BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam mendukung pengelolaan risiko aset TI di Balmon SFR Kelas I Semarang, berbagai penelitian terdahulu telah menerapkan kerangka kerja manajemen risiko seperti ISO/IEC 27005 dan tata kelola TI COBIT 2019 dengan pendekatan yang beragam. Tabel 2.1 merangkum inti dari studi-studi tersebut, mencakup fokus penelitian, metode yang digunakan, karakteristik organisasi atau sistem yang diteliti, serta hasil analisis terkait efektivitas pengelolaan dan strategi mitigasi risiko aset TI.

Tabel 2. 1 Kerangka Penelitian Terdahulu

No	Peneliti (Tahun)	Judul	Tujuan Penelitian	Framework	Temuan
1.	(Pratama & Nugraha, 2025)	Optimizing IT Risk Management through PDCA-Based Continuous Improvement Stages	Mengoptimalkan manajemen risiko TI pada organisasi nirlaba pemerintah.	ISO/IEC 27005:2022, NIST SP 800-30, NIST SP 800-39, ISO/IEC 27002, dan COBIT 2019	Ditemukan 41 aset dengan 7 prioritas risiko melalui ISO/IEC 27005:2022 dan COBIT 2019 sebagai panduan tata kelola per-tahap.

SEKOLAH PASCASARJANA

No	Peneliti (Tahun)	Judul	Tujuan Penelitian	Framework	Temuan
2.	(Mahfud dkk., 2024)	Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency)	Merancang manajemen risiko keamanan informasi di instansi pemerintah daerah.	ISO/IEC 27005:2022, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5	Ditemukan 102 skenario risiko dan 19 usulan kontrol keamanan.
3.	(Budiman dkk., 2024)	The Design of Information Technology Risk Management of The Secretariat of The Cabinet of The Republic of Indonesia	Merancang manajemen risiko TI di lingkungan Sekretariat Kabinet RI.	ISO/IEC 27005:2022, ISO 31000:2018, serta ISO/IEC 27002:2022	Ditemukan 340 skenario risiko (93 dimitigasi) dan 57 rekomendasi kontrol.

SEKOLAH PASCASARJANA

No	Peneliti (Tahun)	Judul	Tujuan Penelitian	Framework	Temuan
4.	(Astini dkk., 2025)	Information Technology Risk Analysis Using ISO 27005:2022 at Diskominfo Tabanan Regency	Melakukan identifikasi risiko pada aset teknologi informasi di Diskominfo Tabanan.	ISO/IEC 27005:2022	Ditemukan 28 aset TI dan 57 ancaman, menganalisis risiko dengan matriks likelihood dan impact, serta menghasilkan rekomendasi mitigasi untuk risiko level tinggi.
5.	(Harahap & Candiwan, 2025)	Risk Mitigation of Security Information Through Optimization Risk Assessment Based on ISO 27005:2022 & NIST SP 800-30 Revision 1 Standards at XYZ Company	Melakukan identifikasi risiko keamanan informasi pada perusahaan XYZ.	ISO/IEC 27005:2022, NIST SP 800-30 Rev.1, ISO/IEC 27002:2022	Ditemukan 9 skenario risiko dengan 9 strategi kontrol mitigasi.

SEKOLAH PASCASARJANA

No	Peneliti (Tahun)	Judul	Tujuan Penelitian	Framework	Temuan
6.	(Purnomo & Harwahyu, 2025)	Risk Management Analysis in Digital Bank XYZ Using the COBIT 2019 Framework	Melakukan evaluasi kematangan manajemen risiko di Bank Digital XYZ.	COBIT 2019	Tingkat kematangan tata kelola TI berada di antara level 3 dan 4.
7.	(Oktaviana dkk., 2024)	Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company	Melakukan evaluasi manajemen risiko TI pada proses bisnis *startup* pasca pandemi.	COBIT 2019	Tingkat kapabilitas berada di level 1. Diperlukan dokumentasi risiko, standardisasi SOP, dan evaluasi rutin.
8.	(Algiffary, Cholil, Tjahjanto, dkk., 2024)	Utilization of COBIT 2019 for an Advanced Strategic Evaluation of IT Risk Management in the Application of e-Government at Palembang City Governance	Melakukan evaluasi manajemen risiko TI *e-government* di Diskominfo Palembang.	COBIT 2019	Rata-rata kematangan berada di level 3.

SEKOLAH PASCASARJANA

No	Peneliti (Tahun)	Judul	Tujuan Penelitian	Framework	Temuan
9.	(Setyadi & Rahman, 2025)	Enhancing IT Governance Based on Risk and Security Analysis in a Private School: A COBIT 2019 Approach	Melakukan evaluasi tata kelola TI dengan fokus analisis risiko dan keamanan di institusi pendidikan.	COBIT 2019	Tingkat kapabilitas mencapai level 2.
10.	(Yasin dkk., 2020)	Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)	Merancang rekomendasi dan roadmap tata kelola keamanan informasi berbasis pemetaan ISO/IEC 27001:2013 ke COBIT 2019	ISO 27001:2013 dan COBIT 2019	Pemetaan 14 kategori kontrol ISO/IEC 27001:2013 ke COBIT 2019 menghasilkan 29 objek core model COBIT 2019 terpilih. Seluruh objek di bawah target Level 3; rekomendasi disusun dalam roadmap 2021–2025

SEKOLAH PASCASARJANA

Penelitian Pratama & Nugraha berfokus pada optimalisasi manajemen risiko TI melalui tahap perbaikan berkelanjutan berbasis siklus PDCA pada organisasi nirlaba pemerintah, dengan menggabungkan ISO/IEC 27005:2022, NIST SP 800-30, NIST SP 800-39, ISO/IEC 27002, dan COBIT 2019. Hasil penelitian menghasilkan kerangka kerja hybrid enam tahap yang diuji pada 41 aset dengan 7

aset prioritas dan divalidasi melalui expert judgment menggunakan Content Validity Index. Dalam penelitian ini, ISO/IEC 27005 berperan menjalankan proses penilaian risiko, sedangkan COBIT 2019 difungsikan sebagai panduan tata kelola pada tiap tahap kerangka tanpa pengukuran tingkat kapabilitas. Temuan tersebut memperlihatkan bahwa ISO 27005 dan COBIT 2019 dapat dipadukan dalam satu kerangka, meskipun keduanya berjalan paralel dan belum menjadikan temuan risiko sebagai dasar evaluasi kematangan tata kelola.

Penelitian Mahfud dkk. berfokus pada perancangan manajemen risiko keamanan informasi di instansi pemerintah daerah dengan menggunakan kombinasi ISO/IEC 27005:2022, ISO/IEC 27001:2022, dan NIST SP 800-53 Revisi 5. Hasil penelitian mengidentifikasi 102 skenario risiko beserta 19 usulan kontrol keamanan. Penelitian ini menunjukkan bahwa penggabungan ISO/IEC 27005 dengan NIST SP 800-53 mampu menghasilkan rancangan manajemen risiko yang terstruktur sekaligus dilengkapi katalog kontrol yang komprehensif. Temuan tersebut menegaskan peran ISO/IEC 27005 dalam menyediakan alur identifikasi dan penilaian risiko keamanan informasi pada konteks instansi pemerintah, meskipun cakupannya masih terbatas pada perancangan kontrol dan belum menjangkau evaluasi kapabilitas tata kelola TI.

Penelitian Budiman dkk. (2024) berfokus pada desain manajemen risiko teknologi informasi di Sekretariat Kabinet Republik Indonesia (Setkab) dengan menggunakan kombinasi ISO 31000:2018, ISO/IEC 27005:2022, dan ISO/IEC 27002:2022. Hasil penelitian menunjukkan adanya 340 skenario risiko, di mana 93 perlu dimitigasi dan 247 risiko dapat diterima. Penelitian ini menemukan bahwa kombinasi kerangka ISO memberikan rancangan manajemen risiko yang sistematis dan terukur. Temuan tersebut memperlihatkan bagaimana ISO 27005 dapat berperan penting dalam memberikan panduan teknis terkait proses manajemen risiko TI.

Penelitian oleh Astini dkk. (2025) menerapkan ISO/IEC 27005:2022 secara menyeluruh pada lingkungan TI Diskominfo Kabupaten Tabanan, mencakup tahap penetapan konteks, identifikasi aset, identifikasi ancaman, identifikasi kontrol yang telah diterapkan, identifikasi kerentanan, hingga evaluasi dan rekomendasi

SEKOLAH PASCASARJANA

mitigasi. Penelitian ini berhasil mengidentifikasi 28 aset TI dan 57 ancaman, dengan tingkat risiko yang dihitung melalui perkalian nilai likelihood dan impact pada skala 1 sampai 5. Hasil penilaian menunjukkan risiko level tinggi pada aset kritis seperti server, router, dan website layanan publik, sehingga rekomendasi mitigasi diarahkan pada penguatan infrastruktur dan kontrol teknis seperti redundansi UPS, enkripsi penyimpanan, dan otentikasi multi faktor. Penelitian ini menjadi rujukan relevan dalam penerapan ISO/IEC 27005:2022 pada konteks instansi pemerintah daerah yang memiliki karakteristik aset dan tata kelola layanan publik yang sebanding dengan objek penelitian ini.

Penelitian Harahap & Candiwan berfokus pada mitigasi risiko keamanan informasi melalui optimalisasi penilaian risiko pada Perusahaan XYZ dengan menggunakan ISO/IEC 27005:2022, NIST SP 800-30 Revisi 1, dan ISO/IEC 27002:2022. Hasil penelitian mengidentifikasi 9 skenario risiko yang disertai 9 strategi kontrol mitigasi. Penelitian ini menunjukkan bahwa penggabungan ISO/IEC 27005 dengan NIST SP 800-30 mampu memperkuat ketepatan proses identifikasi dan penilaian risiko keamanan informasi. Temuan tersebut menegaskan peran ISO/IEC 27005 dalam menyediakan alur penilaian risiko yang sistematis, sekaligus memperlihatkan bahwa fokus penelitian masih terbatas pada penilaian risiko dan penyusunan kontrol, tanpa menjangkau evaluasi tata kelola TI.

Penelitian Purnomo & Harwahyu (2025) mengungkapkan bahwa Bank Digital XYZ telah mencapai tingkat kematangan pada posisi antara level 3 (*Established Process*) dan level 4 (*Predictable Process*). Hal ini berarti organisasi telah memiliki prosedur standar yang terdokumentasi dengan baik dan dijalankan secara konsisten, meskipun masih diperlukan penguatan agar seluruh proses dapat diprediksi dan terukur secara optimal. Temuan ini menegaskan relevansi COBIT 2019 sebagai kerangka evaluasi yang mampu memetakan kelemahan sekaligus memberikan arah strategis dalam peningkatan tata kelola TI, khususnya pada institusi keuangan digital yang menuntut kepatuhan dan keamanan tinggi.

Penelitian Oktaviana dkk. berfokus pada evaluasi manajemen risiko TI pada proses bisnis perusahaan rintisan (startup) pascapandemi dengan menggunakan kerangka kerja COBIT 2019. Hasil penelitian menunjukkan bahwa tingkat

SEKOLAH PASCASARJANA

kapabilitas pengelolaan risiko berada pada Level 1, sehingga diperlukan dokumentasi risiko, standardisasi prosedur operasional, dan evaluasi rutin untuk meningkatkan kematangan tata kelola. Temuan ini menegaskan relevansi COBIT 2019 sebagai kerangka evaluasi kapabilitas yang mampu mengidentifikasi kelemahan pengelolaan risiko TI, khususnya pada organisasi yang masih berada pada tahap awal pembangunan tata kelola.

Penelitian Algiffary dkk. berfokus pada evaluasi strategis manajemen risiko TI dalam penerapan e-government di Dinas Komunikasi dan Informatika Kota Palembang dengan menggunakan kerangka kerja COBIT 2019. Hasil penelitian menunjukkan rata-rata tingkat kematangan tata kelola berada pada Level 3 (*Established Process*), yang berarti proses pengelolaan risiko telah terdokumentasi dan dijalankan secara konsisten. Temuan ini memperlihatkan kemampuan COBIT 2019 dalam mengukur tingkat kapabilitas tata kelola TI pada instansi pemerintah, sekaligus memberikan arah perbaikan untuk mempertahankan dan meningkatkan kematangan proses.

Penelitian Setyadi & Rahman berfokus pada peningkatan tata kelola TI dengan menekankan analisis risiko dan keamanan di institusi pendidikan swasta menggunakan kerangka kerja COBIT 2019. Hasil penelitian menunjukkan tingkat kapabilitas tata kelola mencapai Level 2 (*Managed Process*), yang berarti proses telah dikelola dan direncanakan meskipun belum sepenuhnya terstandarisasi. Temuan ini menegaskan peran COBIT 2019 sebagai kerangka evaluasi yang mampu memetakan kondisi tata kelola TI berbasis risiko dan keamanan, sekaligus memberikan dasar bagi penyusunan rekomendasi peningkatan kematangan proses.

SEKOLAH PASCASARJANA

Penelitian Yasin dkk. berfokus pada perancangan rekomendasi dan roadmap tata kelola keamanan informasi pada institusi kepolisian Ditreskrimsus Polda XYZ, dengan menggabungkan ISO/IEC 27001:2013 dan COBIT 2019 melalui metodologi Design Science Research Methodology (DSRM). Hasil penelitian menghasilkan 29 objek core model COBIT 2019 terpilih yang seluruhnya belum mencapai target kapabilitas Level 3, sehingga disusun rekomendasi struktur organisasi, pemenuhan sumber daya manusia, dan 29 kebijakan dalam bentuk roadmap 2021–2025. Dalam penelitian ini, ISO/IEC 27001 berperan sebagai

sumber cakupan kontrol yang seluruh kategori Annex A-nya dipetakan ke objek COBIT 2019, sedangkan COBIT 2019 difungsikan sebagai kerangka penilaian kapabilitas tata kelola. Temuan tersebut memperlihatkan bahwa integrasi standar keamanan informasi dengan COBIT 2019 dapat menghasilkan penilaian kapabilitas yang terukur, meskipun pemilihan objek masih digerakkan oleh kelengkapan cakupan kontrol standar dan belum melibatkan penilaian risiko berbasis ISO/IEC 27005 sebagai dasar penentuan objek yang dievaluasi.

Dengan demikian, telaah terhadap kesepuluh penelitian tersebut memperlihatkan tiga pola pendekatan. Penelitian yang menerapkan ISO/IEC 27005 umumnya berhenti pada penilaian risiko dan penyusunan kontrol tanpa menjangkau evaluasi kapabilitas tata kelola, penelitian yang menerapkan COBIT 2019 mengevaluasi kapabilitas tanpa didahului asesmen risiko pada tingkat aset, sedangkan penelitian yang mengintegrasikan standar keamanan informasi dengan COBIT 2019 menentukan proses evaluasinya berdasarkan kelengkapan cakupan kontrol standar, bukan berdasarkan kondisi risiko spesifik organisasi. Belum ada penelitian yang menjadikan hasil asesmen risiko sebagai dasar pemilihan proses COBIT 2019 yang dievaluasi tingkat kapabilitasnya. Celah inilah yang diisi oleh penelitian ini dengan mengintegrasikan ISO/IEC 27005:2022 dan COBIT 2019 secara berurutan: ISO/IEC 27005:2022 dipilih karena memberikan panduan terstruktur mengenai proses manajemen risiko mulai dari identifikasi hingga mitigasi, sedangkan COBIT 2019 dipilih karena mampu menilai kapabilitas tata kelola dan pengelolaan risiko TI serta memastikan keselarasan antara pengelolaan risiko dengan tujuan strategis organisasi. Dengan menjadikan keluaran asesmen risiko sebagai dasar penentuan proses yang dievaluasi, penelitian ini diharapkan menghasilkan evaluasi dan rancangan manajemen risiko aset TI yang lebih komprehensif, sistematis, dan aplikatif bagi instansi yang menjadi objek penelitian.

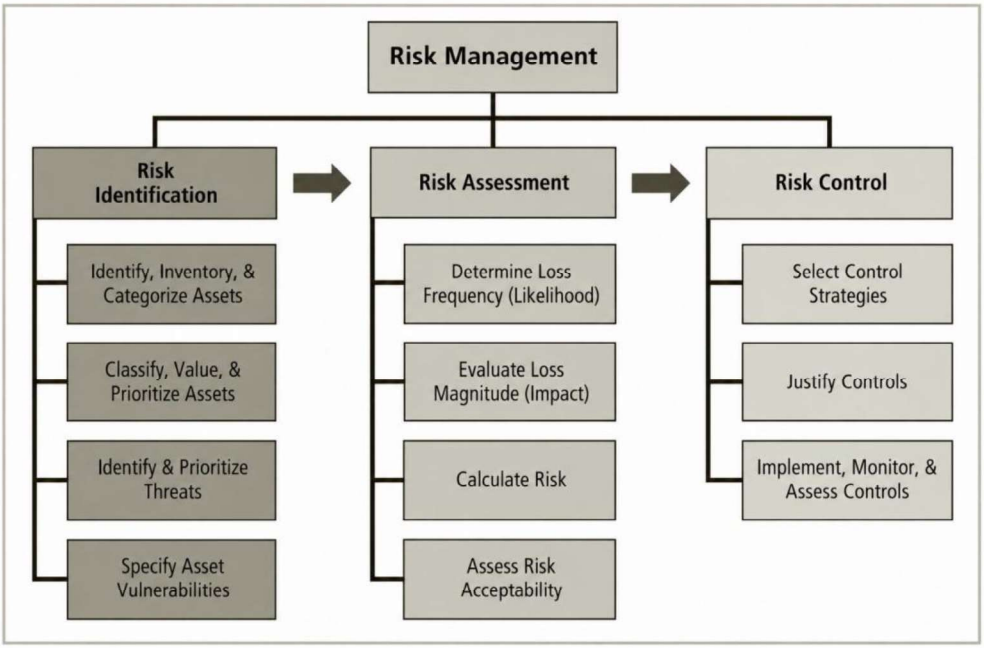
SEKOLAH PASCASARJANA

2.2 Dasar Teori

2.2.1 Manajemen Risiko

Risiko merupakan sebuah efek negatif dari kemungkinan yang terjadi pada sebuah kegiatan, yang juga mempertimbangkan tentang probabilitas dan efek dari

terjadinya kemungkinan tersebut. Manajemen risiko adalah proses sistematis yang mencakup identifikasi, penilaian, dan pengendalian risiko hingga pada tingkat yang dapat diterima, serta menjaga agar tingkat risiko tersebut tetap terkendali (Whitman & Mattord, 2018). Gambar 2.1 menjelaskan tiga proses utama manajemen risiko yaitu identifikasi risiko, penilaian risiko, dan pengendalian risiko.



Gambar 2. 1 *Risk Management*

Sumber: (Whitman & Mattord, 2018)

Manajemen risiko keamanan informasi merupakan langkah praktis dalam mengelola risiko keamanan informasi organisasi dan bertujuan untuk memberikan perlindungan terhadap informasi dan aset organisasi (ISO/IEC, 2022). Efektivitas manajemen risiko bergantung pada integrasinya dalam tata kelola organisasi. Prosesnya mencakup identifikasi, penilaian, dan evaluasi risiko untuk menentukan apakah risikonya masih dalam batas toleransi. Jika dapat diterima, manajemen risiko dianggap memadai, jika tidak, organisasi harus mengambil tindakan untuk menurunkannya.

SEMARANG
SEKOLAH PASCASARJANA

Salah satu fokus penting dalam manajemen risiko adalah aset informasi, yaitu segala bentuk informasi yang dimiliki organisasi dan memiliki nilai strategis (Laudon & Laudon, 2020). Aset informasi dapat tersimpan di berbagai media, sehingga perlindungannya penting karena kebocoran atau penyalahgunaan dapat mengganggu operasional dan daya saing organisasi. Aset informasi kini banyak dikelola melalui aset TI yang berperan penting dalam mendukung efektivitas proses bisnis, namun juga menimbulkan risiko seperti gangguan operasional, kerusakan sistem, dan ancaman keamanan siber (Gartner, 2020).

Risiko terhadap aset TI dapat dibagi menjadi empat kategori, yaitu risiko strategis yang memengaruhi pencapaian tujuan bisnis, risiko bahaya akibat gangguan eksternal seperti bencana atau kejahatan, risiko keuangan yang berdampak pada kondisi finansial, dan risiko operasional yang timbul dari aktivitas harian organisasi (Schlegel & Trent, 2014). Untuk mengantisipasi risiko tersebut, organisasi perlu melakukan identifikasi dan klasifikasi aset TI guna mengenali komponen teknologi yang dimiliki serta menentukan tingkat kepentingan dan prioritas perlindungannya. Tahap ini merupakan dasar dari *risk identification* yang merupakan salah satu tahapan penting dalam manajemen risiko.

2.2.2 ISO/IEC 27005:2022

ISO/IEC 27005:2022 adalah standar internasional yang dikeluarkan bersama oleh International Organization for Standardization dan International Electrotechnical Commission sebagai panduan dalam manajemen risiko keamanan informasi. Standar ini digunakan untuk membantu organisasi mengidentifikasi, menilai, dan mengelola risiko secara lebih terstruktur dan terdokumentasi dengan baik, guna menghindari potensi risiko yang dapat mengganggu tujuan strategis dan keberlangsungan operasional organisasi.

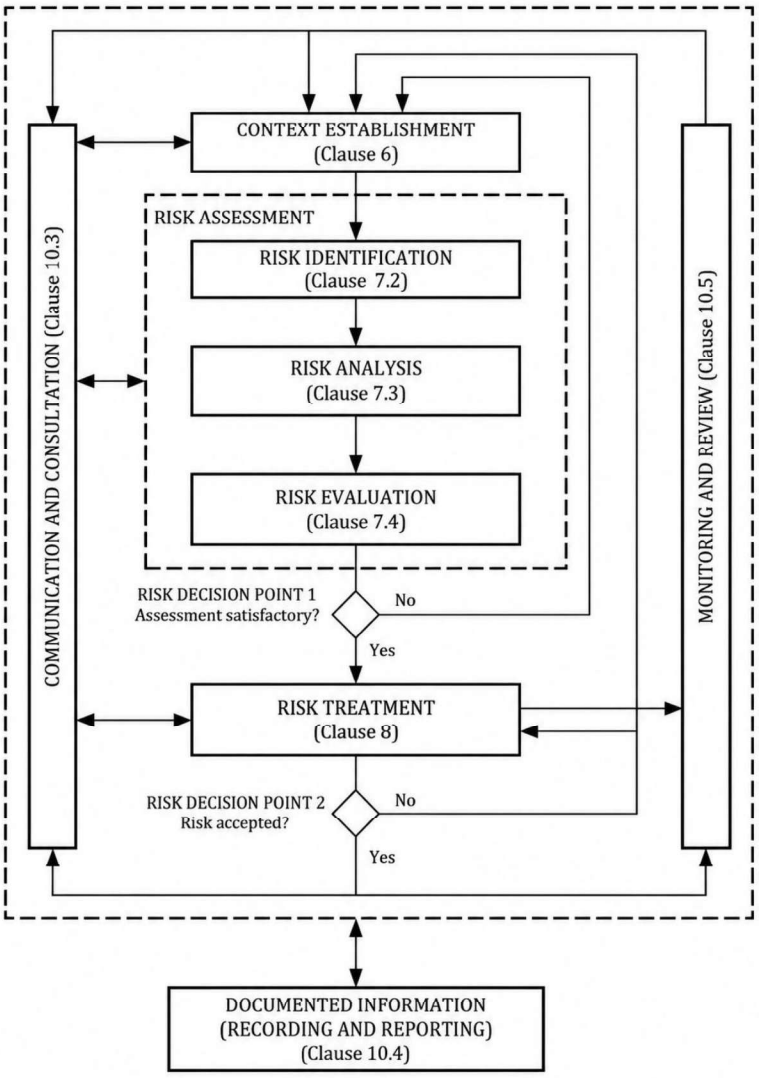
Standar ISO/IEC 27005 menekankan pentingnya pembentukan tim keamanan dalam suatu organisasi yang bertugas menyusun serta mengimplementasikan rencana keamanan informasi. Standar ini menyediakan langkah-langkah sistematis dalam manajemen risiko yang dimulai dengan identifikasi risiko, dilanjutkan dengan penilaian risiko yang relevan dengan konteks

SEKOLAH PASCASARJANA

bisnis organisasi, serta analisis terhadap potensi dampak dan konsekuensinya (Irsheid dkk., 2022).

Selanjutnya, organisasi perlu menentukan prioritas dalam penanganan risiko, menetapkan tindakan mitigasi yang paling efektif, serta melibatkan pemangku kepentingan dalam proses pengambilan keputusan. Proses ini juga mencakup pemantauan berkelanjutan terhadap pelaksanaan penanganan risiko, pendokumentasian informasi sebagai bahan evaluasi dan perbaikan, hingga penyelenggaraan pelatihan bagi staf agar memiliki pemahaman yang memadai mengenai risiko serta langkah mitigasi yang diambil (Irsheid dkk., 2022). Dengan demikian, ISO/IEC 27005 menekankan pendekatan yang komprehensif, meliputi identifikasi aset, ancaman, kerentanan, kontrol, kemungkinan terjadinya risiko, hingga konsekuensi yang ditimbulkan, sehingga organisasi dapat mengelola risiko keamanan informasi secara lebih terstruktur dan berkesinambungan.

SEKOLAH PASCASARJANA



Gambar 2. 2 *Framework* ISO/IEC 27005

Sumber: (ISO/IEC, 2022)

SEKOLAH PASCASARJANA

Dalam praktiknya, ISO/IEC 27005:2022 membagi proses manajemen risiko ke dalam beberapa tahapan yang saling terkait. Setiap tahapan memiliki peran spesifik yang berkontribusi terhadap efektivitas pengelolaan risiko. Proses tersebut terdiri atas tahapan inti yaitu, penetapan konteks (*establishment of context*), penilaian risiko (*risk assessment*) dan penanganan risiko (*risk treatment*). Selain itu terdapat tahapan pendukung yaitu, pemantauan dan tinjauan (*monitoring & review*), komunikasi dan konsultasi (*communication & consultation*) dan informasi

terdokumentasi (*Documented Information*). Berikut uraian detail dari masing-masing tahapan (ISO/IEC, 2022):

1. Penetapan Konteks Organisasi (*Establishment of Context*)

Tahap pertama dalam ISO/IEC 27005 adalah menetapkan konteks organisasi. Penetapan konteks ini penting untuk memastikan bahwa seluruh proses manajemen risiko memiliki acuan yang jelas dan selaras dengan tujuan strategis organisasi. Konteks mencakup pemahaman mengenai visi, misi, struktur organisasi, serta peraturan dan kebijakan eksternal yang memengaruhi pengelolaan risiko.

Dalam penetapan konteks, organisasi perlu mendefinisikan ruang lingkup manajemen risiko, seperti aset informasi apa saja yang akan dinilai, unit organisasi mana yang terlibat, serta batasan lingkungan yang memengaruhi sistem informasi. Selain itu, perlu pula ditentukan kriteria risiko yang akan digunakan sebagai acuan dalam menilai tingkat risiko, misalnya skala konsekuensi, probabilitas, maupun ambang batas penerimaan risiko.

Tahap ini juga menekankan pada identifikasi pemangku kepentingan yang memiliki kepentingan terhadap keamanan informasi, baik dari internal maupun eksternal organisasi. Dengan demikian, penetapan konteks berfungsi sebagai pondasi untuk memastikan bahwa proses manajemen risiko selaras dengan kebutuhan bisnis, regulasi, serta harapan para pemangku kepentingan.

2. Penilaian Risiko (*Risk Assessment*)

Metode penentuan tingkat risiko pada dasarnya berfokus pada upaya mengidentifikasi, menilai, dan mengukur potensi ancaman yang dapat memengaruhi keberlangsungan suatu organisasi. Menurut ISO 27005 (2022), tingkat risiko ditentukan dari kombinasi antara konsekuensi yang mungkin timbul (*Consequence*) dan kemungkinan terjadinya suatu peristiwa (*Likelihood*). Dengan kata lain, semakin tinggi probabilitas suatu ancaman terjadi dan semakin besar konsekuensinya terhadap aset organisasi, maka semakin tinggi pula tingkat risikonya. Proses ini biasanya dilakukan melalui analisis kualitatif, kuantitatif, atau kombinasi keduanya, yang memungkinkan organisasi memahami risiko secara lebih komprehensif.

SEKOLAH PASCASARJANA

Proses penilaian risiko dalam ISO/IEC 27005:2022 terdiri dari tiga sub-proses utama, yaitu: identifikasi risiko, analisis risiko, dan evaluasi risiko.

a. Identifikasi Risiko (*Risk Identification*)

Identifikasi risiko merupakan langkah awal untuk mengenali semua potensi risiko yang dapat memengaruhi keamanan informasi organisasi. Aktivitas ini melibatkan identifikasi aset informasi, ancaman yang mungkin terjadi, kerentanan dalam sistem, serta kemungkinan skenario insiden. Dalam konteks ISO/IEC 27005, aset informasi dapat berupa data digital, perangkat keras, perangkat lunak, jaringan, hingga sumber daya manusia yang terlibat. Ancaman dapat bersumber dari internal maupun eksternal, misalnya serangan siber, kesalahan manusia, bencana alam, atau kegagalan sistem. Sementara itu, kerentanan adalah kelemahan yang memungkinkan ancaman terealisasi, seperti kurangnya kontrol akses, lemahnya enkripsi, atau tidak adanya prosedur cadangan. Untuk mendukung proses ini, ISO/IEC 27005:2022 menyediakan contoh tabel hasil identifikasi ancaman dan kerentanan yang dapat dijadikan acuan organisasi dalam mendokumentasikan keterkaitan antara ancaman dan kerentanan pada setiap aset secara sistematis (ISO/IEC, 2022). Identifikasi risiko bertujuan menghasilkan daftar risiko yang lengkap, sehingga organisasi dapat memiliki gambaran komprehensif mengenai titik rawan dalam lingkup keamanan informasinya.

b. Analisis Risiko (*Risk Analysis*)

Setelah risiko diidentifikasi, tahap selanjutnya adalah melakukan analisis. Analisis risiko dapat dilakukan secara kualitatif, kuantitatif, atau gabungan keduanya. Pendekatan kualitatif biasanya menggunakan skala deskriptif, seperti rendah, sedang, atau tinggi, untuk menilai probabilitas terjadinya risiko dan tingkat konsekuensinya. Pendekatan kuantitatif menggunakan data numerik atau model matematis untuk menghitung probabilitas dan besarnya kerugian potensial. Tujuan utama analisis risiko adalah memberikan ukuran yang lebih konkret mengenai seberapa besar kemungkinan suatu risiko terjadi dan seberapa serius konsekuensi yang ditimbulkan.

Pada pendekatan semi-kuantitatif, tingkat risiko diperoleh dari kombinasi antara nilai *likelihood* dan nilai *consequence* yang masing-masing dinyatakan

SEKOLAH PASCASARJANA

dalam skala numerik. Kombinasi kedua parameter tersebut diformulasikan sebagai perkalian, sebagaimana ditunjukkan pada persamaan 2.1 (Hidayatullah dkk., 2024):

$$Level\ Risiko = Likelihood \times Consequence \quad (2.1)$$

Dengan:

Level Risiko adalah nilai tingkat risiko yang dihasilkan dari suatu skenario risiko

Likelihood adalah nilai kemungkinan terjadinya suatu skenario risiko

Consequence adalah Nilai dampak yang ditimbulkan apabila skenario risiko tersebut terjadi.

Nilai yang dihasilkan selanjutnya dipetakan ke dalam matriks risiko untuk mengelompokkan risiko ke dalam kategori tingkat risiko tertentu, sehingga dapat dibandingkan dengan kriteria penerimaan risiko pada tahap evaluasi.

c. Evaluasi Risiko (*Risk Evaluation*)

Tahap evaluasi dilakukan dengan membandingkan hasil analisis risiko dengan kriteria risiko yang telah ditentukan pada tahap penetapan konteks. Evaluasi ini bertujuan untuk mengidentifikasi risiko mana yang dapat diterima dan risiko mana yang perlu ditangani lebih lanjut. Evaluasi ini membantu organisasi dalam menetapkan prioritas pengelolaan risiko.

3. Penanganan Risiko (*Risk Treatment*)

Setelah risiko dievaluasi, organisasi perlu menetapkan strategi untuk menangani risiko tersebut. ISO/IEC 27005 mengenali beberapa pilihan penanganan risiko, di antaranya:

a. Modifikasi Risiko (*Risk Modification*), mengurangi kemungkinan terjadinya risiko atau menurunkan konsekuensinya melalui penerapan kontrol keamanan, misalnya penggunaan firewall, enkripsi data, atau prosedur keamanan tambahan.

b. Penghindaran Risiko (*Risk Avoidance*), menghapus aktivitas yang menimbulkan risiko, misalnya dengan menghentikan penggunaan sistem tertentu yang sangat rentan.

SEKOLAH PASCASARJANA

c. Berbagi Risiko (*Risk Sharing*), memindahkan tanggung jawab risiko ke pihak lain, misalnya melalui asuransi atau kontrak dengan penyedia layanan.

d. Retensi Risiko (*Risk Retention*), menerima keberadaan risiko tertentu dengan mempertimbangkan bahwa biaya mitigasi lebih besar daripada potensi kerugian.

Setelah opsi perlakuan risiko dipilih dan diimplementasikan, akan tetap ada sisa risiko yang disebut risiko residual. Proses manajemen risiko belum selesai sampai manajemen membuat keputusan formal untuk menerima tingkat risiko residual ini. Penerimaan risiko ini didasarkan pada pemahaman bahwa risiko residual tersebut sudah berada dalam batas toleransi yang telah ditetapkan oleh organisasi. Keputusan ini harus didokumentasikan sebagai bukti akuntabilitas. Proses ini perlu dirancang dengan mempertimbangkan efektivitas biaya serta dampaknya terhadap operasional organisasi.

4. Komunikasi dan Konsultasi (*Communication & Consultation*)

Komunikasi dan konsultasi merupakan proses pendukung yang berkelanjutan dan dua arah. Komunikasi yang efektif diperlukan agar seluruh pihak yang berkepentingan memahami risiko yang dihadapi, strategi mitigasi yang diambil, serta peran masing-masing dalam menjaga keamanan informasi. Tujuannya untuk membangun pemahaman dan kesepakatan bersama di antara para pemangku kepentingan. Tahap ini mencakup pertukaran informasi mengenai keberadaan, sifat, kemungkinan, konsekuensi hingga penanganan dan penerimaan risiko.

SEKOLAH PASCASARJANA

5. Pemantauan dan Tinjauan (*Monitoring & Review*)

Risiko bersifat dinamis, karena ancaman, kerentanan, dan lingkungan bisnis selalu berubah seiring waktu. Oleh karena itu, ISO/IEC 27005 menekankan pentingnya pemantauan dan tinjauan secara berkelanjutan. Pemantauan meliputi pemeriksaan efektivitas kontrol yang diterapkan, pengukuran kinerja manajemen

risiko, serta identifikasi risiko baru yang mungkin muncul. Sementara itu, peninjauan dilakukan secara berkala untuk memastikan bahwa pendekatan manajemen risiko tetap relevan dengan konteks organisasi. Proses pemantauan dan tinjauan dapat dilakukan melalui audit internal, peninjauan kebijakan, serta analisis tren insiden keamanan informasi. Dengan demikian, organisasi dapat merespons perubahan dengan cepat dan menjaga efektivitas sistem manajemen risiko.

6. Informasi Terdokumentasi (*Information Documented*)

Tahap ini berfungsi untuk mencatat keseluruhan proses dan hasil dari manajemen risiko. Dokumentasi ini tidak berdiri sendiri, melainkan mencakup dua aspek utama yaitu, pencatatan proses untuk memastikan konsistensi dan pencatatan hasil, seperti daftar risiko teridentifikasi, pemilik risiko, dan rencana penanganan) sebagai bukti pengambilan keputusan. Tujuannya adalah untuk menyediakan bukti kepatuhan, memastikan akuntabilitas, dan mendukung tinjauan serta perbaikan berkelanjutan pada sistem manajemen keamanan informasi.

2.2.3 COBIT 2019

Control Objectives for Information and Related Technology (COBIT) merupakan sebuah kerangka kerja dalam tata kelola perusahaan informasi dan teknologi atau biasa disebut EGIT. Kerangka COBIT dikembangkan oleh ISACA yang merupakan wadah bagi ekspertis internasional yang tertarik atau bekerja di bidang audit TI, risiko TI, dan tata kelola TI. ISACA berdiri sejak tahun 1967 dan telah berkembang menjadi organisasi yang diakui secara internasional dengan lebih dari 150.000 anggota di seluruh dunia (De Haes dkk., 2020).

COBIT 2019 merupakan penyempurnaan COBIT 5, hasil penyempurnaan kerangka kerja pada COBIT 2019 memiliki 2 aktivitas utama pada tata kelola dan manajemen (ISACA, 2018b) :

1. Tata kelola memastikan bahwa:

SEKOLAH PASCASARJANA

a. Kebutuhan, kondisi, dan opsi pemangku kepentingan dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati bersama.
b. Arah ditetapkan melalui prioritisasi dan pengambilan keputusan.
c. Kinerja dan kepatuhan dipantau sesuai dengan arah dan tujuan yang telah disepakati.

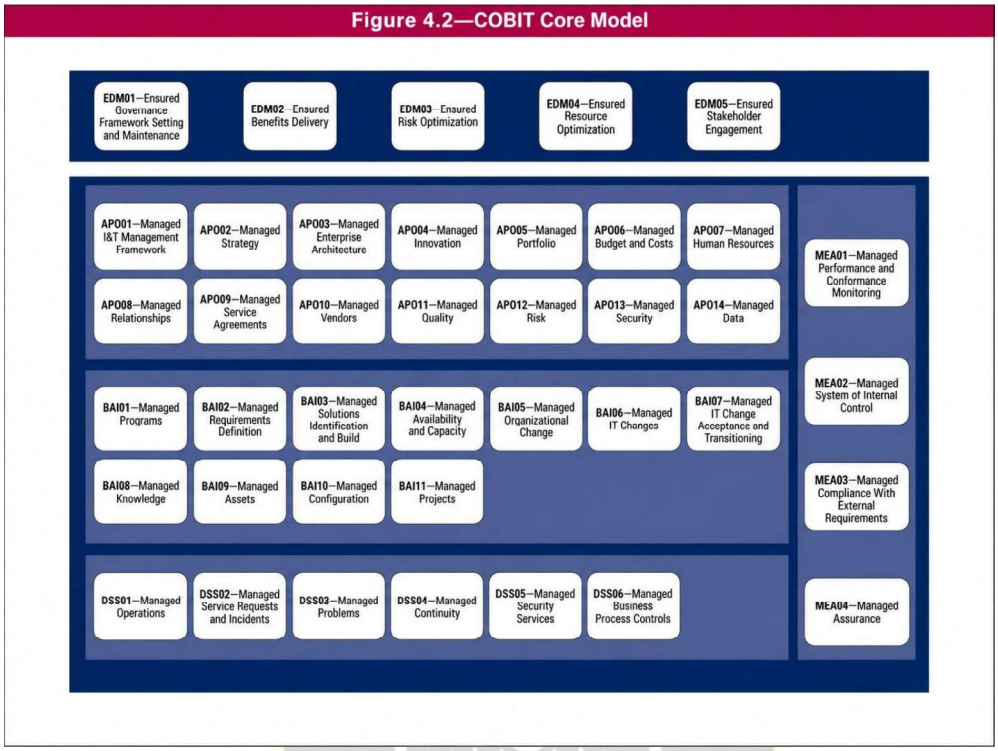
2. Manajemen merencanakan, membangun, menjalankan, dan memantau aktivitas, sesuai dengan arah yang ditetapkan oleh badan tata kelola, untuk mencapai tujuan perusahaan.

Tujuan tata kelola dan manajemen dalam COBIT 2019 dikelompokkan ke dalam 5 domain yang secara keseluruhan memuat 40 Governance and Management Objective (GMO). Setiap GMO berkaitan dengan satu proses yang tingkat kapabilitasnya dapat dinilai. Kelima domain tersebut yaitu:

1. *Evaluate, Direct, and Monitor* (EDM), pada EDM terdapat 5 GMO yang berfungsi untuk mengevaluasi opsi tata kelola, menetapkan arah melalui pengambilan keputusan dan prioritisasi, serta memantau kinerja dan kepatuhan terhadap arah yang telah disepakati.
2. *Align, Plan, and Organize* (APO), pada APO terdapat 14 GMO yang membahas mengenai keseluruhan organisasi, strategi, dan aktivitas pendukung untuk TI.
3. *Build, Acquire, and Implement* (BAI), pada BAI terdapat 11 GMO yang berfungsi untuk menentukan, mengakuisisi, dan mengimplementasikan solusi TI dan solusi integrasi dalam proses bisnis.
4. *Deliver, Service, and Support* (DSS), pada DSS terdapat 6 GMO yang berfungsi untuk menangani pengiriman operasional dan dukungan layanan TI termasuk pada keamanannya.

SEKOLAH PASCASARJANA

5. *Monitor, Evaluate, and Assess* (MEA), pada MEA terdapat 4 GMO yang membahas mengenai pengawasan kinerja dan kesuaian TI pada target kinerja, tujuan pengendalian internal dan persyaratan eksternal.



Gambar 2. 3 Domain dan GMO COBIT 2019

Sumber: (ISACA, 2018b)

COBIT 2019 menggunakan *Capability Level Model* untuk menilai sejauh mana suatu proses tata kelola dan manajemen TI telah dilaksanakan. Model ini menggambarkan tingkat kemampuan organisasi mulai dari proses yang belum terkelola sama sekali (level 0) hingga proses yang sudah optimal dan berorientasi pada perbaikan berkelanjutan (level 5). Dengan demikian, organisasi dapat mengetahui posisi aktualnya sekaligus arah peningkatan yang perlu dilakukan. Skala penilaian tingkat kapabilitas proses pada COBIT 2019 terdiri atas enam level, yaitu:

a. Level 0 (*Incomplete Process*), proses tidak ada atau gagal mencapai tujuan.

SEMARANG
SEKOLAH PASCASARJANA

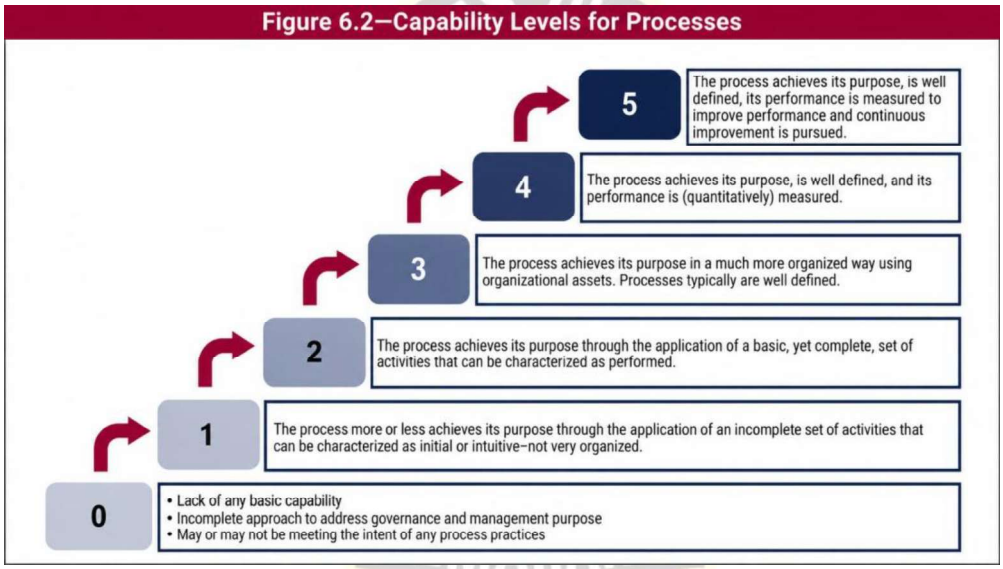
b. Level 1 (*Performed Process*), proses dilaksanakan, tetapi belum terdokumentasi atau konsisten.

c. Level 2 (*Managed Process*), proses sudah dikelola dan direncanakan, ada dokumentasi dasar.

d. Level 3 (*Established Process*), proses terdokumentasi jelas, terstandarisasi, dan dilaksanakan konsisten.

e. Level 4 (*Predictable Process*), proses dipantau, diukur, dan mampu memberikan hasil yang dapat diprediksi.

f. Level 5 (*Optimizing Process*), proses selalu dievaluasi dan ditingkatkan secara berkelanjutan.



Gambar 2. 4 Capability Level Model pada COBIT 2019

Sumber: (ISACA, 2018b)

SEKOLAH PASCASARJANA

Unit dasar penilaian dalam model ini adalah aktivitas. Setiap GMO terdiri atas sejumlah *management practice*, dan setiap practice dijabarkan menjadi aktivitas-aktivitas yang masing-masing telah diberi label capability level tertentu. Suatu proses dinyatakan mencapai suatu capability level apabila seluruh aktivitas pada level tersebut telah terlaksana secara berhasil.

Tingkat keterlaksanaan setiap aktivitas diperoleh dari penilaian sejumlah responden yang memiliki peran terhadap aktivitas tersebut. Nilai capaian suatu

aktivitas ditentukan dengan merata-ratakan skor seluruh responden pada aktivitas yang bersangkutan, yaitu penerapan prinsip perata-rataan skor (Sari dkk., 2024) pada tataran aktivitas, sebagaimana ditunjukkan pada Persamaan 2.2.

$$\text{Skor Aktivitas} = \frac{\sum Skor\ Responden}{\sum Responden} \quad (2.2)$$

Dengan:

Skor Aktivitas adalah rata-rata skor suatu aktivitas

∑ Skor Responden adalah jumlah skor seluruh responden pada aktivitas tersebut

∑ Responden adalah jumlah responden

Skor aktivitas tersebut selanjutnya dikonversi ke dalam bentuk persentase capaian dengan membaginya terhadap skor maksimum skala Likert, kemudian dikalikan seratus persen, sebagaimana ditunjukkan pada Persamaan 2.3 (Sari dkk., 2024).

$$\%\ \text{Capaian} = \frac{Skor\ Aktivitas}{Skor\ Maksimum} \times 100\% \quad (2.3)$$

Dengan:

% Capaian adalah persentase capaian per aktivitas

Skor Aktivitas adalah rata-rata skor suatu aktivitas

Skor Maksimum adalah Skor tertinggi skala Likert, yaitu 5

Persentase capaian tersebut kemudian diklasifikasikan ke dalam empat peringkat capaian sesuai standar ISACA, dapat dilihat pada Tabel 2.2 (ISACA, 2018b).

Tabel 2. 2 Skala Penilaian Tingkat Kapabilitas

Skala	Keterangan	Pencapaian
N	*Not Achieved*	<15
P	*Partially Achieved*	>15 – 50
L	*Largely Achieved*	>50 – 85
F	*Fully Achieved*	>85 – 100

SEKOLAH PASCASARJANA

Penetapan tingkat kapabilitas dilakukan secara berjenjang. Dalam prosedur tersebut, suatu capability level dinyatakan tercapai hanya apabila seluruh aktivitas pada level yang bersangkutan memperoleh peringkat minimal Largely (L). Keberadaan satu atau lebih aktivitas yang memperoleh peringkat Partially (P) atau

Not (N) menyebabkan level tersebut dinyatakan belum tercapai. Rincian prosedur penetapan capability level adalah sebagai berikut (Neto dkk.,2019):

1. Penilaian dimulai dari Level 2 dengan menentukan peringkat capaian (N, P, L, F) untuk setiap aktivitas pada level tersebut.
2. Evaluasi Kesiapan Level 2 dilakukan dengan ketentuan berikut:

a. Jika semua aktivitas Level 2 memperoleh peringkat Largely (L) atau Fully (F), maka proses tersebut dinyatakan telah memenuhi persyaratan Capability Level 2.

b. Jika terdapat aktivitas Level 2 yang memperoleh peringkat Partially (P) atau Not (N), maka proses tersebut belum memenuhi persyaratan Capability Level 2. Dalam kondisi ini, capability level proses ditetapkan pada Level 1, dengan catatan bahwa aktivitas-aktivitas dasar proses telah dilaksanakan meskipun belum dikelola secara konsisten.

3. Jika Level 2 telah terpenuhi, maka penilaian dilanjutkan secara sequential ke aktivitas-aktivitas pada Level 3, Level 4, dan Level 5 dengan prosedur yang sama. Suatu proses hanya dapat dinyatakan mencapai level yang lebih tinggi apabila seluruh aktivitas pada level tersebut memenuhi kriteria peringkat minimal Largely (L). Dengan demikian, tingkat kapabilitas akhir suatu proses ditetapkan pada level tertinggi yang seluruh aktivitasnya telah memenuhi kriteria peringkat minimal Largely (L). Penilaian dihentikan pada level pertama yang memiliki satu atau lebih aktivitas dengan peringkat Partially (P) atau Not (N).

Tingkat kapabilitas aktual yang diperoleh selanjutnya dibandingkan dengan tingkat kapabilitas target yang ditetapkan organisasi untuk mengetahui besarnya kesenjangan. Selisih antara keduanya dihitung sebagaimana ditunjukkan pada Persamaan 2.4 (Wijaya dkk., 2023).

$$Gap = Level\ kapabilitas\ target - Level\ kapabilitas\ aktual \quad (2.4)$$

Dengan:

Gap adalah Selisih atau kesenjangan tingkat kapabilitas

Level kapabilitas target adalah Tingkat kapabilitas yang diharapkan pada suatu objektif proses

SEKOLAH PASCASARJANA

Level kapabilitas aktual Adalah Tingkat kapabilitas aktual saat ini, diperoleh dari hasil penilaian kapabilitas

Semakin besar nilai kesenjangan pada suatu objektif proses, semakin besar pula kebutuhan peningkatan pada proses tersebut, sehingga nilai kesenjangan dapat digunakan sebagai dasar penentuan prioritas perbaikan tata kelola.

2.2.4 Integrasi ISO/IEC 27005:2022 dan COBIT 2019

Kedua metode dalam penelitian ini menempati posisi yang berbeda dan tidak saling menggantikan. ISO/IEC 27005:2022 digunakan sebagai standar penilaian risiko keamanan informasi, dengan lingkup mulai dari penetapan konteks hingga evaluasi risiko, dan menghasilkan daftar skenario risiko aset TI yang telah dinilai serta diprioritaskan. Versi 2022 dipilih secara spesifik karena memformalkan pendekatan identifikasi risiko berbasis peristiwa dan berbasis aset, suatu penyempurnaan struktural yang tidak dimiliki versi sebelumnya. Formalisasi tersebut memungkinkan skenario risiko disusun pada tingkat granularitas yang dapat ditelusuri langsung ke kondisi aset operasional tertentu, bukan pada katalog ancaman generik, sehingga keluarannya layak berfungsi sebagai masukan faktual yang dapat diverifikasi. Penggunaan standar ini berhenti pada tahap evaluasi risiko, karena ISO/IEC 27005:2022 tidak menyediakan instrumen untuk mengukur kapabilitas proses tata kelola yang seharusnya mengendalikan risiko yang ditemukan.

COBIT 2019 digunakan sebagai *framework* tata kelola dan manajemen TI, dengan lingkup mulai dari pemetaan risiko prioritas ke GMO hingga penilaian *Capability Level* dan analisis kesenjangan. *Framework* ini dipilih karena menyediakan GMO yang terstruktur beserta sasaran tata kelola yang eksplisit, sehingga skenario risiko dapat dicocokkan secara sistematis berdasarkan tanggung jawab fungsional, bukan berdasarkan penilaian subjektif. Penggunaannya dimulai setelah daftar risiko prioritas tersedia, karena daftar tersebut menjadi bukti empiris yang menentukan GMO mana yang dinilai. Dengan pembagian tersebut, ISO/IEC 27005:2022 berperan sebagai sumber bukti risiko teknis, sedangkan COBIT 2019 berperan sebagai objek evaluasi tata kelola.

SEMARANG
SEKOLAH PASCASARJANA

Integrasi ISO/IEC 27005:2022 dan COBIT 2019 didasarkan pada sifat komplementer dari standar dan *framework* tersebut yang dapat diterapkan secara sekuensial. Tujuan dari penggabungan keduanya adalah untuk menjembatani kesenjangan antara temuan risiko teknis di lapangan dengan evaluasi proses tata kelola di tingkat manajerial. Studi komparatif yang dilakukan oleh Irsheid dkk. (2022) terhadap berbagai model manajemen risiko menempatkan ISO/IEC 27005 sebagai pendekatan yang berfokus pada proses penilaian risiko keamanan informasi, namun bersifat abstrak dan tidak menetapkan metode teknis tertentu pada tiap langkahnya. Dalam studi tersebut, COBIT versi 5 dikategorikan sebagai model yang tidak berhenti pada proses manajemen risiko, melainkan turut mencakup tata kelola risiko atau *risk governance* untuk mengontrol dan memantau kebijakan keamanan, serta melibatkan pemangku kepentingan melalui mekanisme RACI. Cakupan tata kelola dan keterlibatan peran yang tidak dimiliki pendekatan berbasis penilaian risiko semata inilah yang menjadi dasar pemaduan, sekaligus karakteristik yang dipertahankan dan disempurnakan pada COBIT 2019 (ISACA, 2018b).

Keterpaduan standar dan framework tersebut telah dibuktikan dalam penelitian Flores & Morocho (2020) yang mengintegrasikan COBIT v.5, ISO/IEC 27005, dan OCTAVE-S ke dalam satu kerangka tata kelola dan manajemen risiko untuk layanan sektor publik. Dalam kerangka tersebut, COBIT diposisikan sebagai kerangka payung tata kelola yang menaungi direktif proses manajemen risiko ISO/IEC 27005, sehingga GMO COBIT dapat dipetakan secara langsung terhadap tahapan penilaian dan penanganan risiko ISO/IEC 27005. Keselarasan tersebut menjadi landasan konseptual bahwa hasil penilaian risiko teknis dapat digunakan untuk menelaah proses tata kelola yang relevan, dan tetap berlaku pada COBIT 2019 karena model proses intinya dipertahankan dan disempurnakan dari COBIT 5 (ISACA, 2018b). Langkah pemetaan serupa telah dilakukan Yasin dkk. (2020) yang menerjemahkan kontrol ISO/IEC 27001:2013 ke *core model* COBIT 2019 hingga menghasilkan 29 *core model* COBIT 2019 terpilih sebagai objek penilaian kapabilitas, sehingga meskipun standar yang dipetakan berbeda, penelitian tersebut

SEKOLAH PASCASARJANA

menjadi acuan bahwa cakupan suatu standar keamanan informasi dapat diturunkan menjadi GMO COBIT 2019 yang terukur.

Pemaduan ISO/IEC 27005 dan COBIT 2019 telah dilakukan pada penelitian Pratama & Nugraha (2025), memadukan keduanya dalam satu kerangka hibrida, tetapi COBIT 2019 hanya difungsikan sebagai panduan tata kelola pada tiap tahap proses tanpa dilakukan pengukuran tingkat kapabilitas, sehingga temuan risiko tidak menjadi dasar evaluasi kematangan tata kelola. Pada penelitian yang melakukan pengukuran kapabilitas, penentuan GMO yang dinilai justru bertumpu pada kuesioner berbasis persepsi sebagai mekanisme utama, sebagaimana terlihat pada Fawwazdzaky dkk. (2025), Aflakhah dan Soewito (2023), serta Oktaviana dkk. (2024). Pendekatan semacam ini menimbulkan subjektivitas dalam pemilihan GMO, karena GMO yang dinilai bermasalah ditentukan oleh penilaian responden, bukan oleh kondisi operasional yang terverifikasi. Dengan demikian, celah yang belum terjawab bukan terletak pada pemilihan rujukan, melainkan pada cara temuan risiko diterjemahkan menjadi penentuan GMO COBIT 2019 yang dievaluasi.

Berlandaskan keselarasan pemetaan teoretis dari literatur tersebut, penelitian ini menerapkannya dalam alur metodologi yang berorientasi pada evaluasi efektivitas pengelolaan risiko yang sedang berjalan. Berbeda dengan penelitian sebelumnya yang memadukan keduanya untuk merancang kerangka baru atau memanfaatkan COBIT sebagai panduan kontrol mitigasi, penelitian ini secara spesifik menjadikan hasil penilaian risiko ISO/IEC 27005 sebagai input bukti untuk menentukan GMO COBIT 2019 yang dievaluasi tingkat kapabilitasnya. Pendekatan yang menjadikan temuan risiko teknis sebagai dasar penentuan GMO COBIT 2019 yang dinilai inilah yang dalam penelitian ini disebut sebagai mekanisme transformasi bukti.

Tahap penentuan GMO yang dievaluasi menempati posisi yang menentukan dalam integrasi ini, karena di titik itulah keluaran penilaian risiko ISO/IEC 27005:2022 berpindah menjadi masukan bagi evaluasi tata kelola COBIT 2019, sehingga ketepatan penilaian kapabilitas hingga penyusunan rekomendasi

SEKOLAH PASCASARJANA

bergantung pada benar tidaknya GMO yang ditetapkan. Penurunan GMO dari skenario risiko tidak dapat dilakukan melalui pencocokan istilah antara pernyataan risiko dan nama GMO, karena cara demikian justru mengembalikan subjektivitas yang hendak dihindari. Oleh sebab itu, mekanisme transformasi bukti bersandar pada model tanggung jawab tata kelola COBIT 2019, yaitu bahwa setiap GMO secara fungsional bertanggung jawab untuk mencegah atau mengendalikan jenis risiko tertentu (ISACA, 2018a). Dengan premis tersebut, skenario risiko berkategori Tinggi atau Sangat Tinggi merupakan bukti empiris bahwa proses tata kelola yang bertanggung jawab atas jenis risiko tersebut tidak tersedia atau belum diterapkan secara memadai di instansi, sehingga penurunan GMO merupakan penalaran atas tanggung jawab fungsional, bukan pencocokan istilah.

SEKOLAH PASCASARJANA