kontribusi para ahli dan praktisi pada model COBIT.

Design factor adalah faktor yang dapat mempengaruhi desain sistem tata kelola suatu perusahaan dan menentukan keberhasilan dalam penggunaan TI.

Ada tiga dampak yang ditimbulkan faktor desain terhadap sistem tata kelola :

- Prioritas tujuan manajemen dan target level kapabilitas.
- Variasi komponen.
- Area fokus tertentu.

Design factor merupakan kombinasi dari strategi organisasi, Tujuan organisasi, profil risiko, isu terkait TI, *lasekap* ancaman, persyaratan kepatuhan, peran TI, model pengadaan TI, metode implementasi TI, strategi adopsi teknologi dan ukuran organisasi.



Gambar 2. 20 *Design Factor* COBIT

Enterprise strategy: organisasi memiliki beragam strategi, organisasi umumnya memiliki strategi utama dan setidaknya satu strategi sekunder. *Enterprise strategy* dijelaskan pada gambar dibawah ini.

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues).[10]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients.[11]
Cost Leadership	The enterprise has a focus on short-term cost minimization.[12]
Client Service/Stability	The enterprise has a focus on providing stable and client-oriented service.[13]

Gambar 2. 21 *Enterprise Strategy Design Factor*

Enterprise goal: strategi organisasi diwujudkan melalui pencapaian dari kombinasi tujuan organisasi. Dalam COBIT tujuan organisasi distrukturkan sesuai dengan *Balanced Scorecard (BSC)* dijelaskan pada gambar dibawah ini.

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Gambar 2. 22 *Enterprise Goal Design Factor*

Risk profile mengidentifikasi risiko terkait TI yang terdapat pada organisasi dan mengindikasikan area risiko yang melampau *risk appetite yang dijelaskan pada gambar di bawah ini.*

Reference	Risk Category
1	IT investment decision making, portfolio definition and maintenance
2	Program and projects lifecycle management
3	IT cost and oversight
4	IT expertise, skills and behavior
5	Enterprise/IT architecture
6	IT operational infrastructure incidents
7	Unauthorized actions
8	Software adoption/usage problems
9	Hardware incidents
10	Software failures
11	Logical attacks (hacking, malware, etc.)
12	Third party/supplier incidents
13	Noncompliance
14	Geopolitical issues
15	Industrial action
16	Acts of nature
17	Technology-based innovation
18	Environmental
19	Data and information management

Gambar 2. 23 *Risk Profile Design Factor*

IT-related issues permasalahan yang dihadapi organisasi saat ini, apa saja risiko terkait TI yang telah terwujud sebagai hasil kegiatan *risk assessment* yang dijelaskan pada gambar di bawah ini.

Reference	Description
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT-related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives, or other forms of wasted resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems
O	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department[16]
S	Ignorance of and/or noncompliance with privacy regulations
T	Inability to exploit new technologies or innovate using I&T

Gambar 2. 24 *IT Related Issues Design Factor*

Threat Landscape Klasifikasi ancaman dalam organisasi dijelaskan pada gambar di bawah ini.

Threat Landscape	Explanation
Normal	The enterprise is operating under what are considered normal threat levels.
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

Gambar 2. 25 *Threat Landscape Design Factor*

Compliance Requirement persyaratan kepatuhan yang mengikat organisasi dijelaskan pada gambar di bawah ini.

Regulatory Environment	Explanation
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.

Gambar 2. 26 *Compliance Requirement Design Factor*

Role Of IT atau Peran TI dalam organisasi dijelaskan pada gambar di bawah ini.

Role of IT[17]	Explanation
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

Gambar 2. 27 *Role of IT Design Factor*

Sourcing Model For IT, model penyediaan TI dijelaskan pada gambar di bawah ini.

Sourcing Model	Explanation
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for its own IT staff and services.
Hybrid	A mixed model is applied, combining the other three models in varying degrees.

Gambar 2. 28 *Sourcing Model for IT Design Factor*

IT implementation methods, Implementasi penggunaan TI dijelaskan pada gambar di bawah ini.

IT Implementation Method	Explanation
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

Gambar 2. 29 *IT implementation methods Design Factor*

IT Adoption Strategy, model Adopsi TI organisasi dijelaskan pada gambar di bawah ini.

Technology Adoption Strategy	Explanation
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with adoption of new technologies.

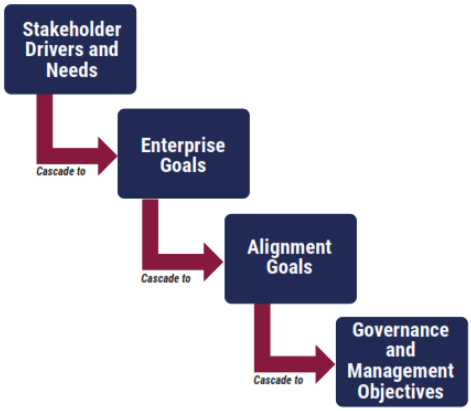
Gambar 2. 30 *IT Adoption Strategy Design Factor*

Enterprise size, ukuran dari organisasi dijelaskan pada gambar di bawah ini.

Enterprise Size	Explanation
Large enterprise (Default)	Enterprise with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

Gambar 2. 31 *Enterprise size Design Factor*

Goal Cascade, Kebutuhan *stakeholder* harus diubah menjadi strategi perusahaan yang dapat ditindaklanjuti. Rangkaian tujuan yang mendukung tujuan perusahaan merupakan salah satu faktor desain utama sistem tata kelola. Hal ini mendukung penentuan prioritas tujuan pengelolaan berdasarkan prioritas tujuan perusahaan.



Gambar 2. 32 COBIT *Goal Cascade*

Rangkaian tujuan lebih lanjut mendukung penerjemahan tujuan perusahaan menjadi prioritas untuk penyelarasan tujuan. Rangkaian tujuan telah diperbaharui secara menyeluruh di COBIT 2019:

- Tujuan perusahaan telah dikonsolidasikan, dikurangi, diperbaharui dan diklarifikasi.
- Penyelarasan tujuan menekankan keselarasan semua upaya TI dengan tujuan bisnis. Istilah yang diperbaharui ini juga berupaya menghindari kesalahpahaman yang sering terjadi bahwa tujuan ini murni menunjukkan tujuan internal departemen TI dalam suatu perusahaan. Seperti tujuan perusahaan, tujuan penyelarasan telah dikonsolidasikan, dikurangi, diperbaharui dan diklarifikasi jika diperlukan.

Berikut adalah *cascading* dari COBIT 2019:

		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

Gambar 2. 33 *Mapping Enterprise Goal to Alignment Goals*

Selanjutnya setelah *Alignment Goals* didapatkan dipetakan.

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

Gambar 2. 34 *Mapping Governance and Management Objective to Alignment Goals*

Performance Management, Manajemen kinerja merupakan bagian penting dari tata kelola dan sistem manajemen. “Manajemen kinerja” mewakili istilah umum untuk semua aktivitas dan metode. Hal ini mengungkapkan seberapa baik tata kelola dan sistem manajemen serta seluruh komponen suatu perusahaan bekerja, dan bagaimana hal tersebut dapat ditingkatkan untuk mencapai tingkat yang diperlukan. Ini mencakup konsep dan metode seperti tingkat kemampuan dan tingkat kematangan. COBIT menggunakan istilah COBIT *Performance*

Management (CPM) untuk menggambarkan aktivitas ini, dan konsep ini merupakan bagian integral dari kerangka COBIT.

Prinsip COBIT *Performance Management* :

1. Prinsip Manajemen Kinerja COBIT CPM harus mudah dipahami dan digunakan.
2. Kinerja seluruh jenis komponen sistem tata kelola; kinerja proses serta kinerja jenis komponen lainnya (misalnya struktur organisasi atau informasi) harus dapat dikelola jika pengguna menginginkannya.
3. CPM harus memberikan hasil yang dapat diandalkan, dapat diulang, dan relevan.
4. Fleksibel dan bisa mendukung kebutuhan beragam organisasi.
5. Mendukung beragam tipe *assessment*, mulai dari *self assessment*, penilaian formal dan audit.

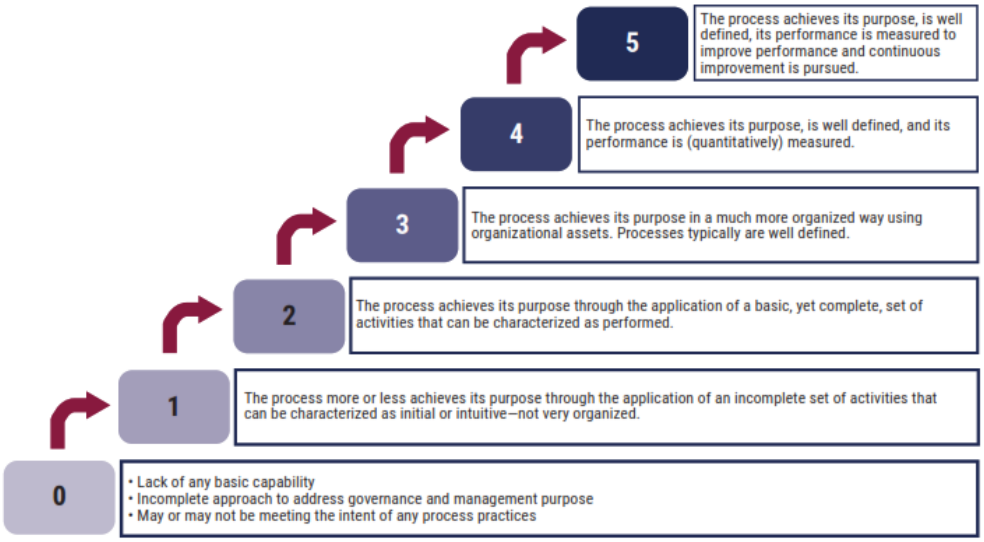
COBIT 2019 *Performance management* menggunakan pengukuran *capability level* di tingkat aktivitas proses, komponen lain dan *maturity level* ditingkat *area focus*.

Jenis komponen tata kelola dan manajemen lainnya (misalnya, struktur organisasi, informasi) mungkin juga memiliki tingkat kemampuan yang ditentukan dalam panduan di masa mendatang.

Tingkat kematangan dikaitkan dengan area fokus (yaitu kumpulan tujuan tata kelola dan pengelolaan serta komponen yang mendasarinya) dan akan tercapai jika semua tingkat kemampuan yang diperlukan tercapai.

Process Capability Levels

COBIT 2019 mendukung skema kemampuan proses berbasis CMMI. Proses dalam setiap tujuan tata kelola dan pengelolaan dapat beroperasi pada berbagai tingkat kemampuan, mulai dari 0 hingga 5. Tingkat kemampuan adalah ukuran seberapa baik suatu proses diterapkan dan dijalankan.



Gambar 2. 35 *Capability Level* COBIT *2019*

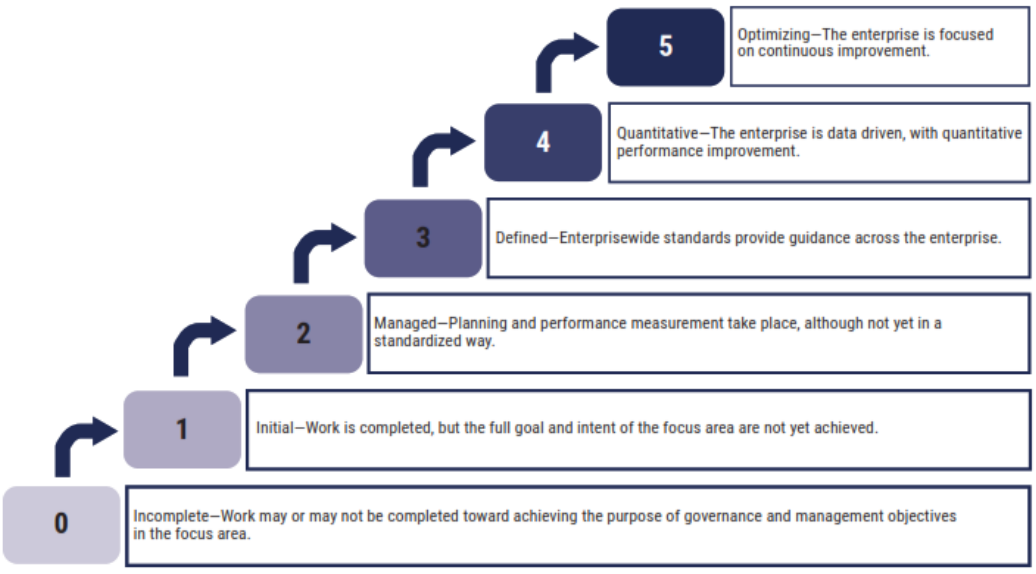
Tingkat kemampuan dapat dicapai pada tingkat yang berbeda-beda, yang dapat dinyatakan dengan serangkaian peringkat. Kisaran peringkat yang tersedia bergantung pada konteks di mana penilaian kinerja dilakukan:

- Beberapa metode formal yang mengarah ke sertifikasi independen menggunakan serangkaian peringkat biner lulus atau gagal.
- Metode yang kurang formal (sering digunakan dalam konteks peningkatan kinerja) bekerja lebih baik dengan rentang penilaian yang lebih luas, seperti rangkaian berikut:
    1. *Fully*, tingkat kemampuan tercapai lebih dari 85 persen. (Hal ini tetap merupakan keputusan penilaian, namun dapat dibuktikan dengan pemeriksaan atau penilaian terhadap komponen-komponen pendukung, seperti aktivitas proses, tujuan proses, atau praktik baik struktur organisasi).
    2. *Largely*, tingkat kemampuan dicapai antara 50 persen dan 85 persen.
    3. *Partially*, tingkat kemampuan dicapai antara 15 persen hingga 50 persen.
    4. *Not*, tingkat kemampuan yang dicapai kurang dari 15 persen.

Capability Level proses didapatkan dengan menilai rata-rata setiap aktivitas dan dibagi dengan jumlah responden yang menghasilkan nilai capability pada suatu domain proses. Adapun perhitungan penilaian tersebut sebagai berikut:

- $\text{Capability Level} = \frac{\sum Rata{-}rata\ skor\ Aktivitas}{\text{Total Responden}}$ 2.1

Tingkat kematangan area fokus, terkadang diperlukan tingkatan yang lebih tinggi untuk menyatakan kinerja tanpa rincian yang dapat diterapkan pada peringkat kemampuan proses individual. Tingkat kedewasaan dapat digunakan untuk tujuan itu. COBIT 2019 mendefinisikan tingkat kematangan sebagai ukuran kinerja pada tingkat area fokus, tingkat kematangan dikaitkan dengan area fokus (yaitu, kumpulan tujuan tata kelola dan pengelolaan serta komponen yang mendasarinya) dan tingkat kematangan tertentu dicapai jika semua proses yang terdapat dalam area fokus mencapai tingkat kemampuan tertentu.



Gambar 2. 36. *Maturity Level For Focus Area*

Pada *focus area* tertentu (*devops*, regulasi tertentu, *cybersecurity*, SME) penentuan performa yang sifatnya lebih *high level* lebih diperlukan dibandingkan pengukuran kinerja per-proses.

• *Focus area*: sekumpulan *governance and management objective, generic* komponen dan variannya .

• *Level maturity:* tertentu tercapai jika seluruh *governance dan management objective* dan komponen dalam *area focus* mencapai *level capability* tertentu

• COBIT belum mendefinisikan *standard schema capability* untuk pengukuran komponen selain proses. Baru ada panduan pencapaian yang bersifat *good practices.*

2.6.1 RACI Chart

RACI *Chart* merupakan bagan pemetaan terhadap tugas dan tanggung jawab kepada pihak-pihak yang terkait. RACI merupakan kepanjangan dari *Responsbile, Accountable, Consulted, and Informed.* RACI *Chart* akan digunakan pada setiap *objective* yang diteliti sehingga RACI pada setiap *objective* akan berubah. Secara lebih jelas RACI *Chart* dijabarkan sebagai berikut:

- *Responsible*, pihak pelaksana kegiatan.
- *Accountable*, pihak yang memiliki tanggung jawab akan kegiatan.
- *Consulted*, pihak yang memberikan saran dan arahan untuk kegiatan.
- *Informed*, pihak yang diberikan hasil dari kegiatan [26].

Pihak-pihak yang dimaksud akan dijelaskan pada tabel peranan/*role* berikut ini:

Tabel 2. 3 RACI *Chart*

Role	Deskripsi
Board	Kelompok eksekutif paling senior dan/atau direktur non-eksekutif yang bertanggung jawab atas tata kelola dan pengendalian sumber daya perusahaan secara keseluruhan.
Executive Committee	Sekelompok eksekutif senior yang ditunjuk oleh Direksi untuk memastikan bahwa Direksi dilibatkan dan selalu mendapat informasi tentang keputusan-keputusan besar.
Chief Executive Officer	Pejabat dengan pangkat tertinggi yang bertanggung jawab atas keseluruhan manajemen perusahaan.
Chief Financial Officer	Sebagian besar pejabat senior bertanggung jawab atas semua aspek pengelolaan keuangan, termasuk risiko dan pengendalian keuangan serta pembukuan yang andal dan akurat.

Tabel 2. 3 RACI Chart Lanj*utan*

Role	Deskripsi
Chief Operating Officer	Pejabat paling senior yang bertanggung jawab atas operasional perusahaan.
Chief Risk Officer	Sebagian besar pejabat senior bertanggung jawab atas semua aspek manajemen risiko di seluruh perusahaan.
Chief Information Officer	Sebagian besar pejabat senior bertanggung jawab untuk menyelaraskan strategi TI dan bisnis serta bertanggung jawab atas perencanaan, sumber daya, dan pengelolaan penyampaian layanan dan solusi TI.
Chief Technology Officer	Sebagian besar pejabat senior bertugas menangani aspek teknis TI, termasuk mengelola dan memantau keputusan terkait layanan, solusi, dan infrastruktur TI.
Chief Digital Officer	Sebagian besar pejabat senior bertugas mempraktikkan ambisi digital perusahaan atau unit bisnis.
IT Governance Board	Kelompok *stakeholder* dan pakar yang bertanggung jawab untuk memandu hal-hal dan keputusan terkait TI, termasuk mengelola investasi yang mendukung TI, memberikan nilai, dan memantau risiko.
Architecture Board	Sekelompok *stakeholder* dan pakar yang bertanggung jawab untuk memandu hal-hal dan keputusan terkait arsitektur perusahaan dan untuk menetapkan kebijakan dan standar arsitektur.
Enterprise Risk Committee	Sekelompok eksekutif yang bertanggung jawab atas kolaborasi dan konsensus tingkat perusahaan yang diperlukan untuk mendukung aktivitas dan keputusan manajemen risiko perusahaan (ERM).
Chief Information Security Officer	Sebagian besar pejabat senior bertanggung jawab atas semua aspek manajemen keamanan di seluruh perusahaan.

Tabel 2. 3 RACI Chart Lanj*utan*

Role	Deskripsi
Business Process Owner	Individu yang bertanggung jawab untuk menjalankan proses dan/atau mewujudkan tujuan proses, mendorong perbaikan proses dan menyetujui perubahan proses.
Portfolio Manager	Individu yang bertanggung jawab untuk memandu manajemen portofolio, memastikan pemilihan program dan proyek yang tepat, mengelola dan memantau program dan proyek untuk mendapatkan nilai optimal, dan mewujudkan tujuan strategis jangka panjang secara efektif dan efisien.
Steering (Programs/ Projects) Committee	Kelompok *stakeholder* dan pakar yang bertanggung jawab untuk memandu program dan proyek, termasuk mengelola dan memantau rencana, mengalokasikan sumber daya, memberikan manfaat dan nilai, serta mengelola risiko program dan proyek.
Program Manager	Individu yang bertanggung jawab untuk memandu program tertentu, termasuk mengartikulasikan dan menindaklanjuti tujuan dan sasaran program serta mengelola risiko dan dampak terhadap bisnis.
Project Manager	Individu yang bertanggung jawab untuk memandu proyek tertentu, termasuk mengoordinasikan dan mendelegasikan waktu, anggaran, sumber daya, dan tugas di seluruh tim proyek.
Project Management Office	Fungsi yang bertanggung jawab untuk mendukung manajer program dan proyek dan untuk mengumpulkan, menilai dan melaporkan informasi tentang pelaksanaan program dan proyek konstituen.
Data Management Function	Fungsi yang bertanggung jawab untuk mendukung aset data perusahaan di seluruh siklus hidup data dan mengelola strategi data, infrastruktur, dan repositori.

Tabel 2. 3 RACI Chart Lanj*utan*

Role	Deskripsi
Head Human Resources	Sebagian besar pejabat senior bertanggung jawab atas perencanaan dan kebijakan mengenai sumber daya manusia di perusahaan.
Relationship Manager	Individu senior yang bertanggung jawab untuk mengawasi dan mengelola antarmuka internal dan komunikasi antara fungsi bisnis dan TI.
Head Architect	Individu senior yang bertanggung jawab atas proses arsitektur perusahaan.
Head Development	Individu senior yang bertanggung jawab atas proses pengembangan solusi terkait TI.
Head IT Operations	Individu senior yang bertanggung jawab atas lingkungan dan infrastruktur operasional TI.
Head IT Administration	Individu senior yang bertanggung jawab atas catatan terkait TI dan bertanggung jawab untuk mendukung urusan administratif terkait TI.
Service Manager	Individu yang mengelola pengembangan, penerapan, evaluasi, dan pemeliharaan berkelanjutan atas produk dan layanan baru dan yang sudah ada untuk pelanggan (pengguna) atau kelompok pelanggan (pengguna) tertentu.
Information Security Manager	Individu yang mengelola, merancang, mengawasi dan/atau menilai keamanan informasi suatu perusahaan.
Business Continuity Manager	Individu yang mengelola, merancang, mengawasi dan/atau menilai kemampuan kelangsungan bisnis suatu perusahaan, untuk memastikan bahwa fungsi-fungsi penting perusahaan terus beroperasi setelah peristiwa-peristiwa yang mengganggu.

Tabel 2. 3 RACI Chart Lanj*utan*

Role	Deskripsi
Privacy Officer	Individu yang bertanggung jawab untuk memantau risiko dan dampak bisnis dari undang-undang privasi dan untuk memandu dan mengoordinasikan penerapan kebijakan dan aktivitas yang memastikan kepatuhan terhadap arahan privasi.
Legal Counsel	Fungsi yang bertanggung jawab untuk memberikan panduan mengenai masalah hukum dan peraturan.
Compliance	Fungsi yang bertanggung jawab atas semua pedoman kepatuhan eksternal.
Audit	Fungsi yang bertanggung jawab atas penyediaan audit internal.

Berdasarkan peran/*role* yang telah diberikan COBIT diatas, selanjutnya akan dipetakan terhadap struktur organisasi yang ada di Polinela sebagai dasar acuan pembuatan RACI *Chart* pada tahap *assessment*.

2.6.2 *Objective* EDM03 dan APO12

COBIT 2019 memiliki dua *objective* yang berkaitan dengan risiko yaitu EDM03, *Ensured Risk Optimization* dan APO12, *managed risk* yang akan dijelaskan lebih lanjut dibawah ini [27]:

EDM03, *Ensured Risk Optimization* memiliki beberapa komponen proses terkait dengan tata kelola antara lain:

- EDM03.01 *evaluate risk management*, secara terus-menerus memeriksa dan mengevaluasi dampak risiko terhadap penggunaan TI saat ini dan masa depan di perusahaan. Pertimbangkan apakah selera risiko perusahaan sudah sesuai dan pastikan bahwa risiko terhadap nilai perusahaan terkait penggunaan TI diidentifikasi dan dikelola.

  *Metric*s pengukurannya berupa :

  - Tingkat dampak perusahaan yang tidak terduga.

- Persentase risiko TI yang melebihi toleransi risiko perusahaan.
- Tingkat *update* evaluasi dari faktor risiko.

Adapun aktivitas yang dilakukan pada komponen ini antara lain:

- Memahami organisasi dan konteksnya terkait dengan risiko TI.
- Tentukan selera risiko organisasi, yaitu tingkat risiko terkait TI yang bersedia diambil oleh perusahaan dalam mencapai tujuan perusahaan.
- Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima untuk sementara waktu dari selera risiko.
- Menentukan sejauh mana penyelarasan strategi risiko TI dengan strategi risiko perusahaan dan memastikan selera risiko berada di bawah kapasitas risiko organisasi.
- Secara proaktif mengevaluasi faktor risiko TI sebelum mengambil keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko merupakan bagian dari proses pengambilan keputusan strategis perusahaan.
- Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait TI dan toleransi pimpinan terhadap kerugian tersebut.
- Menarik dan mempertahankan keterampilan dan personel yang diperlukan untuk manajemen risiko TI

- EDM03.02 *direct risk management*, mengarahkan penetapan praktik manajemen risiko untuk memberikan jaminan yang masuk akal bahwa praktik manajemen risiko TI sudah tepat dan bahwa risiko TI yang sebenarnya tidak melebihi selera risiko direksi.

  Metrics pengukurannya berupa:

  - Tingkat keselarasan antara risiko TI dan risiko perusahaan.
  - Persentase proyek perusahaan yang mempertimbangkan risiko TI.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:

  - Mengarahkan penerjemahan dan integrasi strategi risiko TI ke dalam praktik manajemen risiko dan aktivitas operasional.

- Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan).
- Penerapan langsung mekanisme yang tepat untuk merespons dengan cepat terhadap perubahan risiko dan melaporkan segera ke tingkat manajemen yang tepat, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).
- Mengarahkan bahwa risiko, peluang, permasalahan dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan dieskalasi ke pengambil keputusan terkait.
- Mengidentifikasi tujuan dan metrik utama tata kelola risiko dan proses manajemen yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.

- EDM03.03 *monitor risk management*, pantau tujuan dan metrik utama dari proses manajemen risiko. Tentukan bagaimana penyimpangan atau masalah akan diidentifikasi, dilacak dan dilaporkan untuk perbaikan.

  Metrics pengukurannya berupa:
  - Jumlah potensi area risiko TI yang di identifikasi dan dikelola.
  - Persentase risiko kritis yang telah dimitigasi secara efektif.
  - Persentase rencana tindakan risiko TI dilaksanakan tepat waktu.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Laporkan masalah manajemen risiko apa pun kepada direksi atau komite eksekutif.
  - Memantau sejauh mana profil risiko dikelola sesuai dengan selera risiko dan ambang batas toleransi perusahaan.
  - Memantau sasaran dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan memulai tindakan perbaikan untuk mengatasi penyebab mendasar.

- Memungkinkan peninjauan oleh *stakeholder* utama mengenai kemajuan perusahaan dalam mencapai tujuan yang telah diidentifikasi

APO12, *managed risk* secara terus-menerus mengidentifikasi, menilai dan mengurangi risiko terkait TI dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan dengan tujuan mengintegrasikan manajemen risiko perusahaan terkait TI dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait TI YANG memiliki beberapa komponen proses terkait dengan tata kelola antara lain:

- APO12.01 *collect data*, identifikasi dan kumpulkan data yang relevan untuk memungkinkan identifikasi, analisis, dan pelaporan risiko terkait TI yang efektif.

  Metrics pengukurannya berupa:
  - Jumlah peristiwa kerugian dengan karakteristik utama yang ditangkap dalam repositori.
  - Persentase audit, peristiwa, dan tren yang terekam dalam repositori.
  - Persentase sistem kritis dengan masalah yang diketahui.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Menetapkan dan memelihara metode pengumpulan, klasifikasi, dan analisis data terkait risiko TI.
  - Catat data terkait risiko TI yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.
  - Mengadopsi atau menentukan taksonomi risiko untuk definisi yang konsisten mengenai skenario risiko serta kategori dampak dan kemungkinan.
  - Catat data kejadian risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditentukan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.
  - Mensurvei dan menganalisis data historis risiko TI dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan-

rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.

- Untuk rangkaian acara serupa, atur data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi faktor umum di berbagai peristiwa.
- Tentukan kondisi spesifik yang ada atau tidak ada ketika peristiwa risiko terjadi dan bagaimana kondisi tersebut mempengaruhi frekuensi peristiwa dan besarnya kerugian.
- Melakukan analisis peristiwa dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.

- APO12.02 *analyze risk,* kembangkan pandangan yang kuat mengenai risiko TI aktual, untuk mendukung keputusan risiko.

  Metric pengukurannya berupa:
  - Jumlah skenario risiko TI yang teridentifikasi.
  - Waktu sejak pembaruan terakhir skenario risiko TI.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Tentukan ruang lingkup upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kepentingan bisnis aset.
  - Membangun dan memperbarui skenario risiko TI secara rutin; eksposur kerugian terkait TI; dan skenario mengenai risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang terjadi secara berjenjang dan/atau secara kebetulan. Kembangkan harapan untuk aktivitas pengendalian spesifik dan kemampuan untuk mendeteksi.
  - Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.

- Bandingkan risiko saat ini (paparan kerugian terkait TI) dengan selera risiko dan toleransi risiko yang dapat diterima. Identifikasi risiko yang tidak dapat diterima atau meningkat.
- Mengusulkan respon risiko untuk risiko yang melebihi tingkat selera risiko dan toleransi.
- Tentukan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respon risiko yang dipilih. Identifikasi persyaratan dan harapan untuk pengendalian utama yang tepat untuk respon mitigasi risiko.
- Validasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis tersebut selaras dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui adanya bias.
- Menganalisis biaya/manfaat dari opsi respon risiko potensial seperti menghindari, mengurangi/mitigasi, mentransfer/membagi, dan menerima dan mengeksploitasi/merebut. Konfirmasikan respon risiko yang optimal.

- APO12.03 *maintain a risk profile*, pertahankan inventarisasi risiko dan atribut risiko yang diketahui, termasuk frekuensi yang diharapkan, potensi dampak, dan respon. Dokumentasikan sumber daya terkait, kemampuan, dan aktivitas pengendalian terkini yang terkait dengan item risiko.

  Metric pengukurannya berupa:
  - Kelengkapan atribut dan nilai pada profil risiko
  - Persentase proses bisnis utama yang dimasukkan dalam profil risiko

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Inventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, *vendor*, pemasok, dan agen *outsourcing*.
  - Menentukan dan menyepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan

pengoperasian proses bisnis. Analisis ketergantungan dan identifikasi tautan lemah.

- Gabungkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.
- Catat semua informasi profil risiko secara berkala dan konsolidasikan ke dalam profil risiko gabungan.
- Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko TI perusahaan.
- Berdasarkan seluruh data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini dan tren risiko secara cepat.
- Menangkap informasi mengenai peristiwa risiko TI yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan.

- APO12.04 *articulate risk*, komunikasikan informasi mengenai keadaan saat ini mengenai paparan dan peluang terkait TI secara tepat waktu kepada semua *stakeholder* yang diperlukan untuk mendapatkan respons yang tepat. *Metric* pengukurannya berupa:
  - Tingkat kepuasan *stakeholder* terhadap pelaporan risiko yang diberikan.
  - Kelengkapan pelaporan profil risiko (termasuk informasi yang sesuai dengan kebutuhan *stakeholder*).
  - Penggunaan pelaporan risiko dalam pengambilan keputusan manajemen.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Laporkan hasil analisis risiko kepada seluruh *stakeholder* yang terkena dampak dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan kisaran kerugian atau keuntungan serta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan keuntungan dan risiko.
  - Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan paling mungkin terjadi, paparan kerugian

terkait TI dan TI dan reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.

- Laporkan profil risiko terkini kepada seluruh *stakeholder*. Meliputi informasi mengenai efektivitas proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status remediasi dan dampaknya terhadap profil risiko.
- Secara berkala, untuk wilayah dengan risiko relatif dan kapasitas risiko yang setara, identifikasi peluang terkait TI yang memungkinkan penerimaan risiko lebih besar serta peningkatan pertumbuhan dan keuntungan.
- Meninjau hasil penilaian pihak ketiga yang objektif dan audit internal serta tinjauan jaminan kualitas. Sertakan mereka dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait TI untuk menentukan perlunya analisis risiko tambahan.

- APO12.05 *define a risk management action portofolio*, kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima sebagai portofolio. *Metrics* pengukurannya berupa:
  - Jumlah insiden signifikan yang tidak teridentifikasi dan dimasukkan dalam portofolio manajemen risiko.
  - Persentase proposal proyek manajemen risiko yang ditolak karena kurangnya pertimbangan terhadap risiko terkait lainnya.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:
  - Memelihara inventarisasi aktivitas pengendalian yang ada untuk memitigasi risiko dan memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko. Klasifikasikan aktivitas pengendalian dan petakan ke dalam skenario risiko TI tertentu dan agregasi skenario risiko TI.
  - Tentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.

- Menetapkan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang strategis bagi perusahaan, dengan mempertimbangkan biaya, manfaat, dampak terhadap profil risiko dan peraturan saat ini.

- APO12.06 *respond to risk*, merespon peristiwa risiko yang terwujud secara tepat waktu dengan langkah-langkah efektif untuk membatasi besarnya kerugian.

  Metrics pengukurannya berupa:

  - Merespon peristiwa risiko yang terwujud secara tepat waktu dengan langkah-langkah efektif untuk membatasi besarnya kerugian.
  - Persentase rencana tindakan risiko TI dilaksanakan sesuai rancangan.

  Adapun aktivitas yang dilakukan pada komponen ini antara lain:

  - Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan.
  - Menerapkan rencana respon yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.
  - Kategorikan insiden dan bandingkan eksposur kerugian terkait TI dengan ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.
  - Periksa peristiwa/kerugian masa lalu dan peluang yang terlewatkan dan tentukan akar penyebabnya.
  - Komunikasikan akar masalah, persyaratan respon risiko tambahan, dan perbaikan proses kepada pengambil keputusan yang tepat. Pastikan penyebab, persyaratan respon, dan perbaikan proses disertakan dalam proses tata kelola risiko.

BAB III. METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

Dalam penelitian ini menggunakan data-data kualitatif yang dikumpulkan dengan metode studi literatur, wawancara, observasi, dan kuisioner yang diisi oleh pihak pihak yang bertanggung jawab atau berkepentingan terkait dengan data yang diperlukan. Data-data tersebut dikumpulkan untuk dijadikan *evidence* pada penelitian ini.

3.1.1 Studi Literatur

Studi literatur ini dilakukan dengan cara mengumpulkan informasi-informasi terkait penjelasan definisi, deskripsi, pelaksanaan, dan penelitian terdahulu. Hal ini dilakukan untuk menambah wawasan pada penelitian ini.

3.1.2 Wawancara

Wawancara dilakukan untuk mendapatkan informasi berkaitan dengan dokumen-dokumen, penyamaan persepsi, dan pembuktian dari *evidence* yang ada. Wawancara akan dilakukan kepada pihak-pihak terkait sebagai mana telah diatur pada COBIT 2019 berdasarkan *role* yang dipetakan menggunakan RACI *Chart*.

3.1.3 Observasi

Observasi dilakukan untuk mengetahui kegiatan-kegiatan dan menemukan *evidence* pada kegiatan ini. Metode ini digunakan sebagai pendukung untuk hasil wawancara atau dokumentasi

3.1.4 Kuisioner

Kuisioner dibuat untuk mendukung penemuan informasi seperti wawancara. Pada kuisioner ini disesuaikan dengan kebutuhan data *assessment* pada COBIT 2019.

3.2 Tempat Penelitian

Penelitian ini dilaksanakan di Politeknik Negeri Lampung sebagai *object* yang akan diteliti. Penelitian ini akan berfokus di UPA TIK Polinela sebagai unit yang bertanggung jawab untuk teknologi informasi yang ada di Polinela.

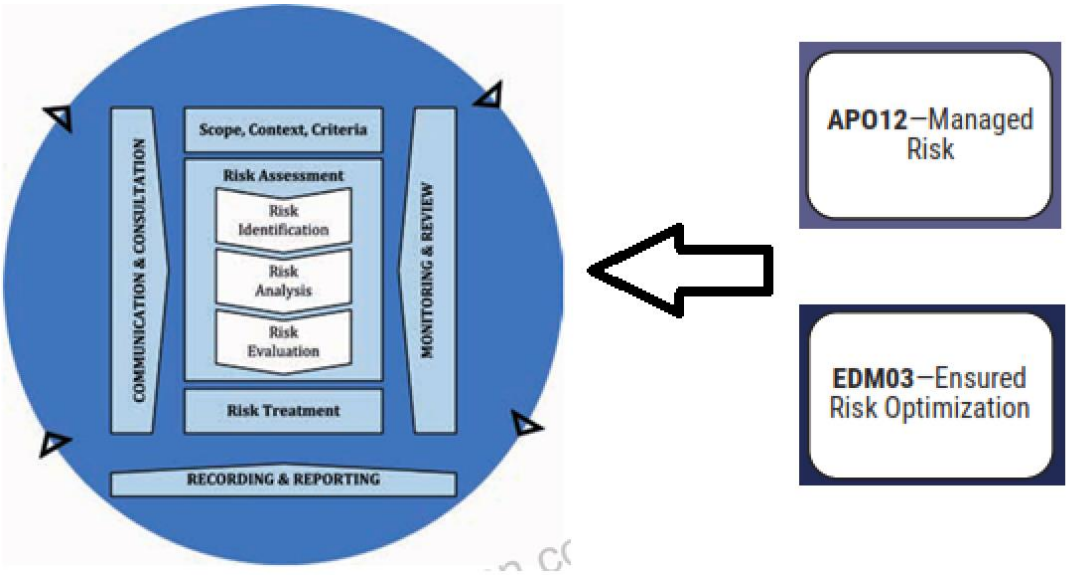
3.3 Waktu Penelitian

Penelitian ini akan dilaksanakan selama lima bulan. Pada bulan Desember dilakukan studi literatur dan koordinasi dengan UPA TIK terkait persiapan penelitian. Pada bulan Januari hingga Februari disusun proposal penelitian yang dilanjutkan pelaksanaan audit lapangan. Bulan Maret pengumpulan data, analisis data, dan evaluasi data. Pada bulan April dilakukan penyusunan hasil penelitian.

3.4 Alur Penelitian

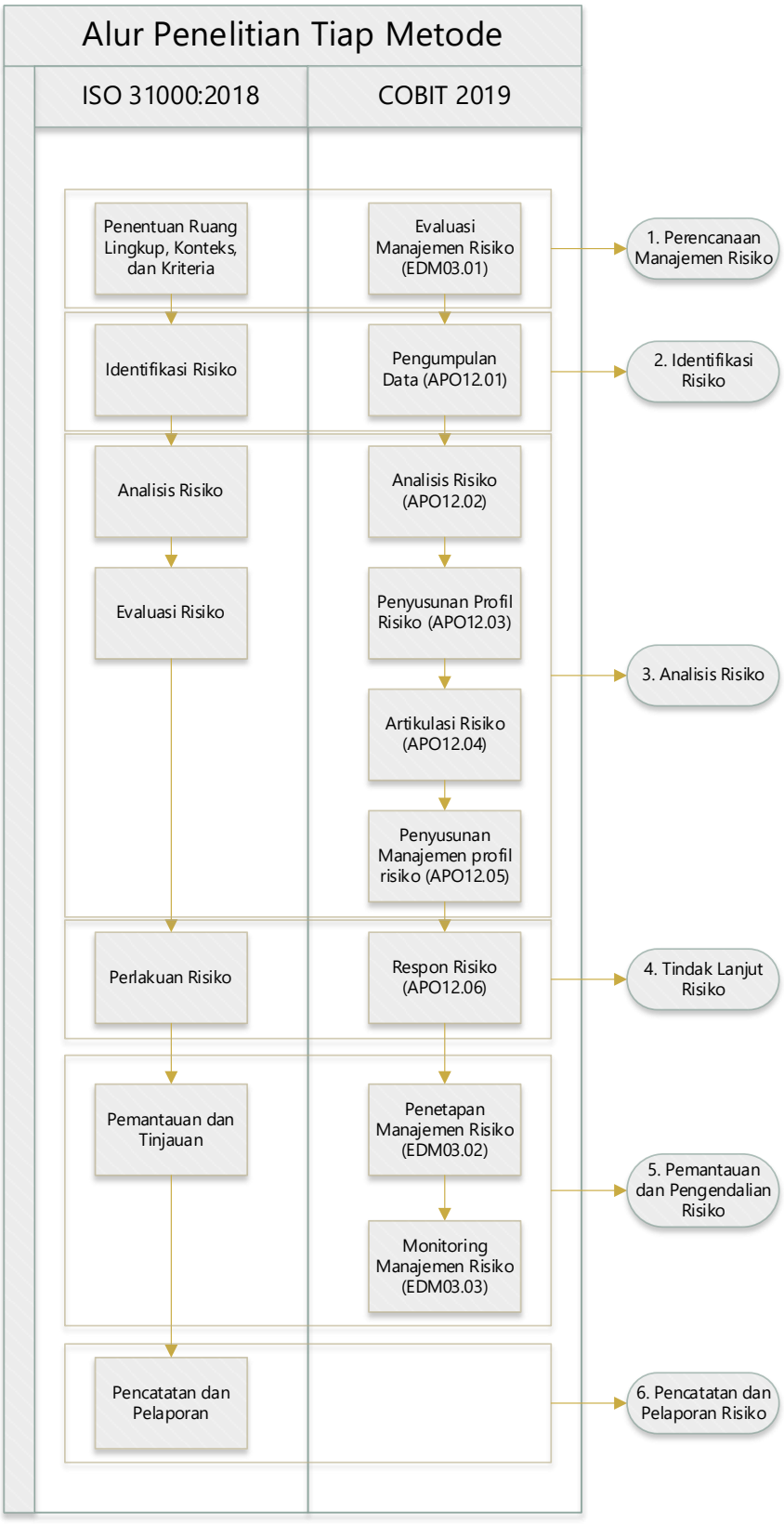
Penelitian ini memaksimal potensi yang dimiliki setiap framework, dengan ISO 31000:2018 menjadi standar dan COBIT 2019 menjadi *best practice*s sehingga keduanya menjadi penting untuk manajemen risiko dan tata kelola TI [28]. Pentingnya ISO 31000:2018 pada Politeknik Negeri Lampung karena selain ISO menjadi standar nasional untuk instansi pemerintah ISO 31000:2018 juga mampu berintegrasi dengan ISO 9001:2015 *Quality management* yang saat ini digunakan oleh Politeknik Negeri Lampung. Untuk COBIT 2019 sebagai *best practice*, dapat memberikan suatu tata kelola dan manajemen TI yang lebih komprehensif. Pada *Risk Event* ISACA yang diadakan di Amsterdam, ISACA menjelaskan COBIT 2019 memiliki *core model* yang berfokus pada tata kelola dan manajemen risiko antara lain EDM03-*Ensured Risk Optimisation* dan APO12-*Managed Risk* [29].

ISO 31000:2018 dan COBIT 2019 memiliki alur kegiatannya masing-masing yang digambarkan pada gambar berikut:



Gambar 3. 1 *Framework* ISO 31000:2018 dan COBIT 2019 *Risk Management*

Kedua Framework ini memiliki alur yang mirip, dengan kelompok proses yang sama. Alur tersebut dibandingkan, dinilai efektivitas, kebermanfaatan dan digunakan satu aktivitas pada setiap kelompok proses yang dapat mencakup kelengkapan untuk masing-masing tahapan. Adapun alur Penelitian dan kelompok proses setiap metode digambarkan pada gambar berikut:



Gambar 3. 2 Tahapan Alur Penelitian ISO 31000:2018 dan COBIT 2019

Adapun berikut adalah perbandingan alur dari kedua *framework* berdasarkan kelompok prosesnya masing masing:

a. Perencanaan Manajemen Risiko

Pada perencanaan ini diharapkan mendapatkan gambaran dari TI di Politeknik Negeri Lampung terkait dengan risikonya. Pada proses COBIT 2019 lebih baik digunakan untuk melakukan evaluasi terhadap yang sudah ada dibandingkan menentukan arah dan tujuan awal dari organisasi. Berdasarkan ini ISO 31000:2018 lebih memiliki tujuan yang dibutuhkan pada penelitian ini. Maka pada tahap perencanaan ini digunakan ISO 31000:2018.

b. Identifikasi Risiko

Pada Identifikasi risiko ini diharapkan mendapatkan mendeskripsikan risiko seluruh risiko yang ada. Menurut COBIT 2019 terdapat delapan aktivitas yang perlu dilakukan dan dijelaskan secara mendetail. Sedangkan ISO 31000:2018 memberikan gambaran untuk menemukan, memahami, dan mendeskripsikan risiko yang dapat membantu atau mencegah objektif dari pencapaian suatu tujuan organisasi yang mana hal ini sudah masuk ke dalam detail yang dijabarkan pada aktivitas COBIT 2019. Maka pada tahap Identifikasi Risiko ini digunakan COBIT 2019.

c. Analisis Risiko

Pada analisis risiko ini diharapkan mendapatkan analisis yang komprehensif terkait risiko yang dapat digunakan untuk proses selanjutnya. COBIT 2019 memiliki tiga objektif pada kelompok proses ini yang mana dijelaskan terperinci di dalam APO12.02, APO12.03 APO12.04. untuk kegiatan Analisis risiko ISO 31000:2018 memiliki analisis yang dapat digabungkan sesuai dengan kebutuhan Politeknik Negeri Lampung dan beberapa faktor yang perlu diperhatikan. Untuk kelompok proses analisis risiko mengikuti COBIT 2019 sebagai best practice dan analisis ISO 31000:2018 yang lebih mendetail terkait masing-masing masing risiko.

d. Tindak Lanjut Risiko

Pada kelompok proses ini keduanya memiliki proses yang sama yaitu risiko di hindari, kurangi, ditransfer atau diterima. Karena kelompok proses ini masih diperlukan sebuah *best practice* dari COBIT 2019 maka digunakan COBIT 2019 pada tindak lanjut risiko ini.

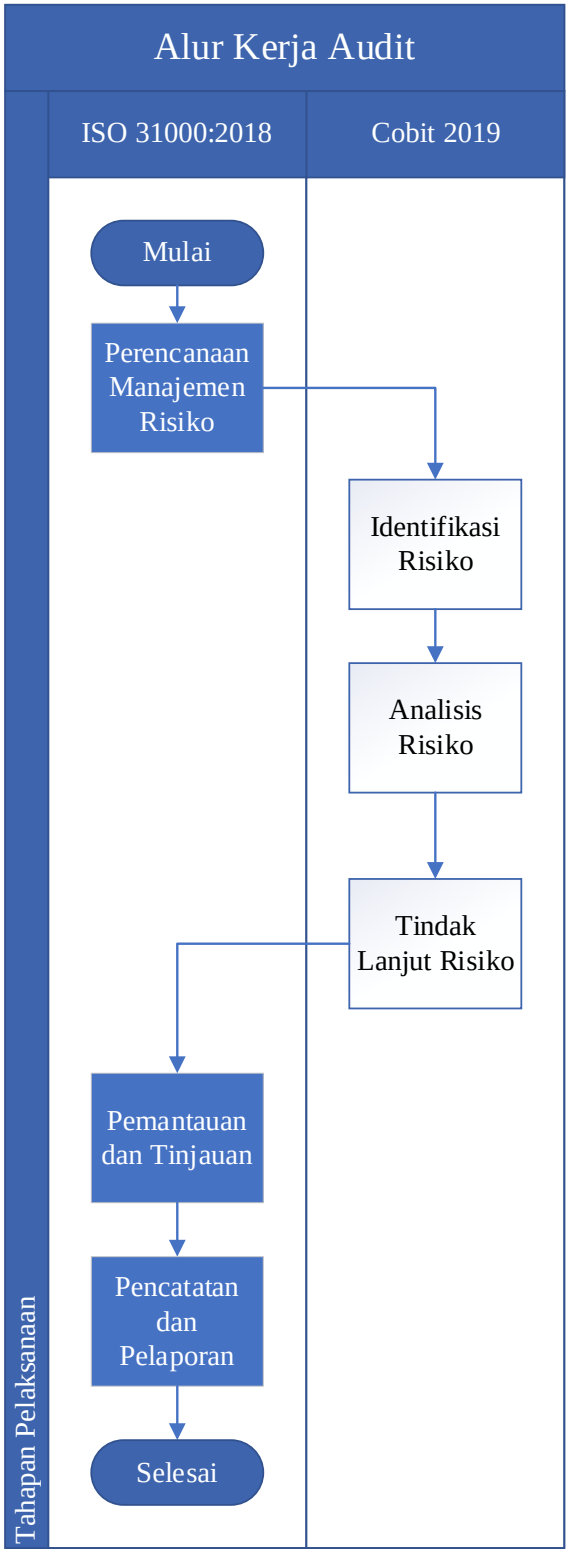
e. Pemantauan dan Pengedalian

Pada COBIT 2019 terdapat kegiatan EDM03.02 dan kegiatan EDM03.03 yang mana ini dilakukan di akhir kegiatan pada akhir proses yang mana perlu inputan dari EDM03.01 yang mana ada tahap perencanaan dilakukan berdasarkan proses ISO 31000:2018 sebagai alur kerja. berdasarkan hal tersebut maka ditetapkan ISO 31000:2018 yang mana memiliki proses pemantauan dan pengendalian pada setiap tahapan dalam proses tidak hanya diakhir proses.

f. Pencatatan dan Pelaporan

ISO 31000:2018 menyediakan proses pencatatan dan Pelaporan yang tidak dimiliki oleh COBIT 2019. Diharapkan pencatatan dan laporan ISO 31000:2018 ini dapat memberikan laporan terkait manajemen risiko, informasi terkait pengambilan keputusan dan meningkatkan aktivitas manajemen risiko.

Berdasarkan hasil perbandingan di atas, maka didapatkan alur kerja sebagai berikut:



Gambar 3. 3 Tahapan Pelaksanaan Audit

Rincian alur kerja tersebut dijelaskan masing-masing pada sub bagian dibawah ini.

3.4.1 Komunikasi dan Konsultasi

Pada tahapan ini dilakukan komunikasi dan konsultasi terhadap *object* yang diteliti. Pada tahapan ini didapatkan hasil *mapping* RACI *Chart* dan proses bisnis yang ada diteliti.

Berdasarkan Organisasi dan Tata Kerja Politeknik Negeri Lampung didapatkan RACI *chart* yang diusulkan sebagai berikut:

Tabel 3. 1 Responden APO12

No	*Role*	Bagian Unit yang Bertanggung Jawab (*Responsible*)
APO12.01 collect data		
1	*Chief Information Officer*	Kepala UPA TIK
2	*Chief Technology Officer*	Kepala UPA TIK
3	*Chief Digital Officer*	Kepala UPA TIK
4	*Chief Information Security Officer*	Kepala UPA TIK
5	*Business Process Owner*	Kepala UPA TIK
6	*Project Management Office*	Kepala UPA TIK
7	*Data Management Function*	Kepala UPA TIK
8	*Head Architect*	Kepala UPA TIK
9	*Head Development*	Kepala UPA TIK
10	*Head IT Operations*	Network Administrator
11	*Head IT Administration*	Helpdesk UPA/Adminsitrasi
12	*Service Manager*	Kepala UPA TIK
13	*Information Security Manager*	Kepala UPA TIK

Tabel 3. 2 Responden APO12 (Lanjutan)

No	Role	Bagian Unit yang Bertanggung Jawab (Responsible)
14	*Business Continuity Manager*	Kepala UPA TIK
15	*Privacy Officer*	Kepala UPA TIK
APO12.02 analyze risk		
1	*Chief Information Officer*	Kepala UPA TIK
2	*Enterprise Risk Committee*	Wakil Direktur Bidang Kerjasama dan Teknologi Informasi
3	*Business Process Owner*	Kepala UPA TIK
	APO12.03	
1	*Chief Information Officer*	Kepala UPA TIK
2	*Enterprise Risk Committee*	Wakil Direktur Bidang Kerjasama dan Teknologi Informasi
3	*Business Process Owner*	Kepala UPA TIK
APO12.03 maintain a risk profile		
1	*Chief Information Officer*	Kepala UPA TIK
2	*Enterprise Risk Committee*	Wakil Direktur Bidang Kerjasama dan Teknologi Informasi
3	*Business Process Owner*	Kepala UPA TIK
APO12.04 articulate risk		
1	*Chief Information Officer*	Kepala UPA TIK

Tabel 3. 2 Responden APO12 (Lanjutan)

No	Role	Bagian Unit yang Bertanggung Jawab (Responsible)
2	*Enterprise Risk Committee*	Wakil Direktur Bidang Kerjasama dan Teknologi Informasi
3	*Business Process Owner*	Kepala UPA TIK
APO12.05 define a risk management action portofolio		
1	*Chief Information Officer*	Kepala UPA TIK
2	*Enterprise Risk Committee*	Wakil Direktur Bidang Kerjasama dan Teknologi Informasi
3	*Business Process Owner*	Kepala UPA TIK
APO12.06 respond to risk		
1	*Chief Risk Officer*	Kepala UPA TIK
2	*Chief Technology Officer*	Kepala UPA TIK
3	*Chief Digital Officer*	Kepala UPA TIK
4	*Chief Information Security Officer*	Kepala UPA TIK
5	*Business Process Owner*	Kepala UPA TIK
6	*Project Management Office*	Kepala UPA TIK
7	*Head Architect*	Kepala UPA TIK
8	*Head Development*	Kepala UPA TIK
9	*Head IT Operations*	Network Administrator
10	*Head IT Administration*	Helpdesk UPA/Adminstrasi
11	*Service Manager*	Kepala UPA TIK

Tabel 3. 2 Responden APO12 (Lanjutan)

No	Role	Bagian Unit yang Bertanggung Jawab (Responsible)
12	*Information Security Manager*	Kepala UPA TIK
13	*Business Continuity Manager*	Kepala UPA TIK
14	*Privacy Officer*	Kepala UPA TIK

3.4.2 Penetapan Suatu Konteks

Dalam penelitian ini telah ditetapkan konteks yang diteliti adalah terkait manajemen risiko teknologi informasi yang menggunakan ISO 31000:2018 dan COBIT 2019. Pada COBIT 2019 menggunakan proses *assessment* pada APO12 sebagaimana ditetapkan oleh ISACA jika berbicara mengenai manajemen risiko teknologi informasi. Dan untuk bentuk pelaporan berdasarkan ISO 31000:2018. Diharapkan dalam penetapan konteks ini didapatkan hasil berupa

1. Tujuan dan Sasaran manajemen risiko yang diharapkan
2. Penanggung jawab manajemen risiko
3. Ruang lingkup dan kedalaman dari manajemen risiko
4. Metode penilaian risiko
5. Identifikasi keputusan yang diambil

3.4.3 Identifikasi Risiko

Setelah penetapan konteks yang diteliti selanjutnya dilakukan identifikasi risiko. Identifikasi ini dilakukan dalam tahap penilaian risiko pada alur proses, yang mana pada penelitian ini menggunakan komponen proses APO12.01 *Collect data* sebagai kerangka kerja *best practice* yang dapat digunakan sebagai bagian dari proses *assessment.* Pada tahapan ini menghasilkan daftar risiko TI yang ada. Daftar risiko TI yang ada dipetakan dalam matrik risiko yang sebagaimana pada tabel berikut:

Tabel 3. 2 Matrik Risiko yang diusulkan

Tingkat Kemungkinan/ Dampak	SR	R	S	B	E
SK	R	R	R	R	M
K	R	R	M	M	T
S	R	M	M	T	T
B	R	M	M	T	T
SB	M	M	T	T	T

Dengan tingkat kemungkinan dikategorikan sebagai berikut:

- Sangat Besar (SB)
- Besar (B)
- Sedang (S)
- Kecil (K)
- Sangat Kecil (SK)

Sedangkan untuk dampak yang dihasilkan dikategorikan sebagai berikut:

- Ekstrem (E)
- Besar (B)
- Sedang (S)
- Rendah (R)
- Sangat Rendah (SR)

Dan menghasilkan risiko dengan tingkat

- Rendah (R)
- Menengah (M)
- Tinggi (T)

Dengan kriteria dikomunikasikan dan dikonsultasikan terlebih dahulu dengan Kepala UPA TIK Politeknik Negeri Lampung. Adapun rincian aktivitas APO12.01 yang dilakukan pada tahapan ini antara lain:

- Menetapkan dan memelihara metode pengumpulan, klasifikasi, dan analisis data terkait risiko TI.
- Mencatat data terkait risiko TI yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.
- Mengadopsi atau menentukan taksonomi risiko untuk definisi yang konsisten mengenai skenario risiko serta kategori dampak dan kemungkinan.
- Catat data kejadian risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditentukan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.
- Mensurvei dan menganalisis data historis risiko TI dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan-rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.
- Untuk rangkaian acara serupa, atur data yang dikumpulkan dan soroti faktor-faktor yang berkontribusi. Tentukan kontribusi faktor umum di berbagai peristiwa.
- Tentukan kondisi spesifik yang ada atau tidak ada ketika peristiwa risiko terjadi dan bagaimana kondisi tersebut mempengaruhi frekuensi peristiwa dan besarnya kerugian.
- Melakukan analisis peristiwa dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk mendapatkan pemahaman tentang faktor risiko internal dan eksternal terkait.

Tabel 3. 3 Daftar *Work Product* APO12.01

Nomor	***Work Product Number***	**Deskripsi**
1	APO12-WP1	Data lingkungan operasional terkait dengan risiko
2	APO12-WP2	Data faktor penyebab dan kejadian risiko
3	APO12-WP3	Isu terkait risiko dan faktor penyebabnya

3.4.4 Analisis Risiko

Analisis risiko juga sama hal nya pada proses identifikasi risiko menggunakan proses komponen APO12.02, APO12.03 APO12.04 APO12.05 serta menggunakan ISO. Setelah melakukan *collect data*, maka risiko tersebut dianalisis, dikembangkan menjadi sebuah gambaran umum risiko yang terjadi pada TI di Polinela. Pada proses ini juga dilakukan desain faktor untuk *Risk Profile* dan *I&T Issues* yang ditetapkan berkaitan dengan manajemen risiko. Pada proses analisis risiko ini dilakukan kegiatan

1. Penentuan ruang lingkup analisis risiko berdasarkan faktor risiko dan aset
2. Pengendalian dan upaya deteksi risiko yang ada
3. Merancang kemungkinan kerugian dari terjadinya risiko
4. membuat selera risiko dan toleransi risiko
5. membuat skenario risiko berdasarkan kategori risiko
6. merancang profil risiko
7. melakukan analisis desain faktor

Dengan aktivitas yang dilakukan diatas diharapkan mendapatkan *Work Product* berupa Profil Risiko, skenario risiko, dan laporan desain faktor *Risk Profile* dan *I&T Issues*.

Aktivitas pada APO12.02 antara lain adalah:

- Tentukan ruang lingkup upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kepentingan bisnis aset.
- Membangun dan memperbarui skenario risiko TI secara rutin; eksposur kerugian terkait TI; dan skenario mengenai risiko reputasi,

termasuk skenario gabungan dari jenis dan peristiwa ancaman yang terjadi secara berjenjang dan/atau secara kebetulan. Kembangkan harapan untuk aktivitas pengendalian spesifik dan kemampuan untuk mendeteksi.

- Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.
- Bandingkan risiko saat ini (paparan kerugian terkait TI) dengan selera risiko dan toleransi risiko yang dapat diterima. Identifikasi risiko yang tidak dapat diterima atau meningkat.
- Mengusulkan respon risiko untuk risiko yang melebihi tingkat selera risiko dan toleransi.
- Tentukan persyaratan tingkat tinggi untuk proyek atau program yang menerapkan respon risiko yang dipilih. Identifikasi persyaratan dan harapan untuk pengendalian utama yang tepat untuk respon mitigasi risiko.
- Validasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Konfirmasikan bahwa analisis tersebut selaras dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui adanya bias.
- Menganalisis biaya/manfaat dari opsi respon risiko potensial seperti menghindari, mengurangi/mitigasi, mentransfer/membagi, dan menerima dan mengeksploitasi/merebut. Konfirmasikan respon risiko yang optimal.

Aktivitas pada APO12.03 antara lain adalah:

- Inventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen layanan TI dan sumber daya infrastruktur TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, *vendor*, pemasok, dan agen *outsourcing*.

- Menentukan dan menyepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan pengoperasian proses bisnis. Analisis ketergantungan dan identifikasi tautan lemah.
- Gabungkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.
- Catat semua informasi profil risiko secara berkala dan konsolidasikan ke dalam profil risiko gabungan.
- Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko TI perusahaan.
- Berdasarkan seluruh data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan risiko saat ini dan tren risiko secara cepat.
- Menangkap informasi mengenai peristiwa risiko TI yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan.

Aktivitas pada APO12.04 antara lain adalah:

- Laporkan hasil analisis risiko kepada seluruh *stakeholder* yang terkena dampak dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan kisaran kerugian atau keuntungan serta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan keuntungan dan risiko.
- Memberikan pemahaman kepada pengambil keputusan tentang skenario terburuk dan paling mungkin terjadi, paparan kerugian terkait TI dan TI dan reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.
- Laporkan profil risiko terkini kepada seluruh *stakeholder*. Meliputi informasi mengenai efektivitas proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status remediasi dan dampaknya terhadap profil risiko.
- Secara berkala, untuk wilayah dengan risiko relatif dan kapasitas risiko yang setara, identifikasi peluang terkait TI yang

memungkinkan penerimaan risiko lebih besar serta peningkatan pertumbuhan dan keuntungan.

- Meninjau hasil penilaian pihak ketiga yang objektif dan audit internal serta tinjauan jaminan kualitas. Sertakan mereka dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait TI untuk menentukan perlunya analisis risiko tambahan.

Aktivitas pada APO12.05 antara lain adalah:

- Memelihara inventarisasi aktivitas pengendalian yang ada untuk memitigasi risiko dan memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko. Klasifikasikan aktivitas pengendalian dan petakan ke dalam skenario risiko TI tertentu dan agregasi skenario risiko TI.
- Tentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.
- Menetapkan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang strategis bagi perusahaan, dengan mempertimbangkan biaya, manfaat, dampak terhadap profil risiko dan peraturan saat ini.

Dan *Work Product* sebagai berikut:

Tabel 3. 4 Daftar *Work Product* APO12.02, APO12.03, APO12.04, APO12.05

Nomor	***Work Product Number***	**Deskripsi**
1	APO12-WP4	Ruang Lingkup dari analisis risiko yang dilakukan
2	APO12-WP5	Skenario risiko TI
3	APO12-WP6	Hasil Analisis Risiko
4	APO12-WP7	profil risiko, termasuk status manajemen risiko yang dilakukan

Tabel 3. 5 Daftar *Work Product* APO12.02, APO12.03, APO12.04, APO12.05 (Lanjutan)

Nomor	*Work Product Number*	Deskripsi
5	APO12-WP8	Dokuementasi skenario risiko berdasarkan bisnis dan fungsi
6	APO12-WP9	Laporan analisis risiko dan profil risiko untuk stakeholder
7	APO12-WP10	Hasil penilaian risiko dari pihak ketiga
8	APO12-WP11	Peluang untuk penerimaan risiko
9	APO12-WP12	proposal untuk mengurangi risiko

3.4.5 Perlakuan Risiko

Selanjutnya dilakukan perlakuan risiko dengan menggunakan komponen proses COBIT 2019 APO12.06. Dengan APO12.06 diharapkan risiko-risiko tersebut dapat diberikan perlakuan sesuai dengan kebutuhan dan dampak yang dihasilkan.

Aktivitas pada APO12.06 antara lain adalah:

- Mempersiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan.
- Menerapkan rencana respon yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.
- Kategorikan insiden dan bandingkan eksposur kerugian terkait TI dengan ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.
- Periksa peristiwa/kerugian masa lalu dan peluang yang terlewatkan dan tentukan akar penyebabnya.
- Komunikasikan akar masalah, persyaratan respon risiko tambahan, dan perbaikan proses kepada pengambil keputusan yang tepat.

Pastikan penyebab, persyaratan respon, dan perbaikan proses disertakan dalam proses tata kelola risiko.

Dan *Work Product* sebagai berikut:

Tabel 3. 5 Daftar *Work Product* APO12.06

Nomor	*Work Product Number*	Deskripsi
1	APO12-WP13	Rencana penanggulangan risiko
2	APO12-WP14	Komunikasi terkait dampak dari risiko
3	APO12-WP15	Akar penyebab terkait risiko

3.4.6 Pemantauan dan Tinjauan

Berdasarkan hasil dokumentasi perlakuan risiko tersebut dikomunikasi kepada direksi/*stakeholder* untuk mendapatkan masukan-masukan untuk profil risiko yang ada, selanjutnya dibuatkan sebuah portofolio manajemen risiko.

3.4.7 Pencatatan dan Pelaporan

Hasil dari portofolio manajemen risiko tersebut didikomentasikan dengan rapih dan dilaporkan sebagai tindak lanjut dari manajemen risiko yang dapat dijadikan pedoman dalam tata kelola risiko di Politeknik Negeri Lampung.

BAB V. KESIMPULAN DAN SARAN

Risiko merupakan nilai tambah maupun nilai kurang untuk perusahaan, dengan adanya manajemen risiko yang baik risiko tersebut dapat dicegah, dikurangi, atau menjadi penguatan dari bisnis perusahaan dalam hal ini pengelolaan TI di UPA TIK Polinela. adapun Kesimpulan dan saran yang didapatkan dalam penelitian ini antara lain:

1. Berdasarkan hasil kuesioner tersebut didapatkan tingkat *capability level* dua dimana tingkat *capability* ini Polinela telah melakukan aktivitas untuk mencapai tujuannya melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan sebagai telah berjalan secara operasional. Terdapat *gap* dengan nilai dua tingkat pada kondisi terkini dan kondisi yang diharapkan karena berdasarkan hasil analisis desain faktor yang dilakukan capability yang diharapkan berada di level empat. Hal ini membuat beberapa masukan terkait aktivitas yang perlu dilakukan pada APO12. Tingkat *capability* saat ini menjadi tingkat *Managed* yang mana risiko-risiko sudah dilakukan manajemen, namun belum terdokumentasi dengan lengkap, belum terukur, dan belum dikembangkan menjadi potensi kedepannya. Diharapkan dengan adanya penelitian ini dapat menjadi alat ukur untuk mencapai tingkat selanjutnya.
2. Risiko-risiko yang telah terdokumentasi tedapat delapan risiko dengan level tinggi yang perlu perhatian tambahan dan segera dilakukan perlakuan risiko. Risiko tersebut diharapkan didokumentasikan dan dipelajari guna mengurangi dampak dari risiko tersebut. Sedangkan untuk 35 risiko menengah dapat dipantau dan dilakukan pengendalian. Untuk level rendah sebanyak 25 risiko dapat dipelajari apakah dapat menjadi peluang nilai tambah karena risiko ini jarang terjadi ataupun memiliki dampak yang rendah. Adapun jika diambil kesimpulan,

rekomendasi pengendalian risiko pada UPA TIK adalah lakukan analisis ulang terhadap kebutuhan bisnis dan ketersediaan aset-aset TI, Perkuat proteksi atau keamanan dari perangkat keras dan lunak yang ada telah ada, pemantauan secara periodik terhadap aset-aset TI, penguatan dan pelatihan staff, dan lakukan *backup* dilakukan secara periodik

3. Dari penggabungan dua *framework* manajemen risiko ini dapat dihasilkan sebuah manajemen risiko yang komprehensif. *Framework* ISO 31000:2018 membentuk sebuah pengendalian risiko sedangkan COBIT 2019 membuat sebuah pondasi untuk kegiatan manajemen yang dilakukan.
4. Saran untuk pengembangan penelitian selanjutnya yaitu, melakukan audit dengan *framework* yang lainnya guna mendapatkan analisis perbandingan antara setiap *framework* dan dapat digunakan sebagai acuan untuk penggunaan *framework* yang tepat untuk memenuhi kebutuhan manajemen risiko.
5. COBIT 2019 memiliki ruang lingkup yang sangat luas, sehingga dapat digunakan untuk melakukan audit dengan ruang lingkup lainnya sebagai contoh, ISO 27000 tentang Manajemen Keamanan, ISO 38500 terkait dengan Tata Kelola dan lainnya.

DAFTAR PUSTAKA

[1] Marius Robert Seran, "Teknologi Informasi Pembentuk Multiplier Effect Dalam Bisnis Corporasi," *J. Manage.*, vol. 3, no. 2, pp. 263–274, 2016.

[2] M. R. A. Ahadis, G. F. Nama, R. Annisa, and M. A. Muda, "AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA PT BANK RAKYAT INDONESIA UNIT 1 PRINGSEWU," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 2, pp. 1454–1462, 2025.

[3] R. dan T. Kementerian Pendidikan, Kebudayaan, *Organisasi dan Tata Kerja Politeknik Negeri Lampung*, no. 021. 2022.

[4] L. Ernawati and H. B. Santoso, "Identifikasi dan Analisa Risiko Penerapan Teknologi Informasi di Lingkungan Perguruan Tinggi," *Seri Pros. Semin. Nas. Din. Inform.*, vol. 1, no. 1, pp. 21–28, 2017.

[5] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019.

[6] N. Al Hakim, R. Fauzi, and I. Santosa, "Analisis Dan Perancangan Proses Manajemen Risiko Ti Menggunakan Kerangka Kerja Cobit 2019 Di Pt Inti (Persero) Analysis and Design of It Risk Management Process Using Framework Cobit 2019 in Pt Inti (Persero)," *e-Proceeding Eng.*, vol. 7, no. 3, pp. 9635–9642, 2020.

[7] E. Ritegno, "Control Objective and Information Related Technology," 2018.

[8] ISO 31000, *BSI Standards Publication Risk management — Guidelines*. 2018.

[9] A. P. Aisyah and L. Dahlia, "Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti," *J. Akunt. dan Manaj.*, vol. 19, no. 02, pp. 78–90, 2022, doi: 10.36406/jam.v19i02.483.

[10] S. Al-Tahat and O. A. Moneim, "Impact of COSO and COBIT5 Regulatory Integration in the Correct Application of Cyber Governance in Jordanian Commercial Banks," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 7138–7144, 2020, doi: 10.30845/ijbss.v12n4p6.

[11] K. Aprianto, E. Endroyono, and S. M. S. Nugroho, "Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan (E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000:2018 in Magetan Regency)," *J.*

IPTEKKOM J. Ilmu Pengetah. Teknol. Inf., vol. 23, no. 2, pp. 107–122, 2021, doi: 10.17933/iptekkom.23.2.2021.107-122.

[12] P. P. Sukmana, T. P. Yoga, and C. Habibi, "Audit Manajemen Risiko Sistem Informasi pada Website Digo.id dengan Framework COBIT 5 dan ISO 31000," *J. Account. Inf. Syst.*, vol. 6, no. 2, pp. 180–201, 2023, doi: 10.32627/aims.v6i2.816.

[13] W. Jordy, L. W. Santoso, and Y. Yulia, "Penerapan Manajemen Risiko IT pada Bank X dengan Menggunakan Framework COBIT 2019," *J. Infra*, vol. 10, no. 2, 2022.

[14] J. S. 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," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 5, pp. 1734–1744, 2021.

[15] R. Anugrah, E. Utami, and A. H. Muhammad, "Analisis Manajemen Risiko TI Pada Perguruan Tinggi XYZ Berbasis COBIT 2019 Dengan Pertimbangan Domain APO12," *J. Ilm. Univ. Batanghari Jambi*, vol. 22, no. 2, p. 991, 2022, doi: 10.33087/jiubj.v22i2.2175.

[16] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[17] H. A. N. Sari, Y. Rahardja, and H. P. Chernovita, "Analisis Manajemen Risiko TI pada DISKOMINFO Salatiga menggunakan Cobit5 dengan Domain APO12," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 1772–1784, 2021, doi: 10.35957/jatisi.v8i4.1089.

[18] T. Penyusun, *Rencana Pengembangan Jangka Panjang Politeknik Negeri Lampung 2020-2045*. 2019.

[19] S. D. Putra, "Struktur Organisasi UPA TIK Polinela."

[20] IT Governance Institute, *Second edition 2*. 2003.

[21] Badan Standardisasi Nasional, *Manajemen risiko - Prinsip dan Pedoman (ISO 31000:2009,DT)*. 2011.

[22] A. R. Viyanto, O. S. Latuihamallo, F. M. Tua, and A. Gui, "Studi Kasus Pada Perusahaan Jasa," *Comtech*, vol. 4, pp. 43–54, 2013.

[23] C. N. Sugiharto, A. Setiawan, and S. Rostianingsih, “Penerapan Manajemen Risiko Teknologi Informasi Pada Perusahaan PT. X,” *J. Infra*, vol. 10, no. 1, pp. 43–49, 2022.

[24] Badan Standardisasi Nasional, *Manajemen Risiko Berbasis SNI ISO 31000*, vol. 6, no. August. Jakarta, 2018.

[25] Information Systems Audit and Control Association, *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. 2018.

[26] ISACA, *COBIT 2019 Framework: Designing an Information and Technology Governance Solution*. 2019.

[27] ISACA Governance and Manajement, *COBIT 2019 Governance and Management Objectives (ISACA)*. 2019.

[28] Ahmet EFE, “A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT,” *J. Audit. Assur. Serv.*, vol. 3, no. 2, pp. 185–205, 2023.

[29] ISACA, “COBIT 2019 And Risk Management,” April. ISACA, Amsterdam, pp. 1–79, 2019.