Jurnal Informasi, Sains dan Teknologi
Vol. 8 No. 1 Juni 2025
ISSN: 2621-0940, ISSN: 2829-2758, Hal 00-00
DOI: https://doi.org/10.55606/isaintek.v8i1.313

Implementasi COBIT 5 Untuk Manajemen Risiko TI pada UMKM (Studi Kasus: UMKM XYZ)

Steven Dermawan
Universitas Pradita

Afifah Trista Ayunda
Universitas Pradita

Ahmad Abdillah Hisyam
Universitas Pradita

Elianna Katherine Untoro
Universitas Pradita

Alamat: Scientia Business Park, Jl. Gading Serpong Boulevard No.1 Tower 1, Curug Sangereng, Kec. Klp. Dua, Kabupaten Tangerang, Banten 15810
Korespondensi penulis: steven.dermawan@student.pradita.ac.id

Abstract. *COBIT 5 is a governance and management framework for information technology designed to assist organizations in achieving their business objectives through effective and integrated IT management. This study aims to evaluate the IT risk governance capability of MSME XYZ by applying the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimisation) domains of COBIT 5. The research employs both quantitative and qualitative approaches through several stages: problem identification, domain selection, data collection, data analysis, gap analysis, risk analysis, and formulation of recommendations. The evaluation results show that the process capability is at Level 4 (Performed Process), indicating that risk management activities are carried out consistently and in a measurable manner, although improvements are still needed in several areas. The risk analysis identified 8 risk factors, comprising a total of 21 risks: 3 classified as high and 18 as medium. Key recommendations include the development of a documented risk treatment plan, improvements to communication and escalation procedures, and the establishment of a comprehensive risk management policy. Suggested mitigation strategies include the creation of a disaster recovery plan, regular system maintenance, routine data backups, provision of alternative network solutions, and continuous monitoring of financial conditions and hardware performance. By implementing these measures, MSME XYZ is expected to enhance its IT risk governance capabilities in a sustainable manner and be better prepared to face future technological challenges.*

Keywords: *COBIT 5, IT Risk Management, APO12, EDM03, MSME.*

Abstrak. COBIT 5 merupakan kerangka kerja tata kelola dan manajemen teknologi informasi yang dirancang untuk membantu organisasi dalam mencapai tujuan bisnis melalui pengelolaan TI yang efektif dan terintegrasi. Penelitian ini bertujuan mengevaluasi kapabilitas tata kelola risiko TI pada UMKM XYZ dengan menerapkan

Received 30 Maret, 2025; Revised Mei 16, 2025; Accepted Mei 24, 2025
*Steven Dermawan, steven.dermawan@student.pradita.ac.id

domain APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisation*) dari COBIT 5. Metode yang digunakan adalah pendekatan kuantitatif dan kualitatif melalui tahapan identifikasi masalah, penentuan domain, pengumpulan data, analisis data, analisis gap, analisis risiko, dan pemberian rekomendasi. Hasil evaluasi menunjukkan bahwa kapabilitas proses berada pada Level 4 (*Performed Process*), yang mengindikasikan manajemen risiko telah dilaksanakan secara konsisten dan terukur, meskipun masih diperlukan penyempurnaan dalam beberapa aspek. Analisis risiko menemukan 8 faktor risiko dengan total 21 risiko, terdiri dari 3 risiko tinggi dan 18 risiko sedang. Rekomendasi utama yang diajukan meliputi penyusunan rencana penanganan risiko terdokumentasi, perbaikan prosedur komunikasi dan eskalasi, serta pembentukan kebijakan manajemen risiko yang komprehensif. Langkah mitigasi yang disarankan antara lain pembuatan *disaster recovery plan*, pemeliharaan sistem berkala, *backup* data rutin, penyediaan solusi jaringan alternatif, serta pemantauan kondisi keuangan dan perangkat keras. Dengan implementasi langkah-langkah tersebut, UMKM XYZ diharapkan mampu meningkatkan kapabilitas tata kelola risiko TI secara berkelanjutan dan lebih siap menghadapi tantangan teknologi di masa depan.

Kata kunci: COBIT 5, Manajemen Risiko TI, APO12, EDM03, UMKM.

LATAR BELAKANG

Dewasa ini, penggunaan teknologi informasi (TI) telah menjadi salah satu pilar utama dalam mendukung operasional bisnis, termasuk pada sektor Usaha Mikro, Kecil, dan Menengah (UMKM). Pemanfaatan TI oleh UMKM tidak hanya memberikan kemudahan dalam pengelolaan data dan proses bisnis, tetapi juga memperluas jangkauan pasar serta meningkatkan efisiensi (Octiva et al., 2024). Namun, seiring dengan meningkatnya ketergantungan terhadap TI, risiko yang terkait dengan penggunaannya juga semakin kompleks, seperti ancaman keamanan siber, kerusakan sistem, dan pelanggaran terhadap kebijakan atau standar yang berlaku (Alfi et al., 2023)

Risiko adalah kondisi yang tidak dapat dihindari dan berpotensi memberikan dampak negatif terhadap pencapaian tujuan organisasi (Hasanah et al., 2024). Oleh karena itu, pengelolaan risiko menjadi aspek penting bagi perusahaan untuk melindungi dan menciptakan nilai. Manajemen risiko adalah proses untuk mengenali, mengevaluasi, dan mengembangkan strategi mitigasi serta komunikasi risiko TI yang dapat merugikan atau berdampak negatif pada organisasi. Manajemen risiko mencakup aktivitas identifikasi, pengukuran, dan evaluasi ancaman yang mungkin timbul dalam operasi perusahaan (Kurniasih & Tobing, 2022). Dengan pengelolaan yang baik, dampak buruk risiko dapat diminimalkan, dihindari, ditanggung, atau dialihkan ke pihak lain (Lisnawati et al., 2023). Dalam konteks ini, UMKM XYZ sebagai UMKM

yang bergerak di bidang *food and beverage* menghadapi tantangan dalam mengelola risiko TI yang dapat mempengaruhi kelangsungan operasional mereka.

Framework COBIT 5 dipilih sebagai pendekatan dalam analisis manajemen risiko TI ini karena menyediakan panduan yang komprehensif untuk mengidentifikasi, menilai, dan mengelola risiko teknologi informasi secara terstruktur (ISACA, 2013). Dalam penelitian ini, domain APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimization*) dari COBIT 5 digunakan karena sangat relevan dalam konteks manajemen risiko TI. Domain APO12 memberikan panduan untuk memastikan bahwa risiko yang terkait dengan TI dikelola dengan baik melalui proses identifikasi, evaluasi, dan mitigasi risiko secara proaktif. Fokus domain ini adalah membantu organisasi dalam mengelola ancaman TI yang dapat berdampak pada pencapaian tujuan bisnis (Fatimah & Ichwani, 2020). Sementara, domain EDM03 mendukung optimalisasi pengelolaan risiko TI dengan memastikan risiko tersebut ditangani dalam kerangka tata kelola yang efektif dan mendukung strategi organisasi secara keseluruhan (Fajri et al., 2023).

Selain itu, *framework* ini menyediakan serangkaian alat yang membantu organisasi dalam menjembatani kesenjangan antara kebutuhan pengendalian, tantangan teknis, dan risiko bisnis (Mutia & Nur'ainy, 2020). Alat-alat ini memungkinkan organisasi untuk mengevaluasi efektivitas pengendalian yang ada, mengidentifikasi celah yang perlu diperbaiki, serta menyesuaikan pendekatan pengelolaan risiko sesuai dengan tingkat kompleksitas dan kapabilitas teknologi yang dimiliki. Dengan menggunakan pendekatan ini, UMKM XYZ diharapkan dapat meningkatkan efisiensi tata kelola TI, mengidentifikasi ancaman yang berpotensi mengganggu bisnis, serta memastikan strategi mitigasi risiko selaras dengan tujuan bisnis mereka.

Melalui penelitian ini, diharapkan dapat diberikan pemahaman yang lebih mendalam mengenai implementasi COBIT 5, khususnya pada domain **APO12** dan **EDM03**, dalam manajemen risiko TI pada UMKM XYZ guna memberikan solusi praktis dan relevan untuk meningkatkan kesiapan UMKM dalam menghadapi tantangan di era digital.

KAJIAN TEORITIS

Peneliti melakukan kajian terhadap berbagai studi terkait untuk menganalisis metode dan hasil yang telah digunakan, sekaligus mengidentifikasi persamaan,

perbedaan, serta celah penelitian yang dapat menjadi dasar bagi pengembangan studi ini.

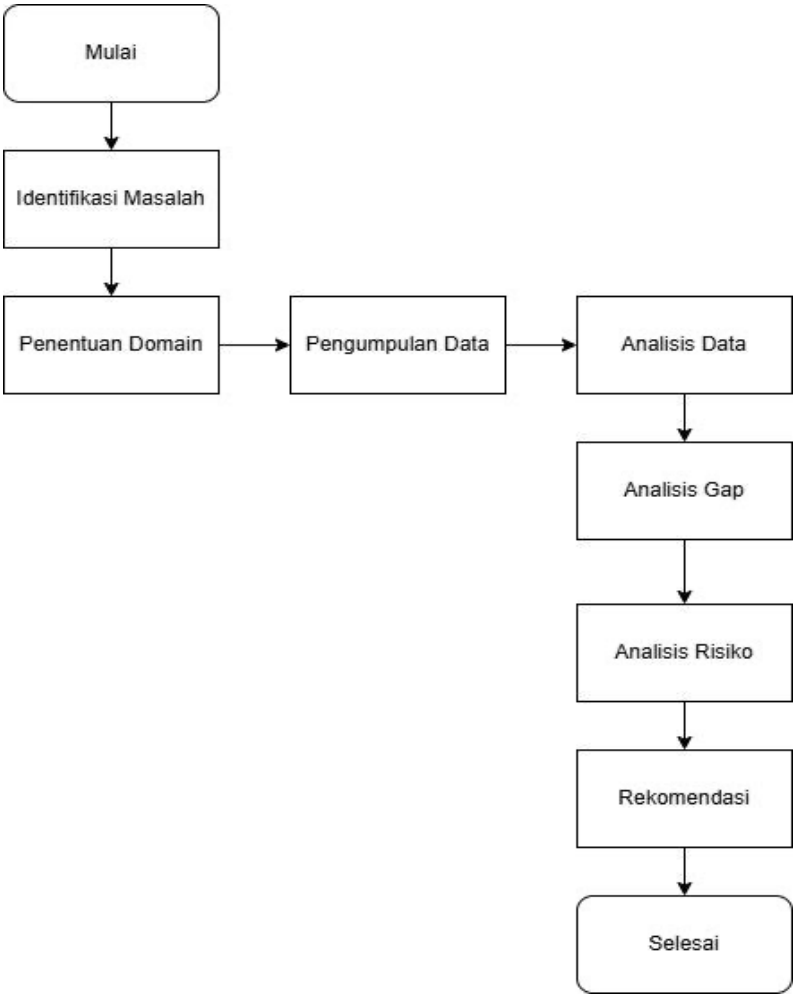
Pertama, penelitian (Wattimena & Tanaamah, 2021) terkait manajemen risiko pada Sistem Informasi Perpustakaan UKSW. Mereka menggunakan domain APO12. Data dikumpulkan melalui wawancara kepada narasumber. Hasil analisis menunjukkan bahwa proses berada pada level 1 dengan kriteria *Partially Achieved*. Untuk mencapai level 2, terdapat empat rekomendasi: (1) membentuk manajemen khusus untuk analisis dan pengendalian risiko di luar BTSI, (2) meninjau proses komunikasi risiko agar penanganan tidak terlambat, (3) menambahkan kriteria efektivitas pengendalian risiko untuk mengukur keberhasilannya dalam mengurangi risiko, dan (4) menyusun dokumen identifikasi risiko serta langkah penanganannya.

Kedua, penelitian (Ambarita & Cholil, 2022) terkait manajemen risiko Divisi Sistem Informasi Pada Universitas Bina Insan Menggunakan Framework Cobit 5. Mereka menggunakan domain APO12. Evaluasi yang dilakukan melalui kuesioner, wawancara, dan observasi menunjukkan bahwa level kapabilitas domain APO12 berada pada level 1, sementara target yang diinginkan adalah level 3, menghasilkan gap sebesar 2 level. Penerapan manajemen risiko TI dengan menggunakan kerangka kerja COBIT 5 menunjukkan kapabilitas pada level 2, yaitu *performed process*. Ini berarti bahwa setiap proses yang diimplementasikan telah mencapai tujuan yang ditetapkan.

Ketiga, penelitian (Rahmadhania et al. 2023) pada tata kelola *IT Risk Management* SMK Telkom Jakarta. Mereka menggunakan domain EDM03 dan APO12. Data diperoleh melalui wawancara dan observasi, yang digunakan untuk menganalisis risiko, serta mengidentifikasi dan membuat mitigasi risiko. Hasil analisis menunjukkan bahwa EDM03 berada pada level 1, sementara APO12 pada level 2, dengan nilai *risk composite* masing-masing 58% (medium) untuk EDM03 dan 54% (medium) untuk APO12. Rekomendasi mitigasi ini dapat digunakan untuk memperbaiki manajemen risiko TI di SMK Telkom Jakarta.

Ketiga penelitian tersebut membuktikan bahwa COBIT 5 merupakan *framework* yang relevan untuk analisis risiko, menyediakan landasan dalam mengevaluasi efektivitas manajemen risiko pada implementasi TI UMKM XYZ.

METODE PENELITIAN



Gambar 1. Metodologi Penelitian

Penelitian ini menggunakan metode kuantitatif dan kualitatif untuk menelaah tingkat kapabilitas dari implementasi TI yang ada serta risiko-risiko yang mungkin timbul. Langkah-langkah penelitian terlampir sebagai berikut.

Identifikasi Masalah

Langkah pertama dalam penelitian ini adalah menelaah, menganalisis, dan mengidentifikasi masalah yang terjadi pada implementasi TI UMKM XYZ. Langkah selanjutnya adalah mengeksplorasi cara-cara untuk menyelesaikan permasalahan tersebut.

Penentuan Domain

Framework yang akan digunakan untuk menganalisis risiko TI adalah COBIT 5. Domain yang dipilih pada *framework* ini adalah EDM03 dan APO12.

Pengumpulan Data

Tahapan ini dilakukan beberapa proses:

1. Observasi

   Observasi dilakukan untuk mendapatkan gambaran umum mengenai implementasi TI pada UMKM XYZ. Aktivitas ini melibatkan kunjungan langsung untuk melihat proses operasional TI secara langsung.

2. Wawancara

   Wawancara dilakukan untuk menggali informasi lebih dalam mengenai permasalahan yang ada pada implementasi TI UMKM XYZ. Proses ini melibatkan pihak-pihak teknis yang bertugas menangani permasalahan yang sering muncul dalam penggunaan sistem tersebut.

3. Kuesioner

   Kuesioner disusun berdasarkan aktivitas yang berkaitan dengan proses TI. Setelah menyusun daftar pertanyaan, narasumber dipilih menggunakan RACI c*hart* untuk mempermudah distribusi kuesioner. Narasumber dalam penelitian ini adalah Business Process Manajer dari UMKM XYZ

Analisis Data

Pada tahap ini dilakukan analisis data kuesioner menggunakan Skala Likert. Skala ini digunakan untuk mengukur opini atau persepsi terhadap suatu kondisi tertentu (Auliyah et al., 2022). Penjelasan mengenai nilai pada Skala Likert dapat dilihat pada tabel berikut.

Tabel 1.Skala likert

Jawaban	Nilai
Sangat Setuju	5
Setuju	4
Netral	3
Tidak Setuju	2
Sangat Tidak Setuju	1

a. Menghitung jawaban dari kuesioner

$$C = \frac{H}{JR} \times 100\%$$

Keterangan:

C = Rekapitulasi jawaban kuesioner

H = Jumlah jawaban kuesioner

JR = Jumlah responden

b. Menghitung nilai *capability level*

$$Nk = \frac{(Nr \times L0)+(Nr \times L1)+(Nr \times L2)+(Nr \times L3)+(Nr \times L4)+(Nr \times L5)}{100}$$

Keterangan:

Nk = Nilai kapabilitas

Nr = Nilai rekapitulasi

L = Level 0 sampai 5

Setelah dilakukan perhitungan hasil kuesioner dan *capability* level dan menghasilkan nilai bilangan bulat, hasil perhitungan akan dilakukan pembulatan dengan skala sebagai berikut:

Tabel 2. Skala Pembulatan Indeks

Skala Pembulatan	Tingkat Model Kapabilitas
4,51 – 5,00	*5 - Optimising Process*
3,51 – 4,50	*4 - Predictable Process*
2,51 – 3,50	*3 - Established Process*
1,51 – 2,50	*2 - Managed Process*
0,51 – 1,50	*1 - Performed Process*
0 – 0,50	*0 - Incomplete Process*

Sumber: (Melani et al., 2021)

Penelitian ini menggunakan Tingkat *Maturity* Model *framework* yang dimiliki COBIT 5 yang berasal dari ISACA pada tahun 2013 untuk mengukur tingkat kematangan pada setiap domain.

Tabel 3. Interpretasi Kapabilitas

Tingkat Model Kapabilitas	Kapabilitas
5 - Optimising Process	Proses yang dapat diprediksi terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan yang diproyeksikan
4 - Predictable Process	Proses yang ditetapkan sekarang beroperasi dalam batas yang ditentukan untuk mencapai hasil prosesnya
3 - Established Process	Proses yang dikelola sekarang diimplementasikan menggunakan proses yang ditentukan yang mampu mencapai hasil prosesnya
2 - Managed Process	Proses yang dilakukan sekarang diimplementasikan dengan cara yang terkelola (direncanakan, dipantau, dan disesuaikan) dan produk kerjanya ditetapkan, dikendalikan, dan dipelihara dengan tepat.
1 - Performed Process	Proses yang diimplementasikan mencapai tujuan prosesnya
0 - Incomplete Process	Proses tidak dilaksanakan atau gagal mencapai tujuan prosesnya. Pada tingkat ini, ada sedikit atau tidak ada bukti pencapaian sistematis dari tujuan proses

Analisis Gap

Langkah selanjutnya setelah skala pembulatan indeks adalah melakukan analisis Gap. Nilai Gap dihitung menggunakan rumus berikut:

Gap = Tingkat Kapabilitas yang Diharapkan − Tingkat Kapabilitas yang Ada (4)

Tingkat yang diharapkan diperoleh dari hasil kuesioner dengan cara memprediksi tingkat kapabilitas berdasarkan opsi jawaban yang paling banyak dipilih dalam kuesioner tersebut.

Analisis Risiko

Setelah melakukan analisis gap, penulis juga menganalisis risiko-risiko dalam implementasi TI pada UMKM XYZ. Risiko akan dikategorikan menjadi risiko tinggi, sedang, dan rendah. Kategori tersebut didapatkan dari matrik risiko yang terlampir dalam gambar.

Tabel 4. Matrik Resiko

KEMUNGKINAN/ LIKELIHOOD		DAMPAK/IMPACT				
		1	2	3	4	5
		Tidak Signifikan	Kecil	Sedang	Besar	Katastropik
Sangat Jarang	1	M	M	H	H	H
Kemungkinan Kecil	2	L	M	M	H	H
Kemungkinan Sedang	3	L	L	M	M	H
Kemungkinan Besar	4	L	L	M	M	H
Sering Terjadi	5	L	L	L	M	H

Keterangan Warna:

H : *High Risk* (Risiko Tinggi)

M : *Moderate* Risk (Risiko Sedang)

L : *Low Risk* (Risiko Rendah)

Rekomendasi

Rekomendasi disusun berdasarkan hasil analisis risiko yang telah dilakukan. Rekomendasi akan disusun berdasarkan tingkat kepentingan dari risiko untuk diselesaikan.

HASIL DAN PEMBAHASAN

Identifikasi Arsitektur Teknologi Informasi

Dalam implementasi TI di UMKM XYZ, terdapat tiga sistem yang digunakan, yaitu sistem POS, sistem purchasing, dan sistem absensi. *Hardware* yang digunakan meliputi *device* kasir (tablet, printer struk), *device* pegawai, CCTV, wifi, dan speaker. Data yang beredar berupa data keuangan, data pegawai, dan data inventori/bahan masakan.

Hasil Temuan

Hasil temuan didapatkan dari observasi, wawancara, dan pemberian checklist kuesioner. Data yang didapatkan mengenai temuan-temuan dijabarkan sebagai berikut:

Tabel 5. Hasil Temuan

Nama Domain	Hasil Temuan
APO12.01	Organisasi mampu mengakomodasi berbagai jenis kejadian dan kategori risiko IT yang berbeda dalam proses pengelolaan risiko.
APO12.02	Cakupan analisis risiko pada organisasi ditentukan secara tepat, mempertimbangkan semua faktor risiko yang relevan dan nilai kritikalitas aset bisnis.
APO12.03	Organisasi belum mengelompokkan skenario risiko yang ada berdasarkan kategori, lini bisnis, dan area fungsional. Risiko pada organisasi telah terorganisir dan dikelompokkan secara rapi untuk mempermudah analisis lebih lanjut.
APO12.04	Pengambil keputusan diberikan pemahaman mengenai skenario terburuk dan skenario paling mungkin terkait risiko pada implementasi TI.
APO12.05	Implementasi TI pada organisasi memiliki keseimbangan antara pengurangan risiko dan pencapaian peluang strategis.

APO12.06	Organisasi belum memiliki rencana yang terdokumentasi secara rinci untuk langkah-langkah spesifik yang harus diambil jika terjadi insiden risiko yang signifikan.
EDM03.01	Organisasi sudah menetapkan tingkat risiko TI yang dapat diterima, termasuk risiko terkait keamanan data, privasi, dan integritas informasi, untuk mendukung pencapaian tujuan dalam implementasi teknologi informasi. Proses formal belum diterapkan untuk secara berkala meninjau dan mengkomunikasikan risiko yang dapat diterima tersebut.
EDM03.02	Organisasi telah mengembangkan budaya yang menekankan pentingnya kesadaran terhadap risiko TI dalam implementasi teknologi informasi. Karyawan didorong untuk secara proaktif mengidentifikasi risiko, peluang, dan potensi dampak bisnis yang terkait dengan penggunaan TI di dalam organisasi.
EDM03.03	Setiap isu yang muncul dalam pengelolaan risiko TI dilaporkan secara transparan kepada pihak yang bertanggung jawab. Prosedur telah disusun untuk memastikan pelaporan masalah manajemen risiko dilakukan secara tepat waktu sehingga tindakan yang diperlukan dapat segera diambil. Prosedur telah disusun untuk memastikan pelaporan masalah manajemen risiko dilakukan secara tepat waktu sehingga tindakan yang diperlukan dapat segera diambil.

Hasil Tingkat Kapabilitas

Hasil dari perhitungan tingkat kapabilitas dijabarkan dalam tabel berikut ini.

Tabel 6. Nilai kapabilitas masing-masing domain

Domain	*Current Maturity*	*Capability Level*	*Expected Target*
APO12	3,83	4	5
EDM03	4	4	5

Berdasarkan hasil perhitungan kuesioner dengan total 9 pertanyaan yang terlampir pada tabel, didapati bahwa seluruh subdomain, yaitu EDM03 dan APO12 berada pada level 4 (*Predictable Process*). Level ini menunjukkan bahwa proses dalam

subdomain tersebut telah terdefinisi dengan baik, dapat diprediksi, dan dijalankan secara konsisten sesuai standar yang telah ditetapkan. Pada tingkat ini, organisasi mampu mengelola dan memantau proses dengan menggunakan pengukuran kuantitatif yang jelas, sehingga menghasilkan hasil yang terukur dan dapat diandalkan. Hal ini mencerminkan tingkat kedewasaan yang tinggi dalam pengelolaan proses, di mana risiko dapat diantisipasi, dan tindakan perbaikan dilakukan secara proaktif untuk memastikan keselarasan dengan tujuan organisasi.

Gap *Analysis*

Tabel 7. Analisis Gap Masing-Masing Domain

Domain	*Current Maturity*	Gap	*Expected Target*
APO12	3,83	1,17	5
EDM03	4	1	5

Dalam evaluasi tingkat kematangan dari setiap domain tersebut, menunjukkan hasil pada level 4. Hasil ini memberikan suatu tanda bahwa proses-proses yang ada pada implementasi TI telah berjalan dengan baik. Hal itu tentu membuahkan fondasi yang solid bagi organisasi. Akan tetapi, masih terdapat gap yang ada. Gap yang paling besar ada pada sub domain APO12 (*Manage Risks*), gap yang paling kecil ada pada sub domain EDM03 (*Ensure Risk Optimization).* Maka, untuk mengoptimalkan kinerja, UMKM XYZ perlu melakukan langkah-langkah perbaikan dan peningkatan kualitas dan kinerja TI.

Dalam rangka meningkatkan keandalan dan efisiensi dari implementasi TI, beberapa rekomendasi telah dirumuskan untuk mengatasi permasalahan yang ada.

Tabel 8. Rekomendasi Gap Masing-Masing Domain

No	Domain	Rekomendasi
1	APO12	Organisasi perlu menyusun rencana penanganan risiko yang terdokumentasi dengan jelas, mencakup langkah-langkah spesifik jika terjadi insiden signifikan, serta dilengkapi dengan prosedur komunikasi dan eskalasi. Analisis risiko harus diperluas dengan dikelompokkan berdasarkan kategori, lini bisnis, dan area fungsional agar lebih mudah dianalisis dan ditindaklanjuti.
2	EDM03	Organisasi perlu menetapkan tingkat risiko TI yang dapat diterima,

termasuk keamanan data, privasi, dan integritas informasi, sebagai acuan dalam pengelolaan risiko TI. Hal ini dapat diwujudkan melalui kebijakan manajemen risiko yang terdokumentasi, penetapan *Risk Appetite* dan *Risk Tolerance*, serta implementasi kerangka kerja seperti ISO 27001 atau COBIT. Monitoring risiko dengan alat seperti SIEM dan penggunaan *key risk indicators* (KRIs) akan memastikan risiko terkendali dan selaras dengan tujuan organisasi.

Identifikasi Risiko

Dari hasil observasi yang ada, berikut adalah tabel identifikasi risiko serta dampak yang mungkin akan terjadi dalam implementasi TI di UMKM XYZ.

Tabel 9. Identifikasi Risiko

Faktor Risiko	Kode Risiko	Risiko	Nilai Likelihood	Nilai Impact	Dampak
Bencana Alam	R01	Gempa Bumi	1	5	Kerusakan fisik perangkat dan server, gangguan operasional sistem.
	R02	Kebakaran	1	5	Kehilangan data, kerusakan perangkat keras, berhentinya layanan.
Human Error	R03	Human error	3	3	Kesalahan input data, kerusakan sistem, atau hilangnya data penting.
	R04	Kesalahan Konfigurasi Sistem	3	3	Sistem gagal berjalan optimal, *downtime*, kehilangan data.
Keamanan Akses/Data/ Siber	R05	Hak akses sistem yang disalahgunakan	3	4	Penyalahgunaan sistem, pencurian data, manipulasi transaksi.
	R06	Mantan karyawan/*user* memiliki akses	3	4	Penyalahgunaan sistem, kebocoran informasi, sabotase layanan.
	R07	Serangan *hacker*	4	4	Pencurian/manipulasi data, reputasi rusak, gangguan

					sistem.
	R08	Kebocoran data	3	4	Informasi terekspos, kerugian finansial, pelanggaran hukum.
	R09	Fraud dan Pembayaran Palsu	3	4	Kerugian finansial, merusak integritas sistem.
Operasional Sistem	R10	Server *down*	4	4	Operasional sistem terhenti, kehilangan transaksi, produktivitas menurun.
	R11	Kegagalan *backup* data	3	4	Kehilangan data permanen, layanan terganggu.
	R12	Kegagalan Transaksi	4	3	Pembayaran terganggu, pendapatan berkurang, kepercayaan menurun.
	R13	Terjadi bug/malfungsi sistem	3	3	Data tidak tercatat, gangguan dalam pemesanan stok barang, transaksi penjualan terganggu,
Infrastruktur Perangkat	R14	Kerusakan *Hardware*	4	4	Operasional sistem berhenti, kehilangan data, biaya penggantian perangkat.
	R15	Pemalsuan data	3	4	Data tidak valid, laporan bisnis rusak, keputusan salah.
	R16	Data corrupt	4	4	Data tidak dapat digunakan, membutuhkan pemulihan sistem.
	R17	Kerusakan *Software*	4	4	Sistem tidak berfungsi, proses operasional terhambat.
	R18	Kehilangan perangkat *hardware*	3	3	Potensi kebocoran data, operasional terganggu, biaya penggantian.

Manajemen Sumber Daya Manusia	R19	Ketergantungan pada satu administrator	4	3	Administrator tidak tersedia, pemeliharaan sistem terganggu.
Ketergantungan Eksternal	R20	Ketergantungan pada pihak ketiga	4	3	Vendor tidak optimal, operasional bisnis terhambat.
Infrastruktur Jaringan	R21	Kualitas jaringan yang kurang baik	5	3	Koneksi terganggu, operasional dan transaksi sistem terganggu.

Mitigasi Risiko

Dari analisis matriks risiko, didapatkan risiko kecil, sedang, dan besar. Hasil analisis risiko dan mitigasi risiko terlampir dalam tabel berikut.

Tabel 10. Mitigasi Risiko

Kode Risiko	Nama Risiko	Tingkat Risiko	Strategi/Mitigasi Risiko
R01	Gempa Bumi	*High*	- Menyediakan *backup data* ke cloud atau server eksternal. - Membuat rencana darurat usaha (*disaster recovery plan*). - Monitoring kondisi bangunan dan asuransi bencana.
R02	Kebakaran	*High*	- Menyediakan alat pemadam kebakaran. - *Backup data* ke cloud secara rutin. - Asuransi usaha untuk perlindungan kerugian akibat kebakaran.
R03	*Human Error*	*Medium*	- Memberikan pelatihan rutin bagi karyawan. - Membuat SOP untuk input data dan operasional. - Monitoring kegiatan harian secara berkala.
R04	Kesalahan Konfigurasi Sistem	*Medium*	- Menggunakan jasa teknisi profesional. - Melakukan audit sistem IT secara berkala. - Dokumentasi lengkap konfigurasi sistem untuk pengawasan.
R05	Hak Akses Disalahgunakan	*Medium*	- Membatasi akses hanya pada karyawan yang berwenang. - Monitoring akses sistem dengan log aktivitas. - Audit berkala pada penggunaan akses.

R06	Mantan Karyawan/*User* memiliki akses	*Medium*	- Segera menonaktifkan akun akses setelah pemutusan kerja. - Audit berkala terhadap hak akses pengguna. - Monitoring aktivitas akun sistem secara *real-time*.
R07	Serangan *Hacker*	*Medium*	- Menggunakan *firewall* dan antivirus yang kuat. - Melakukan update rutin pada sistem keamanan. - Monitoring aktivitas mencurigakan pada sistem.
R08	Kebocoran Data	*Medium*	- Melindungi data pelanggan dengan enkripsi. - Penerapan kebijakan Data *Loss Prevention* (DLP). - Monitoring transfer dan akses data secara berkala.
R09	Fraud dan Pembayaran Palsu	*Medium*	- Menggunakan metode pembayaran yang aman (QRIS, *virtual account*). - Monitoring transaksi keuangan harian. - Audit laporan keuangan secara rutin.
R10	Server Down	*Medium*	- Menggunakan layanan server dengan uptime tinggi. - Monitoring performa server secara berkala. - Menyiapkan server cadangan atau offline-mode sistem sementara.
R11	Kegagalan *Backup* Data	*Medium*	- *Backup data* secara berkala ke *cloud* atau perangkat eksternal. - Uji coba pemulihan data secara berkala. - Monitoring status *backup* untuk memastikan data tersimpan.
R12	Kegagalan Transaksi	*Medium*	- Menyediakan beberapa metode transaksi alternatif. - Monitoring sistem transaksi untuk mendeteksi error. - Bekerja sama dengan penyedia layanan pembayaran terpercaya.
R13	Terjadi bug/malfungsi sistem	*Medium*	- Melakukan maintenance rutin untuk mencegah bug dari sistem yang sudah berjalan. - Menyediakan tim IT *on-call* untuk perbaikan segera jika terjadi malfungsi. - Menjalankan sistem *backup* otomatis untuk melindungi data transaksi, absensi, dan pemesanan.

			- Monitoring sistem secara *real-time* menggunakan *tools* otomatis.
R14	Kerusakan *Hardware*	*Medium*	- Menyediakan perangkat cadangan untuk operasional. - Monitoring kondisi *hardware* secara rutin. - Asuransi perlindungan perangkat usaha.
R15	Pemalsuan Data	*Medium*	- Validasi dokumen secara berkala. - Menggunakan sistem verifikasi data pelanggan atau supplier. - Monitoring laporan keuangan untuk deteksi kejanggalan.
R16	*Data Corrupt*	*Medium*	- Backup data dengan validasi integritas. - Monitoring database secara berkala untuk mencegah kerusakan. - Menggunakan *software* berkualitas untuk pengelolaan data.
R17	Kerusakan *Software*	*Medium*	- Menggunakan software yang legal dan terpercaya. - Update *software* secara berkala. - Monitoring error log untuk deteksi dini masalah *software*.
R18	Kehilangan Perangkat Hardware	*Medium*	- Menggunakan kebijakan inventarisasi perangkat. - Menyediakan perangkat cadangan. - Monitoring lokasi dan penggunaan perangkat oleh karyawan.
R19	Ketergantungan pada satu Administrator	*Medium*	- Melatih beberapa karyawan untuk memahami sistem. - Membuat SOP pemeliharaan sistem. - Monitoring tugas administrator untuk meminimalisir risiko ketergantungan.
R20	Ketergantungan pada Pihak Ketiga	*Medium*	- Menyusun kontrak kerjasama yang kuat dengan SLA. - Monitoring kinerja vendor atau pihak ketiga. - Menyediakan opsi vendor cadangan jika layanan terganggu.
R21	Kualitas Jaringan Kurang Baik	*High*	- Menggunakan provider jaringan yang andal. - Monitoring kualitas koneksi secara berkala. - Menyediakan solusi jaringan alternatif seperti mobile hotspot atau backup ISP.

KESIMPULAN DAN SARAN

Berdasarkan hasil penilaian tingkat kapabilitas tata kelola risiko teknologi informasi pada UMKM XYZ, khususnya pada domain APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisation*), kondisi saat ini telah mencapai Level 4 (*Performed Process*). Hal ini menunjukkan bahwa proses manajemen risiko telah berjalan baik, namun masih memerlukan peningkatan agar lebih optimal. Rekomendasi utama adalah menyusun rencana penanganan risiko yang terdokumentasi dengan langkah-langkah spesifik jika terjadi insiden signifikan, serta dilengkapi dengan prosedur komunikasi dan eskalasi yang jelas. Selain itu, diperlukan kebijakan manajemen risiko tertulis sebagai panduan formal dalam mengelola risiko di masa depan. Analisis risiko yang dilakukan mengidentifikasi 8 faktor risiko dengan total 21 risiko, terdiri dari 3 risiko *high* dan 18 risiko *medium*. Penyusunan dokumentasi yang lebih baik akan memperkuat kemampuan UMKM XYZ dalam mengelola risiko dengan efektif.

Langkah antisipatif yang direkomendasikan mencakup penyusunan rencana darurat usaha (*disaster recovery plan*) untuk menghadapi potensi gangguan operasional. Selain itu, *maintenance* sistem secara rutin diperlukan untuk mencegah bug, serta *backup data* berkala guna menghindari kehilangan informasi penting. UMKM XYZ juga disarankan menyediakan solusi jaringan alternatif seperti *mobile hotspot* atau *backup ISP* untuk menjaga konektivitas. Upaya lain yang perlu dilakukan adalah monitoring laporan keuangan secara berkala guna mendeteksi kejanggalan, serta pemantauan kondisi *hardware* agar perangkat tetap optimal. Dengan implementasi langkah-langkah tersebut, UMKM XYZ diharapkan dapat meningkatkan kapabilitas tata kelola risiko dan menghadapi berbagai tantangan dengan lebih siap. Optimalisasi manajemen risiko akan mendukung keberlangsungan operasional yang lebih stabil dan efisien di masa depan.

DAFTAR REFERENSI

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5. https://doi.org/10.7454/jkskn.v6i2.10082

Ambarita, R. M., & Cholil, W. (2022). Pengukuran Tingkat Risiko Terhadap Kapabilitas Tata Kelola Teknologi Informasi Berdasarkan Framework COBIT 5. *Jurnal Tekno Kompak*, *16*(1), 97. https://doi.org/10.33365/jtk.v16i1.1441

Auliyah, R., Jaya, J. N. U., & Surmiati, S. (2022). Efektivitas Penerapan Sistem Informasi Debitur (SID) BRI Dalam Kebijaksanaan Pemberian Kredit Menggunakan COBIT 5 Domain DSS (Deliver, Service, Support). *JURIKOM (Jurnal Riset Komputer)*, *9*(2), 328. https://doi.org/10.30865/jurikom.v9i2.4035

Fajri, A., Safaat, N. H., & Affandes, M. (2023). Analisis Manajemen Risiko TI Menggunakan Framework COBIT 5 Domain APO12 dan EDM03. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *4*(3), 1523–1530. https://doi.org/10.30865/klik.v4i3.1396

Fatimah, L. W. N. F., & Ichwani, A. (2020). TATA KELOLA TEKNOLOGI INFORMASI DOMAIN APO12 MENGGUNAKAN FRAMEWORK COBIT 5. *JIK: Jurnal Ilmu Komputer*, *5*(1), 31–41. https://doi.org/10.30656/jsii.v7i1.2027

Hasanah, U., Islam, U., Sumatera, N., Perusahaan, R., Perusahaan, M. K., & History, A. (2024). PERAN MANAJEMEN RISIKO DALAM MENINGKATKAN KINERJA PERUSAHAAN. *Musytari : Neraca Manajemen, Akuntansi, Dan Ekonomi*, *10*(5), 1–8.

ISACA. (2013). COBIT 5 for risk. ISACA. https://books.google.co.id/books/about/COBIT_5_for_Risk.html?id=k_hgAwAAQBAJ

Kurniasih, F., & Tobing, A. N. L. (2022). Risk Analysis in The Business Process Management And Recording Electricity Costs (Case Study in an Oil and Gas Company in Indonesia). *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *3*, 21089–21104.

Lisnawati, T., Hussaen, S., & Nuridah, S. (2023). Manajemen Risiko dalam Bisnis E-commerce : Mengidentifikasi ,. *Jurnal Pendidikan ...*, *7*, 8252–8259. https://repository.bsi.ac.id/repo/files/372665/download/11.-Publikasi-Jurnal.pdf

Melani, A. A., Pratama, A. Y., & Anshari, M. F. (2021). Penerapan COBIT-5 Domain DSS01 dan DSS05 Untuk Mengukur Kualitas Tata Kelola Sistem di KSPPS BMT Unit 068-Sampit. *Journal of Information System Research (JOSH)*, *2*(4), 293–302. https://doi.org/10.47065/josh.v2i4.824

Mutia, N., & Nur'ainy, R. (2020). It Governance: Measure Capability Level Using Cobit 5 Framework. *Jurnal Ilmiah Ekonomi Bisnis*, *25*(2), 97–110. https://doi.org/10.35760/eb.2020.v25i2.2609

Octiva, C. S., Haes, P. E., Fajri, T. I., Eldo, H., & Hakim, M. L. (2024). Implementasi Teknologi Informasi pada UMKM: Tantangan dan Peluang. *Jurnal Minfo Polgan*, *13*(1), 815–821. https://doi.org/10.33395/jmp.v13i1.13823

Rahmadhania, Salsa Rizky Nugraha, M. A., & Supardinah, F. (2023). Analisa Risiko Dalam Tata Kelola IT Risk Management Menggunakan Framework COBIT 5 (Studi Kasus : SMK Telkom JAKARTA). *JTKSI (Jurnal Teknologi Komputer Dan Sistem Informasi)*, *6*(2), 156. https://doi.org/10.56327/jtksi.v6i2.1474

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*, *3*(3), 483–498. https://doi.org/10.51519/journalisi.v3i3.183