Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15895
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Pengukuran *Capability level* Manajemen Risiko Dinas Komunikasi dan Informasi Kabupaten Malang Menggunakan Cobit 5

[1]Farid Angga Pribadi, [2]Raviansyah Yudistira Pratama, [3]Rokhimatul Wakhidah
[1,2,3]Politeknik Negeri Malang
Malang, Indonesia

[1]faridangga@polinema.ac.id, [2] raviansyahy@gmail.com, [3]wakhidah@polinema.ac.id

*Penulis Korespondensi
Diajukan : 21/01/2026
Diterima : 08/02/2026
Dipublikasi : 10/02/2026

ABSTRAK
Penelitian ini bertujuan untuk mengukur tingkat kapabilitas manajemen risiko di Dinas Komunikasi dan Informasi Kabupaten Malang menggunakan kerangka kerja COBIT 5. COBIT 5 adalah *framework* yang menyediakan prinsip, praktik, alat, dan model untuk membantu organisasi dalam mencapai tujuan tata kelola dan manajemen teknologi informasi. Dalam penelitian ini, domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan APO13 (*Manage Security*) dari COBIT 5 digunakan sebagai acuan utama. Metodologi yang digunakan melibatkan pengumpulan data melalui observasi, wawancara, dan kuesioner yang ditujukan kepada pegawai Dinas Komunikasi dan Informasi Kabupaten Malang. Data yang diperoleh dianalisis untuk menentukan tingkat kapabilitas manajemen risiko saat ini dan mengidentifikasi area yang perlu ditingkatkan. Hasil penelitian menunjukkan bahwa tingkat kapabilitas manajemen risiko di Dinas Komunikasi dan Informasi Kabupaten Malang berada pada level 2 (*Managed Process*). Ini menunjukkan bahwa proses manajemen risiko telah dilaksanakan dengan baik namun masih memerlukan peningkatan dalam dokumentasi dan pengukuran kinerja secara konsisten. Rekomendasi yang diberikan mencakup peningkatan dokumentasi proses, pelatihan berkelanjutan bagi pegawai, serta penerapan alat bantu teknologi informasi untuk mendukung pengelolaan risiko. Implementasi rekomendasi ini diharapkan dapat meningkatkan kapabilitas manajemen risiko menuju level yang lebih tinggi sesuai dengan standar COBIT 5.

Kata Kunci: Capability Level; COBIT 5; Manajemen Risiko TI; Tata Kelola TI; Teknologi Informasi.

I. PENDAHULUAN

Perkembangan teknologi informasi di era digital saat ini telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan, termasuk dalam lingkungan organisasi pemerintahan. Teknologi informasi tidak lagi hanya berfungsi sebagai alat bantu administratif, tetapi telah berkembang menjadi komponen strategis yang berperan penting dalam mendukung proses operasional, pengelolaan data, serta pengambilan keputusan. Penerapan teknologi informasi memungkinkan organisasi untuk meningkatkan efisiensi dan efektivitas dalam menjalankan tugas dan fungsinya, sehingga mampu memberikan layanan yang lebih cepat, tepat, dan akurat. Dengan adanya teknologi informasi, organisasi dapat mengoptimalkan penggunaan sumber daya yang dimiliki serta meningkatkan produktivitas secara keseluruhan (Utomo dkk., 2012).

Penggunaan teknologi informasi juga memungkinkan organisasi untuk meninggalkan metode konvensional yang cenderung kurang efisien dan rentan terhadap kesalahan. Sistem berbasis teknologi informasi memungkinkan pengelolaan data dilakukan secara otomatis, terintegrasi, dan *real-time*, sehingga mempermudah organisasi dalam melakukan pemantauan dan pengendalian terhadap berbagai proses yang berjalan. Selain itu, teknologi informasi juga memberikan kemudahan

e-ISSN : 2541-1330
p-ISSN : 2541-1332

dalam penyimpanan, pengolahan, serta distribusi informasi, sehingga mendukung terciptanya sistem kerja yang lebih efektif dan efisien. Hal ini menunjukkan bahwa teknologi informasi memiliki peran penting dalam meningkatkan kualitas operasional organisasi serta mendukung pencapaian tujuan organisasi secara optimal (Hariyani & Sudrajat, 2017).

Dalam konteks pemerintahan, penerapan teknologi informasi menjadi salah satu faktor penting dalam mendukung terciptanya tata kelola pemerintahan yang baik atau *good governance*. Teknologi informasi memungkinkan pemerintah untuk meningkatkan transparansi, akuntabilitas, serta efisiensi dalam penyelenggaraan pemerintahan. Dengan adanya sistem teknologi informasi yang terintegrasi, pemerintah dapat memberikan layanan publik yang lebih cepat, transparan, dan akuntabel. Selain itu, teknologi informasi juga memungkinkan pemerintah untuk meningkatkan kualitas pengambilan keputusan melalui penyediaan data dan informasi yang akurat dan tepat waktu (Suradi & Wiyanta, 2017). Oleh karena itu, penerapan teknologi informasi yang efektif menjadi kebutuhan penting bagi instansi pemerintahan dalam meningkatkan kualitas layanan publik.

Dinas Komunikasi dan Informatika Kabupaten Malang merupakan salah satu instansi pemerintah yang memiliki peran penting dalam pengelolaan teknologi informasi di lingkungan pemerintah daerah. Instansi ini bertanggung jawab dalam mengelola berbagai aspek yang berkaitan dengan teknologi informasi, komunikasi, persandian, serta statistik daerah. Dalam menjalankan tugas dan fungsinya, Dinas Komunikasi dan Informatika Kabupaten Malang memanfaatkan teknologi informasi sebagai sarana untuk mendukung operasional organisasi serta meningkatkan kualitas layanan kepada masyarakat. Oleh karena itu, pengelolaan teknologi informasi yang baik dan terstruktur menjadi sangat penting untuk memastikan bahwa teknologi informasi yang digunakan dapat memberikan manfaat yang optimal bagi organisasi (Najwa & Susanto, 2018).

Pengelolaan teknologi informasi yang tidak dilakukan dengan baik dapat menimbulkan berbagai risiko yang dapat mengganggu operasional organisasi. Risiko tersebut dapat berupa gangguan sistem, kehilangan data, kebocoran informasi, serta kegagalan sistem yang dapat berdampak negatif terhadap kinerja organisasi. Oleh karena itu, diperlukan suatu sistem manajemen risiko yang efektif untuk mengidentifikasi, menganalisis, serta mengendalikan risiko yang berkaitan dengan teknologi informasi. Manajemen risiko teknologi informasi merupakan proses yang penting dalam memastikan bahwa teknologi informasi dapat digunakan secara aman, efektif, dan sesuai dengan tujuan organisasi (Firdaus, 2018).

Salah satu kerangka kerja yang dapat digunakan untuk mengelola teknologi informasi dan manajemen risiko adalah COBIT 5. COBIT 5 merupakan *framework* yang menyediakan prinsip, praktik, alat, serta model yang dapat digunakan oleh organisasi untuk mengelola dan mengendalikan teknologi informasi secara efektif. Framework ini membantu organisasi dalam memastikan bahwa teknologi informasi yang digunakan telah selaras dengan tujuan organisasi serta mampu memberikan nilai tambah bagi organisasi. Selain itu, COBIT 5 juga menyediakan panduan dalam mengelola risiko teknologi informasi, sehingga organisasi dapat mengidentifikasi dan mengendalikan risiko yang mungkin terjadi (Information Systems Audit and Control Association, 2012).

COBIT 5 juga memiliki keunggulan dalam kemampuannya untuk mengintegrasikan berbagai standar dan praktik terbaik dalam pengelolaan teknologi informasi. *Framework* ini menyediakan pendekatan yang komprehensif dan terstruktur dalam mengelola teknologi informasi, termasuk dalam aspek tata kelola, manajemen risiko, serta keamanan informasi. Dengan menggunakan COBIT 5, organisasi dapat memastikan bahwa seluruh proses pengelolaan teknologi informasi telah dilakukan secara sistematis dan sesuai dengan standar yang berlaku. Hal ini menjadikan COBIT 5 sebagai salah satu framework yang banyak digunakan oleh berbagai organisasi, baik di sektor swasta maupun sektor pemerintahan (Damayanti & Manuputty, 2019).

Dalam COBIT 5, terdapat beberapa domain yang berkaitan dengan pengelolaan risiko teknologi informasi, di antaranya adalah EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan APO13 (*Manage Security*). Domain EDM03 berfokus pada optimalisasi risiko, APO12 berfokus pada pengelolaan risiko, dan APO13 berfokus pada pengelolaan keamanan informasi. Ketiga domain ini memiliki peran penting dalam memastikan bahwa risiko teknologi informasi dapat dikelola secara efektif dan terstruktur. Dengan menggunakan domain-domain tersebut, organisasi dapat mengidentifikasi tingkat kemampuan dalam mengelola risiko teknologi informasi serta

e-ISSN : 2541-1330
p-ISSN : 2541-1332

menentukan langkah-langkah yang diperlukan untuk meningkatkan kemampuan tersebut (Information Systems Audit and Control Association, 2012).

Untuk mengetahui tingkat kemampuan organisasi dalam mengelola risiko teknologi informasi, diperlukan suatu metode pengukuran yang dapat digunakan untuk menilai tingkat kapabilitas manajemen risiko yang telah diterapkan. *Capability level* merupakan salah satu metode yang dapat digunakan untuk mengukur tingkat kemampuan organisasi dalam mengelola proses teknologi informasi, termasuk manajemen risiko. Pengukuran *capability level* memungkinkan organisasi untuk mengetahui sejauh mana proses manajemen risiko telah diterapkan serta mengidentifikasi area yang memerlukan perbaikan dan peningkatan (Arief, t.t.).

Pengukuran *capability level* juga memungkinkan organisasi untuk melakukan analisis kesenjangan atau *gap analysis* antara kondisi saat ini dengan kondisi yang diharapkan. Dengan melakukan gap analysis, organisasi dapat mengidentifikasi kelemahan yang ada serta menentukan langkah-langkah yang diperlukan untuk meningkatkan kemampuan manajemen risiko. Hasil dari pengukuran *capability level* dan *gap analysis* dapat digunakan sebagai dasar dalam menyusun rekomendasi perbaikan yang bertujuan untuk meningkatkan kualitas pengelolaan teknologi informasi di organisasi (Firdaus, 2018).

Selain itu, penerapan manajemen risiko yang baik juga dapat membantu organisasi dalam meningkatkan keandalan sistem teknologi informasi serta mengurangi potensi kerugian yang dapat ditimbulkan oleh risiko teknologi informasi. Dengan adanya manajemen risiko yang efektif, organisasi dapat mengantisipasi berbagai risiko yang mungkin terjadi serta mengambil langkah-langkah yang diperlukan untuk mengurangi dampak dari risiko tersebut. Hal ini sangat penting bagi instansi pemerintah, karena gangguan pada sistem teknologi informasi dapat berdampak langsung terhadap kualitas layanan publik yang diberikan kepada masyarakat (Damayanti & Manuputty, 2019).

Berdasarkan pentingnya pengelolaan teknologi informasi dan manajemen risiko, maka diperlukan suatu penelitian yang bertujuan untuk mengukur tingkat *capability level* manajemen risiko di Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan *framework* COBIT 5. Dengan melakukan pengukuran *capability level*, diharapkan dapat diperoleh gambaran mengenai tingkat kemampuan organisasi dalam mengelola risiko teknologi informasi. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi yang dapat digunakan untuk meningkatkan kualitas manajemen risiko teknologi informasi di instansi tersebut.

Hasil dari penelitian ini diharapkan dapat memberikan manfaat bagi Dinas Komunikasi dan Informatika Kabupaten Malang dalam meningkatkan kualitas pengelolaan teknologi informasi serta manajemen risiko yang diterapkan. Selain itu, penelitian ini juga diharapkan dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan, khususnya dalam bidang tata kelola teknologi informasi dan manajemen risiko. Dengan adanya penelitian ini, diharapkan organisasi dapat meningkatkan kemampuan dalam mengelola teknologi informasi serta mendukung terciptanya tata kelola teknologi informasi yang efektif, efisien, dan sesuai dengan standar yang berlaku (Najwa & Susanto, 2018).

II. TINJAUAN PUSTAKA

Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi merupakan suatu sistem yang digunakan untuk memastikan bahwa penggunaan teknologi informasi dapat mendukung pencapaian tujuan organisasi secara efektif dan efisien. Tata kelola ini mencakup struktur organisasi, kebijakan, serta proses yang digunakan untuk mengarahkan dan mengendalikan penggunaan teknologi informasi agar selaras dengan tujuan organisasi (Information Systems Audit and Control Association, 2012). Penerapan tata kelola teknologi informasi yang baik memungkinkan organisasi untuk meningkatkan transparansi, akuntabilitas, serta efektivitas dalam pengelolaan teknologi informasi. Selain itu, tata kelola teknologi informasi juga membantu organisasi dalam mengelola risiko serta memastikan bahwa teknologi informasi dapat memberikan nilai tambah dan mendukung keberlangsungan operasional organisasi secara optimal (Damayanti & Manuputty, 2019).

e-ISSN : 2541-1330
p-ISSN : 2541-1332

COBIT 5

COBIT 5 merupakan *framework* yang digunakan sebagai pedoman dalam tata kelola dan manajemen teknologi informasi untuk membantu organisasi mencapai tujuan yang diharapkan. Framework ini menyediakan prinsip, praktik, serta model yang dapat digunakan untuk mengelola teknologi informasi secara sistematis dan terstruktur (Information Systems Audit and Control Association, 2012). COBIT 5 juga mendukung organisasi dalam menyelaraskan penggunaan teknologi informasi dengan tujuan organisasi sehingga dapat meningkatkan efektivitas dan efisiensi operasional. Selain itu, framework ini menyediakan panduan dalam pengelolaan risiko, keamanan informasi, serta pengukuran kinerja dan kapabilitas proses teknologi informasi untuk memastikan bahwa teknologi informasi telah dikelola dengan baik (Firdaus, 2018).

Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi merupakan proses yang dilakukan untuk mengidentifikasi, menganalisis, serta mengendalikan risiko yang berkaitan dengan penggunaan teknologi informasi dalam organisasi. Risiko teknologi informasi dapat berasal dari berbagai sumber, seperti kegagalan sistem, kesalahan pengguna, maupun ancaman keamanan informasi yang dapat mengganggu operasional organisasi (Information Systems Audit and Control Association, 2012). Pengelolaan risiko yang baik memungkinkan organisasi untuk meminimalkan dampak negatif yang ditimbulkan oleh risiko serta meningkatkan keamanan dan keandalan sistem teknologi informasi. Oleh karena itu, manajemen risiko teknologi informasi menjadi bagian penting dalam tata kelola teknologi informasi untuk mendukung keberlangsungan operasional organisasi (Firdaus, 2018).

***Capability level* COBIT 5**

Capability level merupakan suatu metode yang digunakan untuk mengukur tingkat kemampuan organisasi dalam mengelola proses teknologi informasi. Pengukuran *capability level* bertujuan untuk mengetahui sejauh mana suatu proses telah dilaksanakan dan dikelola sesuai dengan standar yang ditetapkan (Information Systems Audit and Control Association, 2012). *Capability level* dalam COBIT 5 terdiri dari beberapa tingkatan, yaitu level 0 hingga level 5, yang menunjukkan tingkat kematangan proses dalam organisasi. Dengan melakukan pengukuran *capability level*, organisasi dapat mengetahui kondisi proses saat ini serta mengidentifikasi area yang memerlukan perbaikan dan peningkatan dalam pengelolaan teknologi informasi (Damayanti & Manuputty, 2019).

Domain EDM03, APO12, dan APO13

Domain EDM03, APO12, dan APO13 merupakan bagian dari *framework* COBIT 5 yang berkaitan dengan pengelolaan risiko dan keamanan teknologi informasi. Domain EDM03 berfokus pada optimalisasi risiko untuk memastikan bahwa risiko teknologi informasi telah dikelola secara efektif dan sesuai dengan tujuan organisasi (Information Systems Audit and Control Association, 2012). Domain APO12 berfokus pada proses manajemen risiko, termasuk identifikasi, analisis, serta pengendalian risiko yang dapat mempengaruhi operasional organisasi (Firdaus, 2018). Domain APO13 berfokus pada pengelolaan keamanan informasi untuk memastikan bahwa informasi organisasi terlindungi dari berbagai ancaman dan risiko yang dapat mengganggu keberlangsungan operasional organisasi (Damayanti & Manuputty, 2019).

III. METODE

Penelitian ini menggunakan pendekatan evaluatif untuk mengukur tingkat *capability level* manajemen risiko teknologi informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang dengan menggunakan *framework* COBIT 5. Pendekatan ini digunakan untuk mengetahui kondisi aktual pengelolaan risiko teknologi informasi serta mengidentifikasi kesenjangan antara kondisi saat ini dan kondisi yang diharapkan dalam organisasi. *Framework* COBIT 5 digunakan karena menyediakan model pengukuran *capability level* yang dapat digunakan untuk mengevaluasi kemampuan proses teknologi informasi secara sistematis dan terstruktur (Pratama, 2024). Tahapan penelitian dimulai dari studi literatur, identifikasi masalah, penentuan domain yang diteliti, hingga analisis *capability level* dan penyusunan rekomendasi perbaikan berdasarkan hasil evaluasi yang dilakukan.

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Penelitian ini berfokus pada domain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan APO13 (*Manage Security*) yang berkaitan langsung dengan pengelolaan risiko dan keamanan teknologi informasi. Ketiga domain tersebut digunakan untuk mengukur sejauh mana organisasi telah mengelola risiko teknologi informasi secara efektif dan sesuai dengan *framework* COBIT 5 (Pratama, 2024). Penentuan responden dilakukan menggunakan metode RACI Chart (*Responsible, Accountable, Consulted, Informed*), yang digunakan untuk mengidentifikasi pihak-pihak yang memiliki tanggung jawab dalam pengelolaan teknologi informasi. Penggunaan RACI Chart membantu memastikan bahwa responden yang dipilih merupakan pihak yang memiliki peran dan pemahaman yang relevan terhadap proses yang dievaluasi, sehingga data yang diperoleh dapat menggambarkan kondisi organisasi secara akurat.

Pengumpulan data dilakukan menggunakan metode kuesioner, wawancara, dan observasi untuk memperoleh informasi yang lengkap dan akurat. Kuesioner digunakan sebagai instrumen utama untuk mengukur *capability level* berdasarkan praktik-praktik yang terdapat dalam COBIT 5, yang memungkinkan pengukuran dilakukan secara terstruktur (Pratama, 2024). Selain itu, wawancara dilakukan dengan pihak terkait untuk memperoleh informasi yang lebih mendalam mengenai proses pengelolaan risiko teknologi informasi serta kendala yang dihadapi dalam pelaksanaannya. Observasi juga dilakukan dengan meninjau dokumen dan prosedur yang berkaitan dengan pengelolaan teknologi informasi guna memastikan kesesuaian antara data yang diperoleh dengan kondisi aktual di organisasi.

Tahap selanjutnya adalah analisis data untuk menentukan tingkat *capability level* pada setiap domain yang diteliti berdasarkan hasil kuesioner, wawancara, dan observasi. Analisis dilakukan dengan menghitung nilai *capability level* dan membandingkannya dengan tingkat *capability level* yang diharapkan melalui analisis kesenjangan atau *gap analysis*, yang digunakan untuk mengidentifikasi perbedaan antara kondisi saat ini dan kondisi yang diharapkan (Pratama, 2024). Hasil dari analisis ini kemudian digunakan sebagai dasar dalam penyusunan rekomendasi perbaikan untuk meningkatkan *capability level* manajemen risiko teknologi informasi. Rekomendasi yang dihasilkan diharapkan dapat membantu organisasi dalam meningkatkan kualitas tata kelola teknologi informasi serta mendukung pengelolaan risiko yang lebih efektif dan terstruktur.

IV. HASIL DAN PEMBAHASAN

Pengukuran *capability level* tata kelola teknologi informasi dilakukan untuk mengetahui tingkat kemampuan organisasi dalam mengelola proses teknologi informasi secara sistematis, terstruktur, dan berkelanjutan. *Capability level* merupakan indikator penting yang menunjukkan sejauh mana suatu organisasi telah mampu menerapkan proses tata kelola teknologi informasi sesuai dengan standar yang telah ditetapkan. Penilaian *capability level* tidak hanya menggambarkan kondisi proses yang sedang berjalan, tetapi juga menunjukkan tingkat kematangan organisasi dalam mengendalikan, mengawasi, serta meningkatkan kualitas proses teknologi informasi. Dengan mengetahui *capability level*, organisasi dapat memahami posisi saat ini serta menentukan langkah-langkah strategis yang diperlukan untuk mencapai kondisi yang diharapkan.

Capability level yang diperoleh menunjukkan bahwa proses tata kelola teknologi informasi telah berada pada level 2 atau Managed Process. Level ini menunjukkan bahwa organisasi telah memiliki proses yang direncanakan dengan baik serta telah dilaksanakan sesuai dengan prosedur yang telah ditentukan. Proses yang berjalan tidak dilakukan secara sembarangan, melainkan telah mengikuti mekanisme yang terstruktur dan telah menjadi bagian dari aktivitas operasional organisasi. Selain itu, proses yang dilakukan juga telah dipantau dan dikendalikan untuk memastikan bahwa proses tersebut berjalan sesuai dengan tujuan yang telah ditetapkan. Hal ini menunjukkan bahwa organisasi telah memiliki kemampuan dalam mengelola proses teknologi informasi secara sistematis.

Capability level 2 juga menunjukkan bahwa organisasi telah memiliki tanggung jawab yang jelas dalam pelaksanaan proses teknologi informasi. Setiap aktivitas yang dilakukan telah memiliki peran dan fungsi yang jelas, sehingga proses dapat berjalan secara terarah dan terkontrol. Organisasi juga telah melakukan pemantauan terhadap pelaksanaan proses teknologi informasi untuk memastikan bahwa proses tersebut berjalan sesuai dengan rencana yang telah ditetapkan. Pemantauan ini bertujuan untuk mengidentifikasi potensi permasalahan yang dapat mempengaruhi proses teknologi informasi serta memastikan bahwa proses yang dilakukan dapat mendukung

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 10, Nomor 1, Januari 2026
http://doi.org/10.33395/remik.v10i1.15895
e-ISSN : 2541-1330
p-ISSN : 2541-1332

operasional organisasi secara optimal.

Selain itu, *capability level* 2 menunjukkan bahwa organisasi telah memiliki pengelolaan proses yang cukup baik, termasuk dalam hal perencanaan, pelaksanaan, serta pengendalian proses teknologi informasi. Organisasi telah mampu mengelola proses teknologi informasi dengan baik sehingga proses tersebut dapat berjalan secara efektif dan efisien. Pengelolaan yang baik terhadap proses teknologi informasi akan membantu organisasi dalam meningkatkan kualitas layanan teknologi informasi serta memastikan bahwa teknologi informasi dapat digunakan secara optimal dalam mendukung kegiatan operasional organisasi.

Meskipun *capability level* yang diperoleh menunjukkan bahwa organisasi telah memiliki pengelolaan teknologi informasi yang cukup baik, organisasi masih memiliki target *capability level* yang lebih tinggi, yaitu *capability level* 3 atau Established Process. *Capability level* ini menunjukkan bahwa organisasi diharapkan memiliki proses yang terdokumentasi secara lengkap, distandarisasi, serta diterapkan secara konsisten dalam seluruh unit organisasi. Pada level ini, proses yang dilakukan tidak hanya dilaksanakan dengan baik, tetapi juga telah memiliki dokumentasi yang lengkap serta telah menjadi standar yang diterapkan secara formal dalam organisasi. *Capability level* ini menunjukkan bahwa organisasi diharapkan memiliki proses yang terdokumentasi secara lengkap, distandarisasi, serta diterapkan secara konsisten dalam seluruh unit organisasi, yaitu :

Tabel 1 *Capability level*

No	Nama Proses	Capability Level Responden			*Capability Level* saat ini
		1	2	3	
1	EDM03 (*Ensure Risk Optimization*)	2	2	2	2
2	APO12 (*Manage Risk*).	2	2	2	2
3	APO13 (*Manage Security*)	2	2	2	2

Berdasarkan tabel 1 *capability level* tersebut, dapat diketahui bahwa seluruh subdomain yang diukur memiliki *capability level* saat ini sebesar level 2, sedangkan *capability level* yang diharapkan adalah level 3. Hal ini menunjukkan bahwa terdapat gap sebesar 1 pada setiap subdomain. Gap ini menunjukkan adanya perbedaan antara kondisi saat ini dengan kondisi yang diharapkan oleh organisasi. Gap tersebut menunjukkan bahwa organisasi telah memiliki proses yang berjalan dengan baik, namun masih memerlukan peningkatan dalam beberapa aspek untuk mencapai tingkat kematangan yang lebih tinggi.

Pada subdomain EDM03 (*Ensure Risk Optimization*), *capability level* yang diperoleh menunjukkan bahwa organisasi telah memiliki kemampuan dalam mengelola risiko teknologi informasi. Organisasi telah mampu mengidentifikasi risiko yang berkaitan dengan penggunaan teknologi informasi serta melakukan pengendalian terhadap risiko tersebut. Pengelolaan risiko yang baik akan membantu organisasi dalam mengurangi potensi gangguan yang dapat mempengaruhi operasional teknologi informasi. Namun, untuk mencapai *capability level* yang lebih tinggi, organisasi perlu meningkatkan dokumentasi proses pengelolaan risiko serta memastikan bahwa seluruh proses pengelolaan risiko telah distandarisasi secara formal.

Pada subdomain APO12 (*Manage Risk*), *capability level* yang diperoleh menunjukkan bahwa organisasi telah memiliki mekanisme dalam mengelola risiko teknologi informasi. Organisasi telah melakukan identifikasi, pemantauan, serta pengendalian terhadap risiko yang berkaitan dengan teknologi informasi. Hal ini menunjukkan bahwa organisasi telah memiliki kesadaran terhadap pentingnya pengelolaan risiko dalam menjaga keberlangsungan sistem informasi. Namun, organisasi masih perlu meningkatkan standarisasi dan dokumentasi proses pengelolaan risiko agar proses tersebut dapat dilaksanakan secara konsisten dan terstruktur.

Pada subdomain APO13 (*Manage Security*), *capability level* yang diperoleh menunjukkan bahwa organisasi telah memiliki mekanisme dalam mengelola keamanan informasi. Organisasi telah melakukan pengawasan terhadap penggunaan teknologi informasi serta melakukan pengendalian terhadap keamanan sistem informasi. Pengelolaan keamanan informasi yang baik akan membantu organisasi dalam menjaga kerahasiaan, integritas, serta ketersediaan informasi. Namun, untuk mencapai *capability level* yang lebih tinggi, organisasi perlu meningkatkan dokumentasi kebijakan

e-ISSN : 2541-1330
p-ISSN : 2541-1332

keamanan informasi serta memastikan bahwa seluruh proses keamanan informasi telah diterapkan secara konsisten.

Gap *capability level* yang terdapat pada seluruh subdomain menunjukkan bahwa organisasi masih memiliki beberapa aspek yang perlu ditingkatkan. Gap ini menunjukkan bahwa organisasi telah memiliki fondasi tata kelola teknologi informasi yang cukup baik, namun masih memerlukan peningkatan dalam hal dokumentasi, standarisasi, serta pengendalian proses teknologi informasi. Dengan melakukan peningkatan tersebut, organisasi akan mampu mencapai *capability level* yang diharapkan.

Peningkatan *capability level* akan memberikan manfaat yang signifikan bagi organisasi, terutama dalam meningkatkan kualitas pengelolaan teknologi informasi. Dengan *capability level* yang lebih tinggi, organisasi akan memiliki proses yang lebih terstruktur dan terdokumentasi dengan baik. Hal ini akan membantu organisasi dalam meningkatkan efektivitas pengelolaan teknologi informasi serta mengurangi risiko yang berkaitan dengan penggunaan teknologi informasi.

Selain itu, peningkatan *capability level* juga akan membantu organisasi dalam meningkatkan keamanan informasi serta memastikan bahwa informasi yang dimiliki dapat dilindungi dengan baik. Keamanan informasi merupakan aspek yang sangat penting dalam pengelolaan teknologi informasi, karena informasi merupakan aset yang memiliki nilai yang sangat penting bagi organisasi. Dengan pengelolaan keamanan informasi yang baik, organisasi akan mampu melindungi informasi dari berbagai ancaman yang dapat mempengaruhi operasional organisasi.

Capability level yang lebih tinggi juga akan membantu organisasi dalam meningkatkan efisiensi dan efektivitas proses teknologi informasi. Proses yang terdokumentasi dengan baik akan memudahkan organisasi dalam melakukan pengawasan, evaluasi, serta perbaikan terhadap proses yang dilakukan. Hal ini akan membantu organisasi dalam meningkatkan kualitas layanan teknologi informasi serta memastikan bahwa teknologi informasi dapat digunakan secara optimal.

Selain itu, peningkatan *capability level* juga akan membantu organisasi dalam meningkatkan kepercayaan terhadap sistem teknologi informasi yang digunakan. Sistem teknologi informasi yang dikelola dengan baik akan memberikan dukungan yang lebih optimal terhadap kegiatan operasional organisasi. Hal ini akan membantu organisasi dalam meningkatkan kinerja serta mencapai tujuan organisasi secara lebih efektif.

Secara keseluruhan, *capability level* yang diperoleh menunjukkan bahwa organisasi telah memiliki tata kelola teknologi informasi yang cukup baik dan telah dilakukan secara terstruktur. Proses teknologi informasi telah direncanakan, dilaksanakan, serta dipantau dengan baik, sehingga dapat mendukung kegiatan operasional organisasi. Namun, organisasi masih perlu melakukan peningkatan untuk mencapai *capability level* yang diharapkan. Dengan melakukan peningkatan tersebut, organisasi akan mampu meningkatkan kualitas tata kelola teknologi informasi serta memastikan bahwa teknologi informasi dapat dikelola secara efektif, efisien, dan aman dalam mendukung pencapaian tujuan organisasi.

V. KESIMPULAN

Tata kelola teknologi informasi merupakan aspek penting dalam mendukung keberlangsungan operasional organisasi, khususnya dalam memastikan bahwa risiko dan keamanan informasi dapat dikelola secara efektif dan terstruktur. Pengelolaan teknologi informasi yang baik memungkinkan organisasi untuk meningkatkan efisiensi, efektivitas, serta keandalan sistem informasi yang digunakan dalam mendukung kegiatan operasional. Pengukuran capability level pada subdomain EDM03 (*Ensure Risk Optimization*), APO12 (*Manage Risk*), dan APO13 (*Manage Security*) menunjukkan bahwa seluruh subdomain berada pada *capability level* 2 atau *Managed Process*. Hal ini menunjukkan bahwa proses tata kelola teknologi informasi telah direncanakan, dilaksanakan, dan dipantau dengan baik serta telah diterapkan dalam aktivitas operasional organisasi secara terstruktur.

Capability level yang diperoleh menunjukkan bahwa organisasi telah memiliki dasar tata kelola teknologi informasi yang cukup baik, namun masih terdapat gap antara *capability level* saat ini dengan *capability level* yang diharapkan, yaitu level 3 atau *Established Process*. Gap tersebut menunjukkan bahwa organisasi masih perlu melakukan peningkatan, terutama dalam aspek dokumentasi, standarisasi proses, dan penerapan prosedur secara konsisten. Dengan adanya

e-ISSN : 2541-1330
p-ISSN : 2541-1332

peningkatan tersebut, organisasi diharapkan mampu meningkatkan kualitas tata kelola teknologi informasi, memperkuat pengelolaan risiko dan keamanan informasi, serta memastikan bahwa teknologi informasi dapat dikelola secara lebih optimal dalam mendukung pencapaian tujuan organisasi secara efektif, efisien, dan berkelanjutan.

VI. REFERENSI

Anindya, V. F. (2024). Manajemen risiko teknologi informasi pada PT XYZ menggunakan framework COBIT 5. JSSI: Jurnal Sistem Informasi dan Sains, 2024.

Arief, M. H., & Suprapto. (2018). Evaluasi manajemen risiko teknologi informasi menggunakan kerangka kerja COBIT 5 (Studi kasus: Perum Jasa Tirta I Malang). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2(1), 101–109.

Arimbi, Y., & Sutabri, T. (2025). Analisis manajemen risiko pelayanan sistem manajemen dealer VIAR menggunakan COBIT 5. Indonesian Journal of Multidisciplinary on Social and Technology, 1(2), 145. https://doi.org/10.31004/ijmst.v1i2.145

Dermawan, S., Trista, A., Hisyam, A. A., & Untoro, E. K. (2025). Implementasi COBIT 5 untuk manajemen risiko TI pada UMKM (Studi kasus: UMKM XYZ). Jurnal Informasi, Sains dan Teknologi, 8(1). https://doi.org/10.55606/isaintek.v8i1.313

Firdaus, M. K. S. (2021). Evaluasi manajemen risiko teknologi informasi menggunakan framework COBIT 5 (Studi kasus: PT PLN P2B Jawa Bali). Applied Information System and Management (AISM), 3(2), 101–106. https://doi.org/10.15408/aism.v3i2.8600

Maharani, M., & Wijaya, A. (2025). Manajemen risiko TI pada BID TIK Polda Sumsel menggunakan framework COBIT 5. Jurnal Sistem dan Teknologi Informasi Komunikasi, 9(1). https://doi.org/10.32524/jusitik.v9i1.1460

Prasetyo, B., Toha, L. Q., & Retnani, W. E. Y. (2023). Risk management using COBIT 5 for risk: a case study on local government in Indonesia. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 8(1), 435–444. https://doi.org/10.22219/kinetik.v8i1.1585

Prastiyawan, D. A., Ambarwati, A., & Setiawan, E. (2020). Analisis manajemen risiko layanan sistem manajemen dealer menggunakan COBIT 5. Matrix: Jurnal Manajemen Teknologi dan Informatika, 10(2), 43–49. https://doi.org/10.31940/matrix.v10i2.1913

Putri, R. M. A., Murniati, W., Ashari, M., & Ashari, H. (2024). Manajemen risiko teknologi informasi menggunakan COBIT 5. Jurnal Informatika Teknologi dan Sains (JINTEKS), 6(3), 708–718. https://doi.org/10.51401/jinteks.v6i3.4780

Ramadhan, M. Y., Nasution, M. I. P., & Triase. (2022). Audit tata kelola teknologi informasi COBIT 5 manajemen risiko. Jurnal Sistem Informasi Kaputama (JSIK), 6(1), 15–23. https://doi.org/10.59697/jsik.v6i1.176

Safina, N., Elvanni, I., Arpiansah, A., & Wulansari, A. (2024). Manajemen risiko pada universitas menggunakan framework COBIT 5. Neraca: Jurnal Ekonomi, Manajemen dan Akuntansi, 2(1), 430–436. https://doi.org/10.572349/neraca.v2i1.792

Sari, H. A. N., Rahardja, Y., & Chernovita, H. P. (2021). Analisis manajemen risiko TI pada Diskominfo Salatiga menggunakan COBIT 5 domain APO12. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8(4), 1772–1784.

Sukmana, P. P., Yoga, T. P., & Habibi, C. (2023). Audit manajemen risiko sistem informasi pada website Digo.id dengan framework COBIT 5 dan ISO 31000. Jurnal Accounting Information System (AIMS), 6(2), 816. https://doi.org/10.32627/aims.v6i2.816

Thenu, P. P., Wijaya, A. F., & Rudianto, C. (2020). Analisis manajemen risiko teknologi informasi menggunakan COBIT 5 (Studi kasus: PT Global Infotech). Jurnal Bina Komputer, 2(1), 1–13.

Wattimena, M. A. G., & Tanaamah, A. R. (2021). Analisis manajemen risiko teknologi informasi menggunakan COBIT 5 (Studi kasus: TSI/teknologi dan sistem informasi perpustakaan UKSW). Journal of Information Systems and Informatics. https://doi.org/10.51519/journalisi.v3i3.183