COMSERVA
JURNAL PENELITIAN DAN PENGABDIAN MASYARAKAT
Volume 5 No. 3 Juli 2025 (966-978)
e-ISSN: 2798-5210
p-ISSN: 2798-5652

Perancangan Tata Kelola dan Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 pada Kota Cerdas Pemerintah Kabupaten

Rahmayanti Mahardikaningtyas[1], Erma Suryani[2]
Institut Teknologi Sepuluh Nopember, Indonesia
Email: rahmajoo999@gmail.com, erma.suryani@gmail.com

ABSTRAK

Transformasi digital berbasis konsep *smart city* mendorong pemerintah daerah untuk mengintegrasikan teknologi informasi dalam pelayanan publik. Namun, ketergantungan tinggi terhadap sistem informasi tanpa manajemen risiko yang memadai berpotensi menimbulkan ancaman serius terhadap efektivitas, keberlanjutan layanan, dan kepercayaan masyarakat. Penelitian ini bertujuan untuk merancang tata kelola dan manajemen risiko teknologi informasi pada Diskominfo Pemerintah Kabupaten menggunakan kerangka kerja COBIT 2019, khususnya domain EDM03 *(Ensure Risk Optimization)* dan APO12 *(Managed Risk)*. Metode yang digunakan adalah deskriptif-kualitatif dengan pendekatan capability assessment, melalui penyebaran kuesioner, observasi, dan wawancara kepada 12 responden kunci yang dipetakan menggunakan model RACI. Hasil penelitian menunjukkan bahwa kapabilitas pengelolaan risiko pada domain EDM03 berada pada level 2 *(Managed)*, sedangkan APO12 berada pada level 3 *(Defined)*. Gap analysis menunjukkan perlunya penguatan dokumentasi prosedur, integrasi sistem pelaporan risiko, serta peningkatan kesadaran keamanan TI. Penelitian ini menyusun rekomendasi mitigasi risiko menyeluruh yang mencakup aspek people, process, dan technology. Implikasinya, jika diimplementasikan dengan baik, rekomendasi ini dapat meningkatkan efisiensi, keandalan layanan, serta memperkuat kesiapan pemerintah daerah menuju transformasi digital yang aman dan berkelanjutan.

Kata Kunci: Kota cerdas; COBIT 2019; Manajemen Risiko TI; Level Kapabilitas TI; Penilaian TI Penilaian Risiko; Mitigasi Risiko.

ABSTRACT

Digital transformation driven by the smart city concept has encouraged local governments to integrate information technology into public services. However, high dependency on information systems without adequate risk management poses serious threats to organizational effectiveness, service continuity, and public trust. This study aims to design IT governance and risk management at the Department of Communication and Informatics (Diskominfo) of a district government using the COBIT 2019 framework, focusing on domain EDM03 (Ensure Risk Optimization) and APO12 (Managed Risk). A descriptive-qualitative method was employed using capability assessment through questionnaires, observations, and interviews with 12 key respondents mapped using the RACI model. The results show that the risk governance capability in EDM03 is at Level 2 (Managed), while APO12 is at Level 3 (Defined). The gap analysis reveals the need to strengthen procedural documentation, integrate risk reporting systems, and increase awareness of IT security. This study provides comprehensive risk mitigation recommendations across people, process, and technology aspects. If properly implemented, these strategies are expected to enhance service efficiency, reliability, and institutional readiness for secure and sustainable digital transformation.

***Keywords**: Smart city; COBIT 2019; IT Risk Management; IT Capability Level; IT Assessment Risk Assessment; Risk Mitigation.*

PENDAHULUAN

Persaingan di berbagai negara-negara di dunia saat ini tidak hanya berfokus pada pembangunan daya saing nasional namun lebih kepada pembangunan kota (Lestari, 2016; Sedyastuti, 2018). Hal ini bertujuan untuk meningkatkan perdagangan, investasi, wisata dan lainnya yang ada di suatu kota. Hal ini mendorong pemerintah kota untuk dapat menciptakan suasana lingkungan yang layak huni, nyaman, aman dan membawa kemakmuran sehingga kota dapat memiliki daya saing yang tinggi (Kemkominfo, 2017).

Dengan berkembangnya teknologi informasi dan komunikasi (TIK) yang pesat, maka mendorong gerakan digitalisasi dalam merubah peradaban manusia di dunia (Mustari, 2023; Purba et al., 2021). Berbagai kota di seluruh dunia mulai berlomba-lomba menerapkan smart city. Hal ini bertujuan untuk mewujudkan sustainability city serta mendorong peningkatan kualitas hidup masyarakat. Untuk mencapai smart city maka penting untuk menerapkan TIK di dalamnya. Investasi TIK di ASEAN pada tahun 2014 telah mencapai US$ 100 juta dan terus meningkat 15% setiap tahunnya (Kearney, 2015).

Berdasarkan kajian literatur, urbanisasi global terus meningkat dengan proyeksi 68% populasi dunia akan tinggal di kota pada tahun 2050 (UN DESA, 2018), sementara di Indonesia diperkirakan mencapai 70% pada 2045 (Bappenas, 2022), menjadikan kota sebagai pusat konsentrasi penduduk dan sekaligus sumber kompleksitas sosial, ekonomi, dan lingkungan. Tantangan seperti kemacetan, polusi, kesenjangan sosial, dan tekanan terhadap sumber daya alam mendorong perlunya transformasi perkotaan menuju kota layak huni dan berkelanjutan. Konsep smart city menjadi strategi penting dalam menjawab tantangan tersebut melalui integrasi teknologi informasi dan komunikasi (TIK) guna meningkatkan efisiensi layanan dan kualitas hidup masyarakat (ITU, 2014; Kemkominfo, 2017). Namun, implementasi smart city yang mengandalkan infrastruktur digital menghadirkan risiko keamanan informasi dan gangguan sistem yang perlu dikelola dengan baik. Oleh karena itu, tata kelola dan manajemen risiko TI menjadi kunci, yang dapat dioptimalkan melalui kerangka kerja COBIT 2019 khususnya domain EDM03 (Ensure Risk Optimization) dan APO12 (Managed Risk), sebagaimana direkomendasikan oleh ISACA (2018) untuk menjamin keberlanjutan dan efektivitas layanan publik digital di pemerintahan daerah.

Keamanan informasi adalah aspek penting dan memainkan peran penting dalam melindungi bisnis organisasi. Organisasi diharuskan untuk menjaga informasi dan aset mereka untuk mempertahankan nilai dan reputasi mereka (Ghamdi, et al., 2020).

Assessmen atau penilaian keamanan Sistem Informasi (SI) dan tata kelola TI diperlukan untuk mengetahui sejauh mana implementasinya sudah memenuhi standar dan kriteria ideal, juga untuk menilai risiko dan perlindungan terhadap aset perusahaan (Senft & Gallegos, 2008). Budaya keamanan informasi yang ideal diidentifikasi dengan ciri-ciri utama yang berkaitan dengan aspek-aspek seperti tenaga kerja yang sadar dan berpengetahuan yang menerapkan perilaku hati-hati dan peduli untuk mematuhi kebijakan yang dipandu oleh manajemen.

Organisasi yang memiliki budaya keamanan informasi yang kuat diidentifikasi mencapai rasa saling percaya dan integritas melalui perlindungan informasi mereka (Veiga, et al., 2020).

Proses tata kelola TI sangat penting bagi perusahaan untuk memutuskan apa dan bagaimana menggunakan sumber daya TI dan mengukur serta mencapai manfaat bisnis yang diharapkan. Konsep kapabilitas proses tata kelola TI didefinisikan sebagai kemampuan perusahaan untuk mengidentifikasi, merancang, mengimplementasikan, dan memanfaatkan proses tata kelola TI berikut: pengambilan keputusan TI, perencanaan TI, modernisasi infrastruktur TI, penyampaian layanan TI, dan pemantauan TI (Joshi, et al., 2021).

Banyak penelitian mengenai kerangka kerja Control Objectives for Information and Related Technology (COBIT) yang menyatakan bahwa COBIT merupakan kerangka kerja asesmen resiko dan mampu menyediakan tata kelola keamanan informasi yang menyeluruh

Manajemen resiko adalah suatu metode untuk menghadapi resiko di masa depan yang dapat memengaruhi kegiatan perusahaan. Proses ini dimulai dengan mengidentifikasi kemungkinan kejadian di masa depan, penilaian resiko yang ditimbulkannya, penentuan respons terhadapnya, dan pengawasan keberjalanan respons tersebut. COBIT 2019 digunakan sebagai landasan atau kerangka kerja dalam menilai tata kelola IT pada suatu organisasi. Berdasarkan ISACA, model inti COBIT yang terkait dengan spesifik tata kelola & manajemen resiko adalah domain EDM03 (Ensured Risk Optimisation) dan APO12 (Managed Risk).

Risk appetite atau selera resiko adalah tingkat resiko yang siap diterima perusahaan, perlu ditetapkan oleh perusahaan untuk menentukan rencana mitigasi resiko. Hasil assessmen maturity level COBIT 2019 dapat digunakan sebagai landasan pembuatan rekomendasi mitigasi resiko, mengelola dan menerapkan manajemen resiko Teknologi Informasi berdasarkan kerangka kerja Capability Maturity Model Integration (CMMI). Untuk memastikan rekomendasi mitigasi resiko tepat sasaran, maka perlu dilakukan perhitungan peringkat resiko. Dalam penelitian ini akan menghasilkan keluaran dari analisis gap EDM03 dan APO12 berupa rekomendasi sistem tata kelola manajemen resiko, SOP(Standard Operating Procedure) untuk mendokumentasikan proses, mengevaluasi dan mengontrol proses kinerja dari sistem dan teknologi informasi di pemerintah kabupaten XYZ. Rekomendasi solusi meliputi aspek People, Process, dan Technology.

Penelitian terdahulu telah membuktikan efektivitas kerangka kerja COBIT 2019 dalam mengelola tata kelola dan risiko TI. Nachrowi et al. (2020) dan Safitri et al. (2021) menunjukkan bagaimana domain EDM03 (Ensured Risk Optimization) dan APO12 (Managed Risk) dalam COBIT 2019 dapat digunakan untuk menilai kapabilitas dan merancang mitigasi risiko. Namun, sebagian besar studi tersebut berfokus pada organisasi besar atau sektor pusat, sehingga belum banyak yang mengkaji penerapannya di konteks pemerintahan kabupaten atau kota kecil-menengah.

Oleh karena itu, terdapat kesenjangan riset (*research gap*) dalam penerapan COBIT 2019 pada institusi pemerintahan lokal. Belum tersedia model khusus yang dapat memetakan kemampuan tata kelola risiko TI di lingkungan pemerintah kabupaten yang umumnya memiliki keterbatasan dalam infrastruktur dan sumber daya manusia. Gap ini menjadi dasar pentingnya penelitian ini untuk mengisi kekosongan pengetahuan dan praktik.

Urgensi penelitian ini semakin jelas setelah dilakukan penilaian terhadap kapabilitas tata kelola TI di Diskominfo Kabupaten Tulungagung. Hasilnya menunjukkan bahwa domain EDM03 baru berada di Level 2 (Managed), sedangkan domain APO12 berada di Level 3 (Defined). Artinya, proses sudah berjalan namun belum terukur secara kuantitatif dan belum terdokumentasi secara menyeluruh. Padahal, target ideal berada di Level 4 (Quantitatively Managed), yang berarti perlunya peningkatan signifikan dalam struktur, dokumentasi, dan pengukuran kinerja risiko TI.

Penelitian ini menawarkan kebaruan (*novelty*) dengan mengaplikasikan COBIT 2019 secara mendalam di tingkat pemerintah kabupaten. Selain itu, penggunaan pendekatan RACI (Responsible, Accountable, Consulted, Informed) dalam memetakan peran-peran penting dalam proses manajemen risiko TI menjadi kekuatan metodologis yang membedakan riset ini dari studi sebelumnya. Penelitian ini juga menyajikan rekomendasi konkret untuk SOP dan penguatan struktur kelembagaan risiko TI.

Tujuan dari penelitian ini adalah untuk melakukan penilaian (assessment) terhadap pengelolaan Teknologi Informasi (TI) pada domain EDM03 (Ensured Risk Optimization) dan APO12 (Managed Risk) dengan menggunakan kerangka kerja COBIT 2019 sebagai dasar metode penelitian dalam menilai risiko TI. Penelitian ini juga bertujuan untuk memetakan dan menganalisis risiko TI yang muncul dalam proses tata kelola di lingkungan Diskominfo pemerintah kabupaten. Selain itu, penelitian ini berupaya menyusun rekomendasi dan langkah-langkah mitigasi terhadap risiko-risiko tersebut guna menyelaraskan pengelolaan proses TI dengan strategi organisasi yang diterapkan oleh Diskominfo pemerintah kabupaten.

Manfaat dari penelitian ini dibagi ke dalam dua aspek, yaitu manfaat teoritis dan manfaat praktis. Secara teoritis, hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan rancangan tata kelola TI sebagai bagian dari perumusan rencana strategis TIK di lingkungan Pemerintah Kabupaten XYZ. Penelitian ini juga dapat dijadikan referensi bagi institusi lain dalam mengidentifikasi dan mengevaluasi tata kelola serta manajemen risiko TI berbasis kerangka kerja COBIT 2019. Dengan demikian, penelitian ini memberikan nilai tambah dalam pengembangan ilmu pengetahuan, khususnya dalam perumusan kebijakan teknologi informasi dan penyusunan regulasi yang relevan di tingkat daerah, seperti peraturan bupati.

Secara praktis, penelitian ini diharapkan memberikan manfaat nyata bagi Pemerintah Kabupaten dalam bentuk rekomendasi yang dapat diterapkan oleh setiap Organisasi Perangkat Daerah (OPD) dalam menyusun dan melaksanakan pengembangan rencana strategis TIK dan manajemen risiko TI secara terintegrasi. Bagi OPD, hasil penelitian ini diharapkan menjadi pedoman pelaksanaan kegiatan pengembangan TIK, khususnya dalam lingkup kerja Diskominfo, sehingga tata kelola TI dapat dijalankan secara lebih efektif, efisien, dan selaras dengan arah kebijakan daerah.

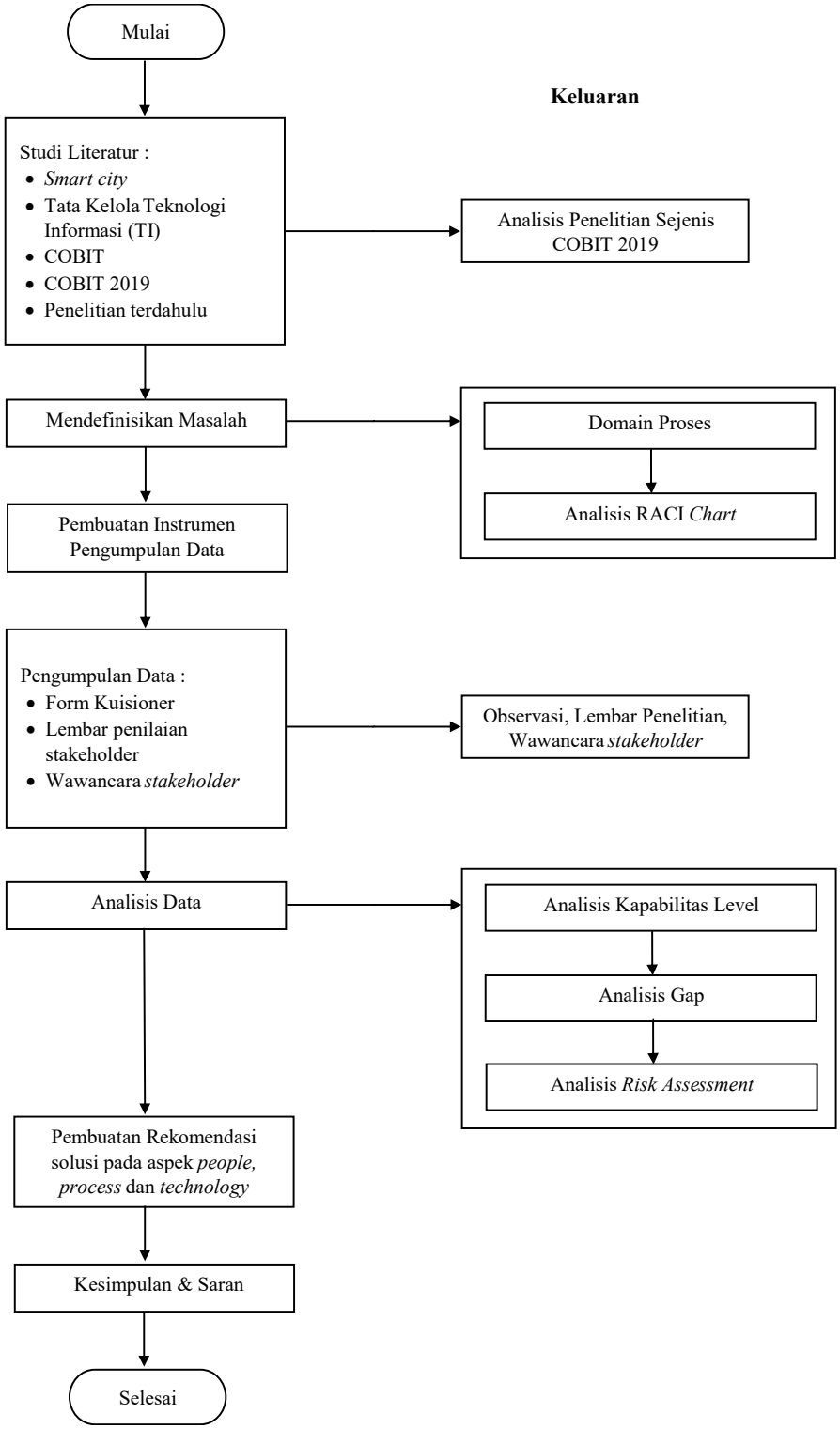
METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus pada instansi pemerintah daerah, khususnya Diskominfo Kabupaten Tulungagung, sebagai bentuk implementasi *smart city.* Populasi penelitian mencakup seluruh unit kerja yang terlibat

dalam pengelolaan TI, sedangkan sampel ditentukan secara purposive sampling berdasarkan peran strategis dan operasional dalam tata kelola TI, seperti kepala bidang, staf teknis, dan pejabat pengambil keputusan. Total terdapat 12 responden kunci yang dipetakan menggunakan pendekatan RACI *(Responsible, Accountable, Consulted, Informed) sesuai* standar COBIT 2019. Instrumen yang digunakan meliputi kuesioner berbasis Microsoft Forms, lembar observasi, dan panduan wawancara mendalam.

Untuk menjamin kualitas data, dilakukan uji validitas melalui triangulasi sumber, yaitu membandingkan hasil wawancara, dokumentasi internal (seperti SOP dan laporan sistem), serta hasil observasi langsung di lapangan. Reliabilitas instrumen diuji melalui pengujian internal consistency antar pertanyaan pada kuesioner. Proses pengumpulan data mencakup observasi struktur tata kelola, wawancara dengan stakeholder, serta dokumentasi terhadap kebijakan dan praktik pengelolaan risiko TI yang berjalan. Semua data diklasifikasi berdasarkan domain COBIT 2019 yang relevan, yaitu EDM03 *(Ensured Risk Optimization)* dan APO12 *(Managed Risk)*.

Setelah data dikumpulkan, analisis dilakukan menggunakan Microsoft Excel untuk perhitungan korelasi antar indikator dan pemetaan gap kapabilitas. Teknik analisis yang digunakan adalah gap analysis, yaitu membandingkan antara kondisi kapabilitas aktual dengan level kapabilitas yang diharapkan berdasarkan framework COBIT 2019. Level kapabilitas dinilai berdasarkan lima tingkatan: Performed, Managed, Defined, Quantitatively Managed, dan Optimizing. Hasil analisis menjadi dasar dalam penyusunan rekomendasi perbaikan tata kelola dan mitigasi risiko TI, yang mencakup aspek People, Process, dan Technology, serta penyusunan SOP dan struktur organisasi baru yang relevan dengan tata kelola TI di lingkungan pemerintah kabupaten.



Setelah dilakukan penurunan tujuan hingga ke proses-proses dalam kerangka kerja COBIT 2019, tahap selanjutnya adalah pengumpulan data. Pada tahap ini, instrumen pengumpulan data disusun sesuai dengan metode yang akan digunakan. Data primer diperoleh langsung dari objek penelitian melalui wawancara, observasi lapangan, dan informasi mengenai para informan, seperti individu yang memiliki peran penting dalam tata kelola TI di

Diskominfo pemerintah kabupaten. Instrumen yang digunakan meliputi Google/Microsoft Forms untuk mendukung pelaksanaan kuesioner serta lembar penilaian. Pemetaan responden dalam proses ini dilakukan berdasarkan peran mereka dalam struktur organisasi dan disesuaikan dengan pedoman COBIT 2019 melalui penyusunan tabel RACI (Responsible, Accountable, Consulted, Informed). Tabel ini disusun untuk setiap proses yang dianalisis, dengan mempertimbangkan relevansi dan keterlibatan tiap pihak dalam proses dan prosedur tata kelola teknologi informasi di lingkungan Diskominfo pemerintah kabupaten. a)

Data Sekunder Data ini berupa data-data lain yang tersedia baik dari Peraturan Bupati/Perbup, dokumen laporan bulanan IT, log infrastruktur TI, atau penelitian sejenis yang dilakukan sebelumnya, data berupa grafik, tabel, diagram. Berdasarkan data tersebut kemudian dilakukan evaluasi data untuk memastikan bahwa informasi tersebut bisa menjawab permasalahan dan penelitian yang dilakukan.

HASIL DAN PEMBAHASAN

Profil Penelitian dan Responden

Objek penelitian adalah Diskominfo Kabupaten Tulungagung, instansi yang berperan penting dalam pengelolaan sistem informasi publik dan infrastruktur digital pemerintah daerah. Dalam konteks tata kelola TI, Diskominfo memiliki tanggung jawab strategis yang mencakup pengelolaan risiko, pemeliharaan keamanan data, serta dukungan terhadap sistem layanan publik berbasis teknologi.

Data primer diperoleh melalui penyebaran kuesioner yang dirancang dengan mengacu pada indikator dan aktivitas dalam domain EDM03 dan APO12. Proses pengumpulan data dilakukan menggunakan Microsoft Forms dan lembar observasi yang ditujukan kepada pihak-pihak yang relevan, seperti kepala bidang, staf teknis, serta pejabat struktural yang terlibat dalam pengambilan keputusan terkait sistem TI. Responden dipetakan menggunakan pendekatan RACI (Responsible, Accountable, Consulted, Informed) sebagaimana dianjurkan oleh COBIT 2019 untuk memastikan representasi yang tepat dari peran tiap aktor dalam proses. Total data yang dikumpulkan berasal dari 12 responden kunci yang memiliki peran strategis dan operasional dalam pengelolaan TI di lingkungan Diskominfo. Validasi terhadap jawaban dilakukan melalui triangulasi dengan dokumentasi prosedur dan hasil wawancara langsung. Penelitian ini berfokus pada dua variabel utama:

EDM03 – Ensure Risk Optimization

Domain ini bertujuan memastikan bahwa risiko yang berhubungan dengan TI diidentifikasi, dikelola, dan dioptimalkan agar selaras dengan strategi organisasi. Variabel ini mencakup pengelolaan risiko strategis dan operasional serta penyelarasan terhadap selera risiko organisasi.

APO12 – Managed Risk

Fokus domain ini adalah pada aktivitas manajerial yang mencakup identifikasi, analisis, respons, dan pemantauan risiko TI secara menyeluruh dan terdokumentasi. Pengelolaan risiko dalam domain ini harus berjalan dengan proses yang terdokumentasi dan dapat diaudit.

Masing-masing domain memiliki indikator penilaian yang terbagi dalam lima level kapabilitas, yaitu:

Level 1 (Performed)
Level 2 (Managed)
Level 3 (Defined)
Level 4 (Quantitatively Managed)
Level 5 (Optimizing)

Temuan Hasil Penelitian

1. **Hasil Penilaian Domain EDM03 – *Ensure Risk Optimization***

Berdasarkan hasil analisis, kapabilitas tata kelola risiko dalam domain EDM03 berada pada Level 2 (Managed). Hal ini berarti bahwa proses pengelolaan risiko telah dilakukan secara konsisten dan dapat direproduksi, namun belum terdokumentasi secara formal dan belum sepenuhnya terintegrasi ke dalam kebijakan organisasi.

Temuan penting dalam domain ini meliputi:

a. Tidak adanya prosedur formal dan terdokumentasi mengenai manajemen risiko TI.
b. Pengelolaan risiko masih bersifat reaktif, tergantung pada individu kunci.
c. Dukungan manajemen atas pengelolaan risiko cukup baik, namun belum ditindaklanjuti dengan kebijakan tertulis atau pembentukan struktur formal seperti Komite Risiko TI.
d. Penilaian risiko hanya dilakukan sesekali dan tidak menjadi bagian dari proses bisnis rutin.

2. Hasil Penilaian Domain APO12 – *Managed Risk*

Pada domain APO12, hasil penilaian menunjukkan bahwa proses berada pada Level 3 (Defined). Artinya, proses manajemen risiko telah memiliki struktur yang lebih jelas, terdokumentasi, dan sudah diimplementasikan dalam beberapa kegiatan, meskipun masih perlu penguatan dalam hal pengukuran dan evaluasi secara kuantitatif.

Beberapa poin temuan dalam domain ini antara lain:

a. Tersedianya dokumentasi proses identifikasi dan penilaian risiko, meskipun belum merata di seluruh unit kerja.
b. Terdapat upaya integrasi sistem manajemen risiko dengan dashboard pelaporan utama, namun integrasi tersebut belum sepenuhnya berjalan.
c. Risiko keamanan sistem informasi sudah mulai diidentifikasi, tetapi belum dibarengi dengan pelatihan rutin mengenai kesadaran keamanan bagi seluruh pengguna sistem.
d. Pelaporan risiko masih dilakukan secara manual dan tidak berbasis pada sistem terpadu.

Gap Analysis dan Interpretasi

Dalam proses gap analysis, dibandingkan antara kondisi aktual dengan target level yang diharapkan yaitu Level 4 (Quantitatively Managed) untuk kedua domain. Hasilnya:

EDM03 masih memiliki gap dua level (dari Level 2 ke Level 4), yang menunjukkan bahwa organisasi belum menerapkan pengukuran berbasis data terhadap risiko dan belum melakukan evaluasi berkelanjutan secara sistematis.

APO12 memiliki gap satu level (dari Level 3 ke Level 4), yang berarti meskipun proses sudah terdokumentasi, pengukuran risiko secara kuantitatif dan sistematis belum diterapkan secara konsisten.

Gap ini menunjukkan bahwa perlu dilakukan perbaikan yang signifikan dalam hal dokumentasi prosedur, pembentukan struktur formal, serta peningkatan kualitas dan frekuensi pelaporan risiko.

Berdasarkan hasil analisis dan gap yang ditemukan, berikut adalah rekomendasi strategis:

a. Peningkatan Tata Kelola Risiko (EDM03):
b. Menyusun dan menetapkan prosedur tertulis untuk seluruh siklus manajemen risiko TI.
c. Membentuk Komite Manajemen Risiko TI di tingkat organisasi.
d. Menyelaraskan selera risiko dengan kebijakan organisasi dan integrasikan dalam pengambilan keputusan.

Penguatan Manajemen Risiko (APO12):

a. Melakukan pelatihan kesadaran risiko secara berkala bagi semua pengguna sistem.
b. Meningkatkan kemampuan integrasi pelaporan risiko dengan sistem dashboard utama agar pengawasan lebih responsif.
c. Mengembangkan alat pengukuran kuantitatif risiko untuk memantau tren dan perkembangan risiko secara objektif.

Aspek SDM dan Infrastruktur:

a. Meningkatkan kapasitas teknis dan manajerial SDM di bidang TI dan manajemen risiko.
b. Memastikan bahwa infrastruktur TI mendukung kelancaran proses mitigasi risiko.
c. Dampak dari Risiko TI

Hasil penelitian ini menunjukkan bahwa jika risiko-risiko TI tidak dikelola secara optimal, maka akan berdampak pada tiga hal utama:

a. Efektivitas Organisasi: Proses layanan publik yang bergantung pada sistem TI menjadi tidak optimal.
b. Keberlanjutan Layanan: Risiko sistem down, kebocoran data, dan serangan siber berpotensi mengganggu pelayanan kepada masyarakat.
c. Kepercayaan Publik: Ketidakmampuan pemerintah daerah dalam mengelola risiko TI dapat menurunkan kepercayaan masyarakat terhadap sistem pemerintahan berbasis elektronik.

Pembahasan

Urgensi Penelitian dan Permasalahan yang Dihadapi

Seiring dengan meningkatnya ketergantungan pemerintah daerah terhadap sistem informasi dalam menyelenggarakan layanan publik, muncul tantangan besar dalam mengelola risiko TI yang dapat mengganggu efektivitas operasional dan kualitas layanan. Dalam konteks transformasi digital dan inisiatif smart city, kegagalan dalam manajemen risiko TI dapat menyebabkan gangguan sistem informasi, kebocoran data pribadi masyarakat, serta turunnya kepercayaan publik terhadap pemerintah.

Urgensi penelitian ini dipicu oleh belum optimalnya praktik tata kelola dan manajemen risiko TI di lingkungan Diskominfo. Berdasarkan hasil analisis, domain EDM03 hanya mencapai level kapabilitas 2 (Managed), sementara domain APO12 mencapai level 3 (Defined). Hal ini menunjukkan bahwa meskipun sudah ada proses dasar pengelolaan risiko,

pelaksanaannya belum terdokumentasi secara menyeluruh, belum terukur secara kuantitatif, dan belum menjadi budaya organisasi. Tingginya ketergantungan pada individu kunci tanpa prosedur formal menjadi titik lemah utama yang harus segera diperbaiki.

Penyebab Ketidaktercapaian Level Target

Beberapa faktor utama yang menyebabkan ketidaktercapaian level target dalam domain EDM03 dan APO12 antara lain:

Ketiadaan Prosedur Formal

Tidak adanya kebijakan tertulis atau prosedur resmi terkait pengelolaan risiko TI menyebabkan proses berjalan secara ad hoc. Hal ini membuat kegiatan manajemen risiko tidak dapat direplikasi dan dievaluasi secara objektif.

Ketergantungan pada Individu Kunci

Struktur organisasi belum memiliki Komite Manajemen Risiko atau tim yang secara khusus bertugas menangani risiko TI. Ketergantungan pada perorangan menciptakan ketidakstabilan proses manajemen risiko saat terjadi pergantian personel.

Minimnya Integrasi Sistem

Sistem informasi yang digunakan belum sepenuhnya terintegrasi dengan sistem pelaporan atau dashboard utama yang memungkinkan deteksi dini dan pelaporan otomatis terhadap risiko.

Kurangnya Kesadaran Keamanan TI

Belum ada program awareness atau pelatihan berkelanjutan terkait keamanan informasi yang ditujukan kepada seluruh pengguna sistem, baik internal Diskominfo maupun mitra eksternal.

Ketidaksesuaian Infrastruktur dan SDM

Infrastruktur TI dan kompetensi SDM belum sepenuhnya mendukung implementasi manajemen risiko yang terstandar dan sistematis.

Solusi dan Strategi Peningkatan

Berdasarkan temuan di atas, solusi yang ditawarkan dalam penelitian ini bersifat struktural, prosedural, dan kultural. Strategi ini mengacu pada prinsip-prinsip COBIT 2019 dan best practices dari berbagai penelitian terdahulu.

Penyusunan Prosedur Formal Manajemen Risiko TI

Menyusun SOP dan kebijakan formal terkait siklus manajemen risiko, mulai dari identifikasi, analisis, penilaian, respons, hingga monitoring. Prosedur ini menjadi dasar untuk standarisasi praktik risiko di semua unit kerja.

Pembentukan Struktur Organisasi Formal

Pembentukan Komite Manajemen Risiko TI atau penunjukan unit khusus yang bertanggung jawab langsung dalam perencanaan, pelaksanaan, dan evaluasi manajemen risiko.

Implementasi Sistem Manajemen Risiko Terpadu

Mengintegrasikan sistem pelaporan risiko dengan dashboard utama untuk memudahkan pemantauan, pengawasan, dan pengambilan keputusan berbasis data secara *real-time.*

Pelatihan dan *Awareness* Berkelanjutan

Melaksanakan program pelatihan keamanan TI dan kampanye kesadaran risiko secara rutin bagi seluruh stakeholder agar terbangun budaya organisasi yang peka terhadap risiko.

Penguatan Infrastruktur dan Pengembangan SDM

Mengalokasikan anggaran untuk modernisasi infrastruktur dan peningkatan kapasitas teknis pegawai melalui pelatihan bersertifikasi serta benchmarking dengan pemerintah daerah lain yang lebih maju dalam tata kelola TI.

Dampak Positif Jika Solusi Diimplementasikan

Jika solusi yang diusulkan diimplementasikan secara menyeluruh, beberapa dampak positif yang dapat dicapai antara lain:

Meningkatkan Efektivitas Layanan Publik

Risiko-risiko yang berpotensi mengganggu layanan seperti downtime sistem, kebocoran data, dan keterlambatan pelaporan dapat diminimalkan.

Memperkuat Reputasi Pemerintah Daerah

Dengan sistem risiko yang terkendali, kepercayaan masyarakat terhadap layanan digital pemerintah akan meningkat.

Mendorong Efisiensi Operasional

Proses yang terdokumentasi dan terukur akan mengurangi redundansi dan mempercepat respon terhadap insiden atau potensi risiko.

Mendukung Penerapan *Smart City*

Tata kelola dan manajemen risiko TI yang andal merupakan fondasi penting bagi inisiatif smart city yang berbasis pada integrasi dan keterhubungan sistem.

Penelitian ini memiliki beberapa kesamaan maupun perbedaan signifikan dengan studi-studi terdahulu sebagaimana dirangkum dalam latar belakang. Beberapa studi yang relevan antara lain: Penelitian oleh Setiawan dan Nugroho (2021) di Dinas Kominfo Provinsi Jawa Barat menunjukkan bahwa domain APO12 juga hanya mencapai level 3 karena lemahnya integrasi dan kurangnya indikator pengukuran kuantitatif. Namun, mereka sudah memiliki kebijakan formal tertulis yang belum dimiliki Diskominfo Tulungagung. Studi oleh Priyanto (2022) menyatakan bahwa organisasi sektor publik seringkali menghadapi tantangan dalam menginternalisasi manajemen risiko TI karena tidak adanya keselarasan antara TI dan tujuan strategis. Penelitian ini menegaskan hal tersebut, mengingat tidak ditemukan dokumen yang menghubungkan manajemen risiko TI dengan arah kebijakan digital pemerintah daerah. Penelitian oleh Rahmadani dan Azizah (2020) dalam konteks pemerintah kota menyebutkan bahwa pelatihan keamanan informasi yang berkelanjutan terbukti meningkatkan kepatuhan pegawai terhadap standar pengelolaan data. Ini sejalan dengan solusi yang diusulkan dalam penelitian ini, yakni pentingnya peningkatan awareness secara terus-menerus.

Novelty yang ditawarkan dalam penelitian ini adalah pendekatan spesifik terhadap pemetaan kapabilitas COBIT 2019 dalam konteks pemerintahan daerah kecil-menengah, yang umumnya belum menjadi fokus dalam literatur. Selain itu, penggunaan pendekatan RACI untuk pemetaan peran dalam proses risiko menjadi nilai tambah yang memperkuat struktur analisis dibandingkan penelitian sebelumnya. Secara teoritis, penelitian ini memperkaya pemahaman terhadap penerapan kerangka kerja COBIT 2019 dalam pengelolaan risiko TI di sektor publik. Penelitian ini menunjukkan bahwa meskipun kerangka kerja tersebut dirancang

untuk fleksibilitas, namun perlu adanya kesiapan kelembagaan dalam bentuk prosedur dan struktur organisasi. Secara praktis, hasil penelitian ini dapat digunakan sebagai rujukan bagi pemerintah daerah lainnya untuk melakukan self-assessment terhadap tingkat kapabilitas mereka dalam tata kelola TI, khususnya pada aspek risiko. Dengan memanfaatkan prinsip dan pendekatan COBIT 2019, pemerintah daerah dapat lebih terarah dalam melakukan perbaikan dan integrasi sistem TI.

Pembahasan ini menekankan bahwa tata kelola dan manajemen risiko TI bukan sekadar tanggung jawab teknis, melainkan fondasi strategis bagi tata kelola pemerintahan berbasis digital. Dalam konteks Diskominfo Kabupaten Tulungagung, masih terdapat gap signifikan antara kondisi saat ini dan level kapabilitas yang diharapkan. Namun dengan dukungan manajemen, penyusunan prosedur, pembentukan struktur formal, serta penguatan sistem dan SDM, organisasi ini memiliki potensi besar untuk mencapai kematangan dalam pengelolaan risiko TI. Dampak positif dari implementasi solusi tidak hanya menciptakan efisiensi dan efektivitas layanan, tetapi juga berkontribusi langsung terhadap pembangunan kepercayaan publik, peningkatan daya saing daerah, serta kesiapan menuju transformasi digital nasional. Oleh karena itu, investasi pada manajemen risiko TI adalah investasi strategis yang tidak bisa ditunda.

KESIMPULAN

Berdasarkan hasil analisis risiko TI yang dilakukan pada sistem Tata Kelola Sistem Informasi di Kominfo Pemkab Tulungagung menggunakan kerangka kerja COBIT 2019, dapat disimpulkan bahwa aspek tata kelola (governance) berada pada level kapabilitas 2 (Managed) dalam domain EDM03. Hal ini menunjukkan bahwa pengelolaan risiko TI telah dilakukan dan didukung oleh manajemen, namun belum sepenuhnya terdokumentasi dan terstruktur secara formal. Belum adanya prosedur baku dalam manajemen risiko TI, mulai dari identifikasi, penilaian hingga validasi risiko, menjadi kelemahan utama dalam tata kelola. Selain itu, praktik manajemen risiko masih bergantung pada individu kunci, tanpa adanya komite manajemen risiko yang berfungsi khusus dalam struktur organisasi. Di sisi lain, aspek manajemen (management) berada pada level kapabilitas 3 (Defined) dalam domain APO12, menunjukkan bahwa proses manajemen risiko sudah terdefinisi dan diimplementasikan untuk mengukur serta melaporkan risiko TI, namun masih memerlukan penguatan pada aspek kesadaran keamanan TI dan integrasi sistem yang efisien.

Dampak dari berbagai risiko TI yang teridentifikasi, sebanyak 48 risiko, tidak hanya memengaruhi efektivitas organisasi dan layanan publik, tetapi juga berpotensi menurunkan kepercayaan masyarakat terhadap pemerintah. Oleh karena itu, penerapan manajemen risiko yang efektif menjadi kebutuhan mendesak. Faktor dominan yang memengaruhi keberhasilan implementasi adalah kesiapan sumber daya manusia, disusul oleh kecukupan infrastruktur dan keamanan TI. Strategi mitigasi yang disarankan mencakup peningkatan kesadaran keamanan TI melalui pelatihan rutin, evaluasi infrastruktur penyimpanan data dan pembaruan standar klasifikasi kerahasiaan dokumen, serta penguatan proteksi teknologi dan pencegahan social engineering. Selain itu, diperlukan kerjasama formal dengan konsultan dan vendor sistem untuk menjamin kelancaran integrasi dan operasional sistem secara menyeluruh.

DAFTAR PUSTAKA

Bappenas. (2022). *Rencana Pembangunan Jangka Menengah Nasional 2020–2024*. Kementerian Perencanaan Pembangunan Nasional Republik Indonesia.

Ghamdi, S. R., Alzahrani, A. I., & Razak, A. (2020). *Information security governance: A systematic literature review*. *Journal of Information Security and Applications, 52*, 102480. https://doi.org/10.1016/j.jisa.2020.102480

ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. ISACA.

ITU. (2014). *Measuring the Information Society Report 2014*. International Telecommunication Union.

Kearney. (2015). *ASEAN ICT Investment Trends and Opportunities*. Kearney.

Kemkominfo. (2017). *Inisiatif Smart City di Indonesia*. Kementerian Komunikasi dan Informatika RI.

Nachrowi, D., Sulistika, R., & Yulianto, R. (2020). *Application of COBIT 2019 EDM03 and APO12 domains in risk governance assessment*. *International Journal of Engineering and Technology, 9*(3), 1205–1212.

Priyanto, H. (2022). *Challenges in aligning IT risk management with strategic objectives in public sector institutions*. *Journal of Public Administration and Governance, 12*(2), 45–60.

Lestari, R. B. (2016). Membangun Citra Sebuah Kota Dalam Persaingan Global Melalui City Branding. *Junal Ilmiah STIE Multi Data Palembang*, *5*(1), 68–79.

Mustari, M. (2023). *Teknologi informasi dan komunikasi dalam manajemen pendidikan*. Gunung Djati Publishing Bandung.

Purba, N., Yahya, M., & Nurbaiti, N. (2021). Revolusi industri 4.0: Peran teknologi dalam eksistensi penguasaan bisnis dan implementasinya. *Jurnal perilaku dan strategi bisnis*, *9*(2), 91–98.

Sedyastuti, K. (2018). Analisis pemberdayaan UMKM dan peningkatan daya saing dalam kancah pasar global. *INOBIS: Jurnal Inovasi Bisnis Dan Manajemen Indonesia*, *2*(1), 117–127.

Rahmadani, D., & Azizah, F. (2020). *The impact of continuous information security training on compliance in local government institutions*. *Journal of Cybersecurity Education, 4*(1), 23–35.

Senft, C., & Gallegos, M. (2008). *Top management support and education: Critical success factors in IS security*. *Information Management & Computer Security, 16*(2), 100–115.

Setiawan, A., & Nugroho, Y. (2021). *COBIT 2019 APO12 maturity assessment in provincial Diskominfo*. *Indonesian Journal of Information Systems, 3*(1), 15–25.
UN DESA. (2018). *World Urbanization Prospects: The 2018 Revision*. United Nations Department of Economic and Social Affairs.

Veiga, A., Eloff, J. H. P., & Botha, J. (2020). *Building information security culture: Model and empirical evidence*. *Computers & Security, 94*, 101760. https://doi.org/10.1016/j.cose.2020.101760