BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Analisis

Menurut Noeng Muhadjir (1998:104), Analisis merupakan suatu kegiatan identifikasi atau usaha sistematis untuk mencari dan mencatat hasil berdasarkan proses observasi, wawancara, dan metode lain yang diterapkan dalam pengumpulan data. Tujuan dari analisis ini adalah untuk meningkatkan pemahaman peneliti terhadap kasus yang sedang diteliti, serta menyajikannya sebagai temuan yang bermanfaat bagi pihak lain.Dengan menerapkan proses analisis, peneliti dapat menggali informasi yang mendalam dari data yang sudah terkumpul.

Pada proses analisis untuk mencapai pemahaman yang lebih mendalam tidak cukup hanya dilakukan analisis pada tingkat deskripsi atau pengelompokan data saja. Tetapi perlu dilanjutkan dengan upaya mencari makna dari data yang telah diidentifikasi. Proses mencari makna ini melibatkan interpretasi dan penafsiran terhadap informasi yang terkandung dalam data, sehingga dapat memberikan wawasan dan pemahaman lebih luas.

Analisis pada dasarnya mencakup kejadian, tindakan, atau keadaan yang sesungguhnya, yang terdapat dalam data yang telah dikumpulkan. Dalam konteks penelitian kualitatif, ada sebuah tabel konkret yang berisi kejadian, tindakan, peristiwa, dan keadaan yang sebenarnya. Jadi konseptualisasi, kategorisasi, dan deskripsi dalam penelitian kualitatif berasal dari kejadian yang ditemukan selama

kegiatan lapangan. Oleh karena itu, pengumpulan dan analisis data tidak dapat dipisahkan, keduanya berlangsung secara bersamaan (Uin & Banjarmasin, 2018).

2.1.2 Risiko dan Manajemen Risiko

Risiko merupakan suatu kejadian yang pasti terjadi dan dapat menimbulkan permasalahan terhadap pencapaian tujuan dan keinginan tertentu. Risiko menjadi suatu tantangan bagi setiap organisasi karena diperlukan kemampuan untuk melakukan manajemen risiko yang tepat. Penerapan manajemen risiko sangat perlu untuk memberikan perlindungan terhadap organisasi tersebut serta mampu menciptakan nilai tambah (YAP Pardjo, 2017).

Sebuah organisasi,instansi, atau perusahaan manapun harus memahami pentingnya manajemen risiko, karena mengingat pertumbuhan dan kompleksitas aktivitas yang dapat meningkatkan risiko yang dihadapi oleh organisasi. Salah satu tujuan utama penerapan manajemen risiko adalah melindungi perusahaan atau organisasi dari potensi kerugian atau risiko yang mungkin timbul di masa mendatang. Dan hasil dari manajemen risiko sangat bermanfaat bagi perusahaan atau organisasi tersebut sebagai masukkan dan bahan pertimbangan (Arifudin O et al., 2020). Jadi manajemen risiko merupakan proses yang dilakukan untuk menemukan, mengukur, dan membuat strategi untuk mengelola risiko yang belum terjadi pada suatu organisasi (Soputan et al., 2014).

2.1.3 Analisis Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi adalah suatu proses penting dalam organisasi untuk mengidentifikasi, mengukur, dan mengembangkan strategi dalam

mengelola risiko dengan memanfaatkan sumber daya yang tersedia. Dalam proses ini ada beberapa pendekatan yang diambil untuk mengelola risiko, yang mencakup transfer risiko, menghindari risiko, mengurangi dampak negatifnya, dan menerima sebagian atau seluruh konsekuensi dari risiko tertentu (Thenu et al., n.d.).

Analisis teknologi informasi berbasi manajemen risiko merupakan proses analisis yang diterapkan untuk menganalisis risiko yang berkaitan dengan teknologi informasi. Dalam teknologi informasi, tujuan dari manajemen risiko adalah untuk memperoleh pemahaman yang lebih mendalam mengenai potensi risiko atau potensi kegagalan yang dapat mempengaruhi pencapaian tujuan organisasi. Karena pada dasarnya, peran teknologi informasi sangat penting dalam mendukung kebutuhan dan pencapaian tujuan organisasi. Oleh karena itu, diperlukan manajemen risiko Teknologi Informasi (TI). Analisis manajemen risiko teknologi informasi melibatkan identifikasi, evaluasi, dan pengelolaan risiko-risiko yang mungkin terjadi dalam penggunaan teknologi informasi (Putu et al., n.d.).

2.1.4 Metode COBIT 2019

COBIT merupakan singkatan dari Control Objectives for Information and Related Technologies, yang berupa sebuah kerangka kerja yang merangkum berbagai aspek terutama terkait dengan pengendalian internal yang berkaitan dengan teknologi informasi. COBIT mempunyai tujuan utama yaitu sebagai proses pengembangan, pengenalan, dan penyajian kewenangan kontrol objektif. COBIT berguna sebagai panduan komprehensif dalam mengelola dan mengendalikan aspek-aspek teknologi informasi (Anugrah et al., 2022).

COBIT mempunya prinsip dasar, prinsip-prinsip ini menjelaskan kebutuhan utama untuk membangun sistem tata kelola informasi dan teknologi dalam sebuah perusahaan. Prinsip ini dapat dijadikan pedoman untuk kerangka kerja tata kelola yang efektif.

Enam Prinsip Sistem Tata kelola:

1. Kebutuhan Pemangku Kepentingan

   Setiap perusahaan atau organisasi membutuhkan sistem tata kelola untuk memenuhi harapan pemangku kepentingan dan menghasilkan nilai melalui penggunaan informasi dan teknologi. Nilai ini tercermin dari keseimbangan antara manfaat yang diperoleh, risiko yang dihadapi, dan sumber daya yang digunakan.

2. Komponen yang Holistik

   Sistem tata kelola perusahaan terdiri dari beberapa komponen yang beragam, tetapi semua komponen tersebut harus bekerja secara menyeluruh dan terpadu.

3. Sistem yang Dinamis

   Sistem tata kelola harus bersifat dinamis, jika terjadi perubahan maka dampak terhadap sistem tata kelola harus diperhitungkan. Dengan ini makan dapat membantu menciptakan sistem tata kelola yang baik dan siap menghadapi masa depan.

4. Pemisah antara Tata Kelola dan Manajemen

   Sistem tata kelola harus dengan jelas dalam membedakan antara aktivitas tata kelola dan aktivitas serta struktur manajemen.

5. Penyesuaian dengan Kebutuhan Perusahaan

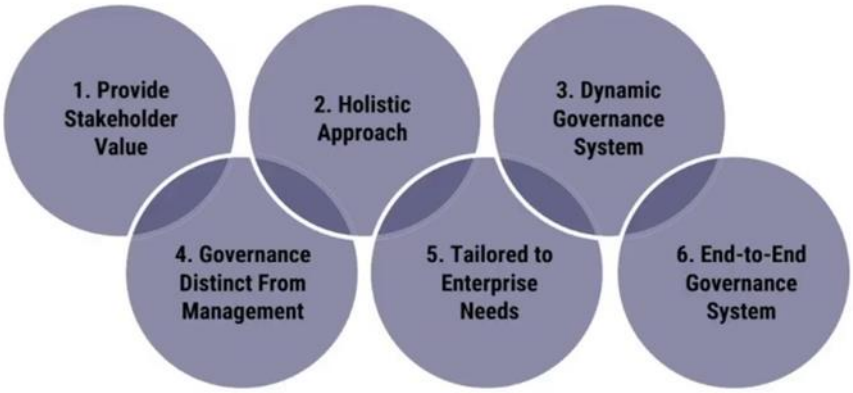
   Sistem tata kelola harus disesuaikan dengan kebutuhan spesifik perusahaan, dengan beberapa faktor untuk menyesuaikan dan memprioritaskan komponen sistem tata kelola.

6. Cakupan Menyeluruh

   Sistem tata kelola harus mencakup seluruh bagian perusahaan, tidak hanya fokus pada fungsi teknologi informasi saja, tetapi mencakup semua proses teknologi dan informasi yang dilakukan oleh perusahaan untuk mencapai tujuannya.

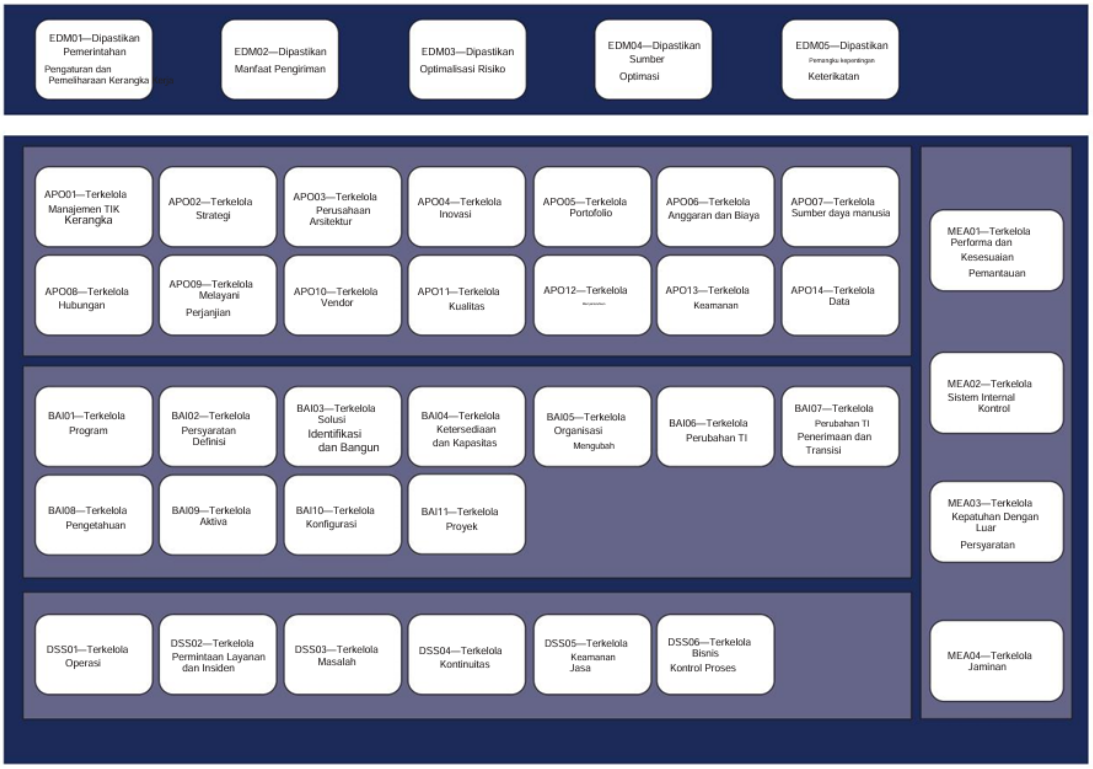
Sebelumnya, COBIT menggunakan kerangka kerja COBIT 5 yang hanya memiliki 5 prinsip fokus utama dalam teknologi informasi dan memberikan panduan yang terintegrasi bagi seluruh organisasi. Namun dengan perkembangan kebutuhan dan pengelolaan tata kelola teknologi informasi semakin kompleks, maka terjadinya perubahan yang awalnya COBIT 5 menjadi COBIT 2019. COBIT versi terbaru sekarang sudah dilakukan pengembangan dengan teknologi saat ini, dan juga sudah dilakukan integrasi dengan framework lain seperti ITIL, TOGAF dan CMII (Syuhada, 2021).

Dalam COBIT 2019, terdapat enam prinsip yang didefinisikan untuk menjelaskan persyaratan inti dalam sistem tata kelola suatu instansi atau perusahaan, yang dapat dilihat pada Gambar 2.1.



Gambar 2.1 Prinsip COBIT 2019 (ISACA, 2018)

Berdasarkan Gambar 2.1 dijelaskan bahwa saat ini COBIT versi 2019 memiliki enam prinsip mulai dari, pemenuhan kebutuhan kepentingan (*stakeholder*), pendekatan holistic, penerapan sistem tata kelola secara dinamis, pemisahan tata kelola dan manajemen, penyesuaian dengan kebutuhan, dan mencakup keseluruhan organisasi (Syuhada, 2021).



Gambar 2.2 Model Inti COBIT 2019

Bisa dilihat pada Gambar diatas bahwa metode COBIT versi 2019 saat ini, menetapkan lima domain sebagai tujuan utama dan masing-masing domainnya mempunyai fokus tertentu. Model COBIT tersebut dapat digunakan dan di sesuaikan dengan keadaan perusahaan maupun organisasi.

2.1.5 Evaluate, Direct, Monitor (EDM)

Menurut ISACA 2019 EDM ini merupakan kerangka kerja yang bertujuan untuk proses pendekatan yang konsisten, terintegrasi, dan selaras dalam tata kelola perusahaan, yang berkaitan dengan teknologi informasi untuk mendukung strategi dan tujuan perusahaan secara keseluruhan. Sehingga setiap rencana, kebijakan, dan kegiatan yang berhubungan dengan teknologi informasi harus dirancang dan

dijalankan dengan mempertimbangkan dengan tujuan perusahaan, sehingga sejalan dengan visi dan misi sasaran jangka panjang perusahaan.

Dalam proses ini juga menekankan pentingnya nilai yang diharapkan supaya tercapai. Proses untuk tercapainya nilai tersebut harus diukur dengan jelas secara efektif dan transparan, sehingga semua pihak, dari segi internal atau eksternal bisa memahami dan memantau bagaimana suatu keputusan dan proses dijalankan. Semua proses atau aktivitas harus dipastikan memenuhi semua persyaratan atau aturan hukum, standar keamanan informasi, atau hal lainya. Intinya proses EDM ini harus dirancang agar mendukung pencapaian tujuan bisnis atau perusahaan, tapi tidak dilakukan secara terpisah, dan harus diawasi dengan transparansi yang tinggi.

EDM ini memiliki beberapa subdomain atau aktivitas untuk prosesnya, subdomain tersebut yaitu sebagai berikut:

1. EDM01 (Memastikan pengaturan dan pemeliharaan kerangka kerja tata kelola), Proses ini bertujuan untuk menganalisis tata kelola IT perusahaan, dan mengelola tata kelola dengan jelas untuk menentukan wewenang, tanggung jawab untuk mencapai misi, dan tujuan perusahaan.
2. EDM02 (Pemberian manfaat yang pasti), tujuan dari domain ini yaitu untuk mengoptimalkan terkait nilai-nilai bisnis dalam proses bisnis, layanan TI, dan aset TI di dalam suatu perusahaan.
3. EDM03 (Memastikan optimasi risiko), EDM03 ini bertujuan untuk mengevaluasi terkait pengaruh risiko pada penggunaan teknologi informasi saat ini dan masa yang akan datang.

4. EDM04 (Memastikan optimalisasi sumber daya), tujuan dari domain ini yaitu untuk memastikan atau menciptakan suatu bisnis yang baik beserta sumber daya dan teknologinya. dan diharapkan proses ini dapat mendukung perusahaan untuk mencapai tujuannya secara efektif dan dengan biaya yang optimal.
5. EDM05 (Memastikan keterlibatan pemangku kepentingan), tujuan domain ini yaitu untuk memastikan bahwa semua pemangku kepentingan di perusahaan dapat terlibat dalam proses identifikasi sistem tata kelola TI, pengukuran kinerja TI, supaya proses tersebut selaras atau sejalan dengan strategi perusahaan.

2.1.6 Align, Plan, Organize (APO)

APO (*Align, Plan, Organize*) adalah suatu kerangka kerja yang bermanfaat dalam pemahaman menyeluruh terkait organisasi, strategi, dan kegiatan yang mendukung bidang teknologi informasi. Kerangka kerja ini membantu dalam menyelidiki struktur organisasi dan mengidentifikasi aktivitas yang mendukung implementasi dan pengelolaan teknologi informasi. APO ini memiliki beberapa subdomain yang dapat dijelaskan sebagai berikut :

1. APO01 Kerangka manajemen IT terkelola, tujuan dari subdomain APO ini untuk merancang suatu sistem manajemen IT perusahaan, tetapi sesuai dengan tujuan perusahaan dan faktor desain lainnya.
2. APO02 Strategi terkelola, tujuan domain ini untuk mendukung terkait strategi transformasi digital organisasi dan memberikan nilai yang diharapkan.

3. APO03 Mengelola Arsitektur perusahaan, domain ini bertujuan untuk membentuk perusahaan yang berkaitan dengan prinsip desain dan evolusi, untuk mencapai tujuan operasional yang standar dan efisien.
4. APO04 Inovasi Terkelola, domain ini bertujuan untuk meningkatkan dan mencapai keunggulan dalam pengalaman pelanggan, efisiensi operasional dengan memanfaatkan perkembangan IT.
5. APO05 Portofolio terkelola, tujuan domain ini untuk mengoptimalkan terkait kinerja seluruh portofolio program individual, kinerja serta perubahan dan permintaan perusahaan.
6. APO06 (Anggaran dan biaya terkelola), domain ini bertujuan mengelola terkait keuangan yang berhubungan dengan IT dan fungsi bisnis, dengan menggunakan domain ini dapat memungkinkan penggunaan sumber daya yang efektif dan transparansi, sehingga memungkinkan perusahaan untuk membuat keputusan.
7. APO07 (Mengelola sumber daya manusia), domain ini merupakan suatu proses perencanaan,evaluasi dan pengembangan SDM supaya optimal, dengan tujuan tercapainya SDM yang optimal sehingga memenuhi tujuan perusahaan.
8. APO08 (Hubungan terkelola), menciptakan hubungan yang formal dan transparansi saling percaya antara pemangku kepentingan bisnis, dengan tujuan untuk meningkatkan kepercayaan diri, rasa percaya dan penggunaan sumber daya yang efektif.

9. APO09 (Perjanjian layanan terkelola), menyelaraskan terkait produk dan layanan untuk mendukung IT dengan kebutuhan yang diharapkan perusahaan, dengan tujuan untuk memastikan bahwa suatu produk,layanan dapat memenuhi kebutuhan yang akan datang.
10. APO10 (Vendor terkelola), mengelola produk atau layanan IT yang telah disediakan vendor, dan diharapkan dapat memenuhi kebutuhan perusahaan, dengan tujuan mengoptimalkan kapabilitas IT yang tersedia.
11. APO11 (Kualitas terkelola), menerapkan dan mengkomunikasikan terkait semua proses perusahaan, dengan tujuan untuk mengirim solusi dan layanan teknologi yang konsisten untuk memenuhi kualitas perusahaan.
12. APO12 (Risiko terkelola), bertujuan untuk mengelola risiko di suatu perusahaan dan menurut ISACA 2019 bahwa domain APO12 merupakan metode untuk menggabungkan manajemen risiko teknologi informasi dengan manajemen risiko perusahaan secara keseluruhan (ERM) dan menyeimbangkan biaya dan keuntungan manajemen risiko perusahaan (Anugrah et al., 2022). Dan APO12 ini berperan sebagai panduan dalam proses manajemen risiko yang berkesinambungan, dengan fokus pada identifikasi, penilaian, dan mitigasi risiko terkait teknologi informasi. Sehingga risiko tersebut tidak dapat melampaui batas toleransi yang telah ditetapkan (Mario, Andre, dan Andeka, 2021).
13. APO13 (Keamanan terkelola), melakukan pemantauan, pengoprasian terkait sistem manajemen keamanan informasi, dengan tujuan mempertahankan dampak dan terjadinya insiden keamanan informasi.

2.1.7 Bulid, Acquire and Implement (BAI)

BAI ini merupakan domain yang berkaitan untuk proses pembangunan, akuisi dan implementasi solusi TI, yang berdasarkan kebutuhan perusahaan. Sebagian besar domain ini bertujuan untuk mengelola dan memberikan solusi TI dan memastikan solusi yang dihasilkan dapat sesuai dengan kebutuhan perusahaan dan dapat diterapkan di lingkungan perusahaan tersebut secara efektif. BAI ini memiliki beberapa subdomain atau aktivitas dalam proses yang dapat diterapkan, aktivitas tersebut sebagai berikut:

1. BAI01 (Manajemen program), melakukan pengelolaan terkait semua program dengan pendekatan manajemen program standar dengan tujuan untuk mewujudkan nilai-nilai bisnis yang diharapkan dan memastikan terkait kontribusi program pada portofolio investasi.
2. BAI02 (Definisi persyaratan dikelola), mengidentifikasi solusi dan persyaratan sebelum akuisi dan memastikannya supaya sesuai dengan persyaratan perusahaan. Tujuan domain ini untuk menciptakan solusi yang dapat meminimalkan risiko perusahaan.
3. BAI03 (Identifikasi dan membangun solusi terkelola), mengelola terkait layanan yang teridentifikasi dengan tujuan untuk memastikan pengiriman layanan digital yang cepat, sehingga dapat menghemat waktu dan biaya.
4. BAI04 (Ketersediaan dan kapasitas terkelola), memastikan kebutuhan masa depan dengan saat ini untuk ketersediaan, kinerja dan menyediakan

layanan yang hemat, dengan tujuan menjaga ketersediaan layanan, sumber daya efisien, dan mengoptimalkan kinerja.

5. BAI05 (Perubahan organisasi terkelola), melakukan dan memaksimalkan terkait perubahan di perusahaan dengan berkelanjutan dan cepat dengan mengurangi risiko, dan tujuanya untuk mempersiapkan dan melakukan komitmen untuk perubahan bisnis.
6. BAI06 (Managed IT changes), mengelola semua perubahan dan terkendali yang berkaitan dengan proses bisnis, sistem dan infrastruktur, dengan tujuan untuk mengaktifkan pengiriman perubahan yang cepat dan membantu untuk mengurangi risiko negatif pada lingkungan yang berubah.
7. BAI07 (Penerimaan dan transisi perubahan TI terkelola), membuat solusi baru yang operasional dengan tujuan sebagai solusi yang aman dan sejalan dengan keinginan yang sudah disepakati.
8. BAI08 (Managed knowledge), Mengelola dan menjaga ketersediaan informasi manajemen yang relevan, dengan tujuan untuk memberikan pemahaman dan informasi kepada staf yang berguna untuk pengambilan keputusan yang tepat.
9. BAI09 (Aset dikelola), mengelola asset untuk mendukung kemampuan layanan yang bisa diandalkan dan selalu tersedia, sehingga semua asset TI dapat mendapatkan nilai yang optimal dari penggunaannya.
10. BAI10 (Konfigurasi terkelola), mempertahankan hubungan antara sumber daya utama dengan kemampuan yang diperlukan, dengan tujuan untuk

memberikan informasi yang memadai terkait asset layanan sehingga layanan tersebut dapat terkelola dengan efektif.

11. BAI11 (Proyek terkelola), mengelola semua proyek di perusahaan dan memastikan sejalan dengan strategi perusahaan, dengan tujuan untuk merealisasikan hasil proyek dan hasilnya dapat maksimal dalam program dan investasi yang sudah ditentukan.

2.1.8 Deliver, Service and Support (DSS)

Menurut ISACA 2019, DSS ini merupakan domain yang berfokus untuk proses pengiriman, layanan, dan dukungan untuk sistem informasi dan teknologi informasi. Tujuan utama dari domain DSS ini adalah untuk menganalisis dan memastikan bahwa layanan Teknologi Informasi yang disediakan dapat memenuhi kebutuhan organisasi dan Teknologi Informasi dapat mendukung operasi bisnis. DSS ini memiliki beberapa domain, yaitu sebagai berikut:

1. DSS01 (Operasi terkelola), melaksanakan kegiatan operasional untuk memberikan layanan IT, dengan tujuan menyampaikan hasil dan operasional IT sesuai dengan proses yang telah direncanakan.
2. DSS02 (Permintaan dan insiden layanan terkelola), mengelola semua insiden dengan efektif dan tepat waktu, tujuannya untuk meminimalkan gangguan secara cepat, dan menilai dampak perubahan pada insiden layanan sesuai dengan permintaan pengguna.
3. DSS03 (Masalah terkelola), mengelola terkait masalah sampai ke akar penyebabnya dengan cepat, untuk mencegah masalah tersebut terulang kembali, dan meningkatkan kepuasaan pelanggan.

4. DSS04 (Kontinuitas terkelola), menerapkan rencana bagi organisasi TI untuk merespons suatu masalah dengan cepat, sehingga dapat beradaptasi dengan cepat.
5. DSS05 (Keamanan terkelola), mengelola sistem keamanan informasi dengan mempertahankan risiko keamanan informasi yang bisa diterima perusahaan, dan meminimalkan dampak dari insiden keamanan. DSS05 dikenal sebagai manajemen layanan keamanan yang mencakup berbagai aktivitas yang berkaitan dengan pengelolaan keamanan, tujuan subdomain ini untuk menganalisis dan memastikan bahwa semua keamanan informasi teknologi berjalan dengan baik. Aktivitas dalam subdomain ini melibatkan implementasi, pemantauan, dan peningkatan control yang berguna untuk melindungi data dan sistem TI dari potensi ancaman (D.V.Gusman et al., 2021).

2.1.9 Monitor, Evaluate, and Asess (MEA)

MEA ini merupakan domain yang dilakukan untuk memastikan bahwa semua proses IT sesuai dengan apa yang telah ditentukan oleh perusahaan. Dengan domain ini berfokus untuk melakukan pemantauan dan memastikan bahwa teknologi informasi dapat mendukung sasaran bisnis atau perusahaan secara optimal. Domain ini memiliki beberapa subdomain atau aktivitasnya yaitu, sebagai berikut:

1. MEA01 (Pemantauan kinerja dan kesesuaian terkelola), mengumpulkan dan menyelaraskan terkait matrik perusahaan dengan tujuan untuk

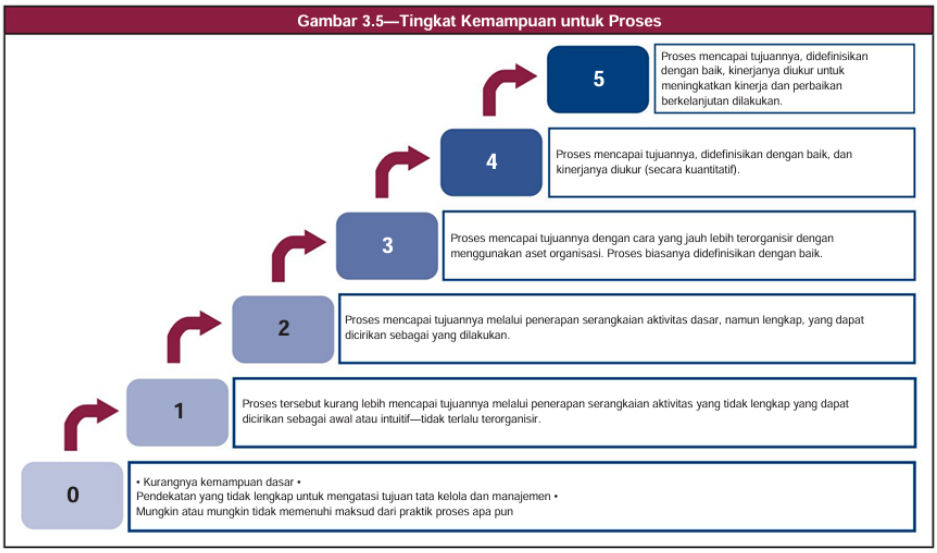
memberikan transparansi kinerja supaya sesuai dengan pencapaian atau tujuan yang diharapkan.

2. MEA02 (Sistem pengendalian internal terkelola), mengelola dan memantau lingkungan pengendalian, dengan tujuan memperoleh transparansi dari berbagai pemangku kepentingan, dan dapat membantu dalam pencapaian tujuan perusahaan yang memadai terkait risiko residual.
3. MEA03 (Kepatuhan terkelola dengan persyaratan eksternal), Memastikan bahwa proses TI dan bisnis harus didukung sesuai dengan undang-undang peraturan, dan memastikan mendapatkan jaminan terkait persyaratan yang sudah diidentifikasi dapat memenuhi semua persyaratan eksternal yang berlaku.
4. MEA04 (Jaminan terkelola), Melakukan perencanaan dan memastikan jaminan untuk mematuhi persyaratan internal yang sesuai dengan peraturan dan tujuan strategis. Diharapkan dapat membantu dalam merancang penjaminan yang efektif di dalam organisasi sehingga penjaminan dapat diterima dengan baik.

2.1.10 LEVEL CAPABILITY

Penilaian tingkat kemampuan, atau dikenal sebagai "*Capability Level*", adalah bagian dari COBIT 2019, dan berfungsi untuk memberikan pedoman yang jelas tentang kriteria yang harus dipenuhi untuk mencapai level tertentu. Dapat dianggap telah mencapai tingkat kemampuan tertentu jika setiap proses atau semua aktivitas berhasil dilakukan pada tingkat tertentu. Proses penilaian ini didasarkan

pada *Integration of Capability Maturity* (CMI), yang memiliki rating dari 0 hingga 5 dan menunjukkan seberapa baik proses atau aktivitas tersebut telah dilakukan.



Gambar 2.3 Tingkat Kemampuan proses (ISACA 2019)

Berdasarkan gambar proses tingkat kemampuan tersebut dijelaskan dan diberikan keterangan pada setiap levelnya:

1. Level 0, adalah proses yang mencapai tujuan dengan cara yang sangat terbatas, dengan aktivitas yang belum lengkap.
2. Level 1, adalah proses awal yang mulai mencapai tujuan, tetapi serangkaian aktivitas belum lengkap.
3. Level 2, adalah proses yang sudah mencapai tujuan dan diterapkan atau dikelola dengan lebih terorganisir, menggunakan aset yang ada di dalam organisasi.
4. Level 3, proses mencapai tujuan dengan baik dan didefinisikan dengan jelas.

5. Level 4, proses terdefinisi dengan baik dan kinerjanya diukur secara kuantitatif untuk meningkatkan kinerja.
6. Level 5, proses sudah mencapai tujuannya dengan cara yang efisien dan terus melakukan perbaikan berkelanjutan.

2.1.11 Metode ISO 31000

ISO 31000 merupakan panduan dalam mengelola risiko di suatu organisasi. ISO 31000 adalah panduan internasional untuk menerapkan manajemen risiko, yang terdiri dari tiga elemen utama, yaitu prinsip, kerangka kerja, dan proses. Prinsip manajemen risiko membentuk dasar praktik dan filosofi manajemen dengan tujuan meningkatkan kemungkinan pencapaian tujuan organisasi dan mengurangi dampak risiko yang mungkin terjadi. Kerangka kerja manajemen risiko melibatkan penerapan sistem manajemen risiko di seluruh organisasi secara sistematis dan terstruktur, dan prosesnya terdiri dari tindakan pengelolaan risiko yang berurutan dan saling terikat (Bima Mahardika et al., n.d.).

ISO 31000 dibuat oleh International Organization for Standardization (ISO) sebagai pedoman untuk mitigasi risiko. Tujuannya adalah menciptakan standar yang dapat diadopsi oleh berbagai jenis bisnis untuk mengatasi risiko yang muncul dalam proses bisnis mereka. Dalam edisi 2009, ISO 31000 mendefinisikan ketiga elemen manajemen risiko sebagai serangkaian elemen berturut-turut. Artinya, proses manajemen risiko diarahkan secara berurutan, mulai dari mengidentifikasi risiko, kemudian menilai risiko tersebut, dan pengelolanya. Tetapi, dalam edisi 2018, ISO 31000 menghadirkan perubahan dengan mendefinisikan keterbukaan

dan keterkaitan di antara ketiga elemen tersebut. Elemen-elemen tersebut tidak hanya dijalankan secara berurutan, melainkan juga saling terkait dan terbuka satu sama lain. Ini menunjukkan bahwa proses manajemen risiko tidak harus diartikan sebagai langkah-langkah terpisah, tetapi sebagai suatu kesatuan yang saling mempengaruhi dan berinteraksi.

Dengan adanya perubahan ini, ISO 31000 versi 2018 menggambarkan bahwa manajemen risiko sebagai proses yang lebih kompleks yang terdiri dari banyak elemen yang saling terhubung, dan pendekatan yang efektif untuk mengatasi risiko organisasi dapat dibuat dengan saling terhubung atau bekerja sama (Patrick et al., 2022).

Menurut panduan Buku ISO 31000, Metode ini memiliki beberapa prinsip yang bertujuan untuk meningkatkan kinerja, mendorong inovasi, dan pencapaian tujuan. Prinsip ini memberikan panduan tentang karakteristik manajemen risiko yang efisien dan efektif, serta menjelaskan maksud dan tujuan manajemen risiko. Prinsip-prinsip ini juga harus dipertimbangkan dalam proses manajemen risiko, dan diharapkan dapat membantu organisasi dalam mengelola kemungkinan risiko atau dampak ketidakpastian terhadap tujuan yang ini dicapai. Prinsip-prinsip ISO 31000 sebagai berikut:

1. Terintegrasi

   Pada proses manajemen risiko harus terintegrasi, karena pengelolaan risiko tidak dilakukan secara terpisah tapi dilakukan penggabungan dan menjadi bagian yang tidak terpisahkan.

2. Terstruktur dan Komprehensi

Manajemen risiko harus dilakukan dengan cara terorganisir dan mencakup semua aspek yang relevan.

3. Disesuaikan

   Kerangka kerja dan proses manajemen risiko harus dirancang agar sesuai dengan kondisi khusus organisasi.

4. Inklusif

   Melibatkan semua pihak yang berkepentingan secara tepat waktu dalam proses manajemen risiko. Dengan adanya keterlibatan memungkinkan pandangan, pengetahuan, dan persepsi mereka dipertimbangkan dan membantu mempermudah proses manajemen risiko.

5. Dinamis

   Manajemen risiko harus mampu mengantisipasi, mendeteksi, dan merespons perubahan yang terjadi di organisasi. Karena, risiko bisa muncul atau berubah seiring waktu.

6. Informasi Terbaik yang Tersedia

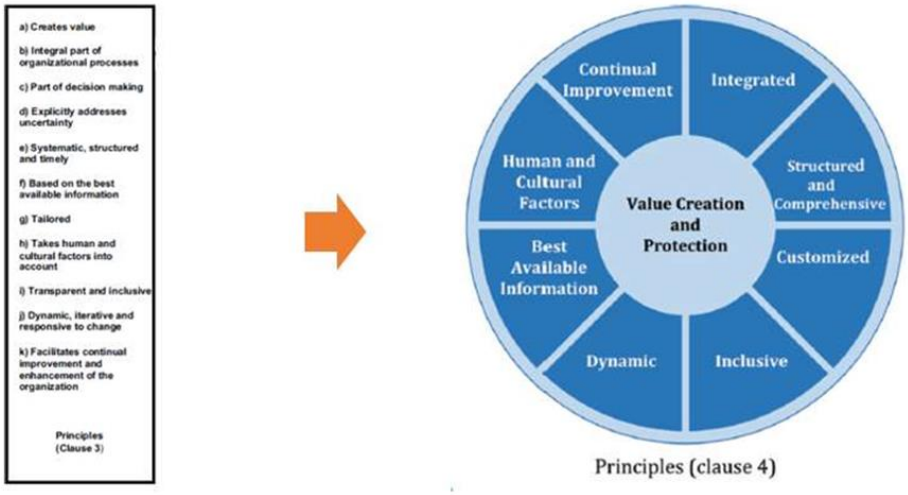
   Manajemen risiko harus didasarkan pada informasi yang relevan dan terkini. Informasi harus jelas, tepat waktu, dan tersedia bagi semua pemangku kepentingan yang membutuhkan.

7. Faktor Manusia dan Budaya

   Dalam proses manajemen risiko, semua aspek mulai dari perencanaan hingga pelaksanaan dapat dipengaruhi oleh cara orang-orang berpikir dan bertindak di dalam organisasi. Sehingga perilaku manusia dan budaya dapat memiliki dampak besar bagi proses manajemen risiko.

8. Perbaikan Berkelanjutan

   Manajemen risiko harus selalu diperbarui dan ditingkatkan berdasarkan pembelajaran dan pengalaman sebelumnya.



Gambar 2.4 Perbedaan ISO 31000: 2009 dan ISO 31000:2018

(Utamajaya et al., 2021)

Berdasarkan Gambar 2.1 dapat dilihat perbedaan atau perubahan yang terjadi dari ISO 31000 versi 2009 ke ISO 31000 versi 2018. Pada ISO 2009 dapat dilihat bahwa prinsip manajemen risiko terdapat 11 prinsip, dan pada ISO 2018 berubah menjadi 8 prinsip saja. Jadi pada ISO versi 2018 ini antar prinsip saling terikat atau terhubung (Utamajaya et al., 2021).

ISO 31000 ini mempunyai kerangka kerja yang bertujuan untuk memberikan landasan yang mencakup pedoman manajemen risiko, proposal, kewajiban dan komitmen. Kerangka kerja ini mencakup rencana, hubungan, tanggung jawab, sumber daya, proses, dan berbagai aktivitas. Dengan adanya kerangka kerja ini dapat membantu untuk proses integrasi manajemen risiko atau pengelolaan risiko.

Gambar 2.5 Kerangka Kerja ISO 31000

Berdasarkan Gambar diatas, kerangka kerja ISO 31000 meliputi mengintegrasikan, merancang, menerapkan, evaluasi, dan meningkatkan. Kerangka kerja pada gambar. Proses-proses kerangka kerja ISO 31000 yaitu, sebagai berikut:

1. *Leadership and Commitment*

   Top management atau badan pengawas harus memastikan bahwa manajemen risiko ini terintegrasi dalam setiap aspek organisasi, dengan melakukan penyesuaian dan implementasi kerangka kerja yang ada, jadi top management bertanggung jawab atas pengelolaan risiko, dan pengawas bertugas mengawasi pelaksanaan proses analisis risiko.

2. *Integration*

   Proses integrasi dalam manajemen risiko ini bersifat dinamis dan harus disesuaikan dengan kebutuhan atau keadaan suatu organisasi. Proses integrasi ini meliputi proses pemahaman struktur atau konteks organisasi,

tata kelola, strategi dan operasi di organisasi. Proses integrasi ini bertujuan untuk menyelaraskan antara manajemen risiko dengan tujuan organisasi.

3. *Design*

   Pada proses ini merupakan proses untuk merancang kerangka kerja manajemen risiko, jadi sebelum melakukan penerapan atau analisis manajemen risiko, harus melakukan pemahaman konteks organisasi (Faktor sosial,budaya,politik,dan ekonomi dari segi internal). Dan untuk sumber daya juga harus diperhatikan dalam proses manajemen risiko, seperti keterampilan dan proses yang diperlukan.

4. *Implementation*

   Dalam penerapan kerangka kerja manajemen risiko, perlu merencanakan sumber daya dan waktu yang sesuai, menentukan pengambilan keputusan yang jelas, memastikan pemahaman yang baik dalam mengelola risiko. Dan juga perlu adanya keterlibatan pemangku kepentingan untuk membantu dalam proses dan pengambilan keputusan.

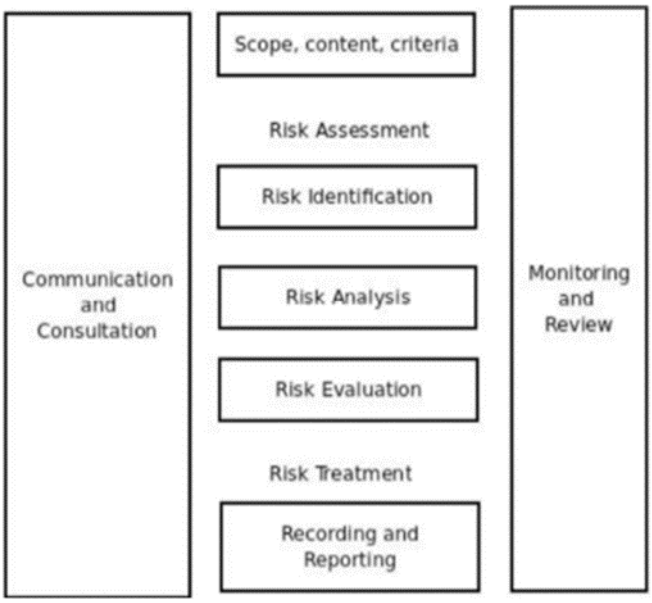
5. *Evaluation*

   Dalam proses penilain efektivitas kerangka kerja, maka organisasi perlu secara rutin kedepannya untuk mengukur kinerja tersebut, dan kerangka kerja manajemen risiko diharapkan tetap memadai dan mendukung pencapain bisnis.

6. *Improvement*

Dalam proses kedepannya organisasi harus melakukan pemantauan secara terus menerus, organisasi juga perlu melakukan identifikasi terkait kekurangan atau peluang untuk mengatasi masalah (perbaikan) yang mungkin terjadi.

Saat ini pada proses manajemen risiko menggunakan ISO 31000 terdapat enam kegiatan yang dapat dilihat pada Gambar 2.6



s

Gambar 2.6 Proses Manajemen Risiko ISO 31000

Berdasarkan Gambar 2.6 ini menjelaskan terkait proses-proses yang dilakukan saat manajemen risiko menggunakan ISO 31000 dengan berbagai tahapan sebagai berikut:

1. Komunikasi dan konsultasi yang bertujuan untuk membantu membersihkan dasar dalam pengambilan keputusan dan pertimbangan dalam mengambil keputusan terkait tindakan tertentu bagi pihak yang mempunyai risiko tersebut.

2. Penentuan Konteks (*Scope, Context, Criteria*) bertujuan untuk menyelaraskan proses bisnis pada risikonya dalam ruang lingkup yang sudah ditentukan. Hal ini dilakukan agar penilaian risiko dapat berjalan efektif sesuai dengan konteks dan kriteria yang sudah ditetapkan, serta untuk mengambil tindakan yang tepat atas ancaman yang ada.
3. Penilaian Risiko (*Risk assessment*) adalah proses identifikasi, analisis, dan evaluasi risiko.
4. Perlakuan Risiko (*Risk treatment*) bertujuan untuk memilih Solusi yang tepat guna mengatasi risiko yang ada.
5. Pemantauan dan Peninjauan (*Monitoring dan Review*) bertujuan untuk meninjau dan memastikan peningkatan kualitas yang efektif dari proses bisnis, pelaksanaan, hingga hasilnya.

2.1.12 State of The Art

Pada analisis manajemen risiko teknologi informasi menggunakan ISO 31000 dan COBIT 5, tabel 2.1 menggambarkan perbandingan dengan penelitian sebelumnya yang relevan dengan fokus penelitian. Ditemukan sejumlah perbedaan dan kesamaan antara hasil penelitian ini dan penelitian-penelitian sebelumnya, yang tercermin dalam penerapan framework yang digunakan.

Tabel 2.1 State of The Art

No	Penulis dan Tahun	Judul	Permasalahan	Hasil dan Simpulan
1	Mario Andre Giovanno Wattimena, dan Andeka Rocky Tanaamah, 2021.	Analisis Manajemen Risiko Teknologi Informasi	Sejauh mana menilai risiko yang akan terjadi dan memanfaatkan COBIT 5.	Hasil dalam mengelola risiko perpustakaan bagian 5 domain APO12 berada di level 1 kriteria

		Menggunakan COBIT 5 Pada TSI/Teknologi dan Sistem Informasi Perpustakaan UKSW		proses tercapai. Dan terdapat 4 rekomendasi mencapai level 2 untuk proses capability level domain APO12.
2	Khrisna Aprianto, Endroyono, dan Supeno Mardi Susiki Nugroho (2021)	Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan	Terdapat beberapa risiko dalam proses pelaksanaan kerja, karena dilakukan secara elektronik.	Hasil terdapat 21 risiko yang sesuai dengan pencapaian sasaran organisasi, Risiko pengendalian sebanyak 15.
3	Prilly Peshaulia Thenu, Agustinus Fritz Wijaya, Christ Rudianto, 2020	Analisis Manajemen Risiko Teknologi Informasi menggunakan COBIT 5 (Studi kasus: PT global Infotech)	Dengan menggunakan TI maka risiko akan muncul dan dapat mengakibatkan kerugian.	Hasilnya Terdapat 4 risiko kecil, seperti risiko kotoran , dari alam, server down. Hasil pengukuran capability APO12 berada di level 1, kurang pengontrolan risiko TI, terdapat dua rekomendasi untuk perusahaan dalam mengelola risiko.
4	Dio Ferbilian tanjung, Aulia Oktaviana, dan Aris Puji Widodo, 2021.	Analisis Manajemen Risiko Startup pada Masa Pandemi Covid-19 menggunakan COBIT 2019	Proses bisnis era pandemi berubah menjadi work form home, perubahan struktur organisasi, proses distribusi informasi perlu	Hasilnya perusahaan dapat melakukan perubahan sesuai kondisinya dengan menerapkan manajemen risiko secara baik, dan sesuai dengan panduan COBIT 2019.

			dilakukan perubahan.	
5	Ayunda Della Ariesta, Suprapto, dan Andi Reza Perdanakusuma, 2022.	Evaluasi Tata kelola dan Manajemen Risiko Teknologi Informasi pada PT.MyECO teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12	Perusahaan tersebut telah menerapkan TI dengan membuat Aplikasi, sehingga akan menimbulkan risiko yang beragam.	Hasil Tingkat kemampuan capability level pada proses EDM03 pada level 1, APO12 pada level 1 kurang lebih telah mencapai tujuan.
6	Firza Zukhariadna Afriliandra, Suprapto, dan andi Reza perdanakusumah, 2023.	Evaluasi Tata Kelola Manajemen Risiko Teknologi Informasi pada PT XYZ menggunakan Kerangka Kerja COBIT 2019	Perusahaan menerapkan TI yang berupa situs web, namun dalam penerapannya biasanya terjadi *erorr* sehingga perlu optimasi performa sistem.	Hasilnya Tingkat kemampuan pada proses EDM03 pada level 1 dikategorikan sebagai awal intuitif, APO12 pada level 1 kurang lebih telah mencapai tujuan. Untuk risiko TI masih didokumentasikan secara insedental dan dikategorikan intuitif.
7	Muhammad Ilham Fachrezi, Ariya Dwika Cahyono, dan Penidas Fiodinggo Tanaem (2021)	Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000: 2018 Diskominfo Kota Salatiga	Aset TI memiliki peran penting tetapi terdapat potensi ancaman serangan terhadap teknologi tersebut	Hasil terdapat 2 kemungkinan risiko level rendah, 11 level medium, dan 4 kemungkinan level high. Sehingga harus ditingkatkan lebih baik lagi.

8	Aan Muslimin, Adi Sapto Raharjo, dan Sri Lestari, 2020	Manajemen Risiko teknologi Informasi terkait Pandemi COVID-19 pada SDN 1 Negara Batin menggunakan Framework COBIT 5 dan ISO/IEC 31000	Aktivitas dalam belajar di SDN tersebut mengalami kendala, dan beberapa administrasi Staff dan guru terhambat.	Hasilnya manajemen risiko TI dapat digunakan untuk mengelola risiko TI dan membantu berjalannya kegiatan. Diperoleh 24 risiko TI dengan kegiatan infrastruktur yang ada. Risiko level rendah 9, level sedang 10, dan level tinggi 5.
9	Miftakhun, 2020	Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo menggunakan ISO 31000	Dalam pekerjaannya menggunakan website tetapi terdapat permasalahan yang sering muncul, seperti sistem error dan susah login sebagai akses website.	Hasilnya terdapat 24 kemungkinan risiko, dengan level tinggi 3, level medium 10, dan level rendah 11.
10	Finandy Ari Hardianto, dan Yogantara Setya Dharmawan, 2021.	Manajemen Risiko TI ISO 31000 dengan COBIT 5 dan FMEA (PT.XYZ)	Belum dilakukan penerapan pengelolaan risiko pada PT tersebut.	Hasilnya terdapat keterkaitan antara framework pengelolaan risiko yang bisa digunakan untuk pengelolaan risiko dan sudah sesuai dengan kebutuhan yang ada. Terdapat 19 risiko, dengan level tinggi 4, level medium 10, dan level rendah 9. Dan juga dari 19 risiko terdapat terhadap respond

				penanganan mitigasi respond. 16

2.1.13 Matriks Penelitian

Matriks penelitian pada tabel 2.2 merupakan matriks untuk perbanding antara penelitian yang saat ini dengan penelitian sebelumnya yang saling berhubungan. Dan terdapat beberapa perbedaan dan persamaan dengan penelitian sebelumnya yang bisa dilihat dari penggunaan framework, objek dan tujuan.

Tabel 2.2 Matriks Penelitian

No	Judul	Nama Penulis dan Tahun	Tujuan	Objek	Framework		
			Analisis	Teknologi	COBIT 5	COBIT 2019	ISO 31000
1	Manajemen Risiko TI ISO 31000 dengan COBIT 5 dan FMEA (PT.XYZ)	Finandy Ari Hardianto, dan Yogantara Setya Dharmawan, 2021.	✓	✓	✓	-	✓
2	Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 Pada TSI/Teknologi dan Sistem Informasi Perpustakaan UKSW	Mario Andre Giovanno Wattimena, dan Andeka Rocky Tanaamah, 2021.	✓	✓	✓	-	-
3	Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan	Khrisna Aprianto, Endroyono, dan Supeno Mardi Susiki Nugroho (2021)	✓	✓	✓	-	✓
4	Analisis Manajemen Risiko Teknologi Informasi menggunakan COBIT 5 (Studi	Prilly Peshaulia Thenu, Agustinus Fritz Wijaya, Christ Rudianto, 2020	✓	✓	✓	-	-

	kasus: PT global Infotech)						
5	Analisis Manajemen Risiko Startup pada Masa Pandemi Covid-19 menggunakan COBIT 2019	Dio Ferbilian tanjung, Aulia Oktaviana, dan Aris Puji Widodo, 2021.	✓	-	-	✓	-
6	Evaluasi Tata kelola dan Manajemen Risiko Teknologi Informasi pada PT.MyECO teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12	Ayunda Della Ariesta, Suprapto, dan Andi Reza Perdanakusuma, 2022.	✓	✓	-	✓	-
7	Evaluasi Tata Kelola Manajemen Risiko Teknologi Informasi pada PT XYZ menggunakan Kerangka Kerja COBIT 2019	Firza Zukhariadna Afriliandra, Suprapto, dan andi Reza perdanakusumah, 2023.	✓	✓	-	✓	-
8	Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000: 2018 Diskominfo Kota Salatiga	Muhammad Ilham Fachrezi, Ariya Dwika Cahyono, dan Penidas Fiodinggo Tanaem (2021)	✓	✓	-	-	✓
9	Manajemen Risiko teknologi Informasi terkait Pandemi COVID-	Aan Muslimin, Adi Sapto Raharjo, dan Sri Lestari, 2020	✓	✓	✓	-	✓

	19 pada SDN 1 Negara Batin menggunakan Framework COBIT 5 dan ISO/IEC 31000						
10	Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo menggunakan ISO 31000	Miftakhun, 2020	✓	✓	-	-	✓
11	Penerapan framework ISO 31000 dan COBIT 2019 untuk Analisis Manajemen Risiko TI (Studi Kasus:BPBD Kab.Tasikmalaya) , 2024	Penelitian Ai Wulan Windiawati, 2024	✓	✓	-	✓	✓

Berdasarkan Tabel 2.2 matriks penelitian, dijelaskan perbedaan antara penelitian sebelumnya dengan penelitian yang akan dilakukan saat ini. Penelitian saat ini, dalam latar belakang permasalahan, memiliki perbedaan dengan penelitian sebelumnya karena latar belakang saat ini diambil sesuai dengan permasalahan yang terjadi pada objek penelitian tersebut. Pada objek tempat penelitian yang dilakukan juga berbeda dengan penelitian sebelumnya. Mungkin terdapat beberapa kesamaan antara penelitian sebelumnya dengan penelitian saat ini, yaitu mulai dari topik terkait manajemen risiko dan metode yang digunakan. Tetapi pada penelitian saat ini, untuk proses analisis manajemen risikonya menggunakan COBIT 2019 versi terbaru saat ini, dan menggunakan subdomain APO12 yang digabungkan

dengan ISO 31000. Sedangkan pada penelitian sebelumnya masih menggunakan COBIT 5, dan cara penggabungan kedua metode tersebut berbeda.

2.1.14 Relevansi Penelitian

Pada bagian relevansi penelitian ini akan membandingkan dari penelitian sebelumnya dengan penelitian sekarang yang memiliki keterkaitan terkait penelitian yang dilakukan. Relevansi penelitian ini dapat dilihat lebih jelas pada Tabel 2.3.

Tabel 2.3 Relevansi Penelitian

Peneliti	Judul	Objek	Masalah	Metode
Penelitian Ai Wulan Windiawati, 2024	Penerapan Framework ISO 31000 dan COBIT 2019 untuk analisis manajemen risiko teknologi informasi (Studi kasus: BPBD Kab.Tasikmalaya)	Analisis Teknologi Informasi berbasis manajemen risiko teknologi informasi di BPBD Kab.Tasikmalaya	Belum pernah dilakukan analisis terkait manajemen risiko teknologi informasi, dan gangguan API.	ISO 31000 dan COBIT 2019
Ayunda Della Ariesta, Suprapto, dan Andi Reza Perdanakusuma, 2022	Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12	PT.MyECO Nusantara	Mempunyai aplikasi untuk mengontrol perangkat listrik, tetapi implementasi TI tidak sesuai dan dapat memungkinkan adanya risiko	COBIT 2019

Berdasarkan Tabel 2.3 terdapat perbedaan dengan penelitian sebelumnya dalam Objek penelitian yang dilakukan berbeda, untuk penelitian sebelumnya

dilakukan di PT.MyECO sedangkan penelitian saat ini dilakukan di BPBD Kab. Tasikmalaya, dan dengan permasalahan latar belakang yang berbeda. Untuk persamaan terkait topik yang diangkat membahas topik yang sama yaitu tentang "Manajemen Risiko Teknologi Informasi", dan Metode yang digunakan. Tetapi pada penelitian sebelumnya menggunakan COBIT 2019 dengan subdomain APO12 dan EDM05, sedangkan penelitian saat ini menggabungkan ISO 31000 dengan COBIT versi 2019 dengan subdomain APO12 dan DSS05, dan dalam proses analisis yang dilakukan memiliki proses yang berbeda.

Penelitian sebelumnya telah menerapkan sistem teknologi informasi dan memiliki aplikasi yang digunakan, tetapi setiap implementasi teknologi tidak selalu sesuai dengan kondisi yang diharapkan, sehingga dari penerapan teknologi informasi yang tidak sesuai akan muncul risiko pada perusahaan tersebut. Untuk mengatasi permasalahan yang ada maka dilakukan evaluasi tata kelola dan manajemen risiko dengan menggunakan COBIT 2019. Tetapi pada penelitian sebelumnya hanya sampai pada pemberian rekomendasi berdasarkan subdomain EDM03 dan APO12 saja, dan tidak ada daftar risiko yang mungkin terjadi atau pemetaan kategori risikonya, sehingga saran dari penelitian tersebut dapat mencoba menggunakan metode lainnya seperti ISO, ITIL atau standar lain.

Jadi berdasarkan penelitian sebelumnya, penelitian saat ini mengembangkan dengan menggunakan ISO 31000 dan COBIT 2019 untuk menganalisis risiko teknologi informasi. Dengan menggunakan metode tersebut dapat mendapatkan penilaian keadaan sebenarnya dan dari keadaan yang sebenarnya terjadi akan mendapatkan hasil risiko-risiko yang mungkin terjadi dengan jelas.