LOFIAN: Jurnal Teknologi Informasi dan Komunikasi
https://ejournal.umbp.ac.id/index.php/lofian
Vol. 5, No. 2, Pebruari 2026, Halaman 48-56

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Analisis Tata Kelola Keamanan Data dan Kontinuitas Layanan Berdasarkan Framework COBIT 2019 pada Platform E-Commerce Lokal (Studi Kasus: MedanMart)

Oktaviana Bangun[1], Elysabeth Cry Aruan[2], Suci Aisa Sirait[3], Tiara Yedidha Keliat[4], Selvia englika br Sitepu[5], Peranika Br perangin angin[6]

[1,2,3,4,5,6]*Universitas Mandiri Bina Prestasi*
Jl. Letjen Jamin Ginting No. 285-297, Kec. Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia - 20155

[1]*okta@dsn.umbp.ac.id*, [2]*elysabetharuan71@gmail.com*, [3]*suciaisasirait@gmail.com*, [4]*tiarakeliat04@gmail.com*, [5]*sitepuselvia10@gmail.com*, [6]*peranikaperanika52@gmail.com*

DOI: https://doi.org/10.58918/lofian.v5i2.294

Corresponding Author:
Oktaviana Bangun
okta@dsn.umbp.ac.id

History:
Submitted: 09-02-2026
Accepted: 16-02-2026
Published: 26-02-2026

Abstract

Local e-commerce platforms and digital MSMEs in Indonesia currently encounter formidable obstacles regarding data security governance and maintaining service continuity. To address these issues, this research evaluates the management of data security and service stability at MedanMart, a prominent local e-commerce platform in Medan City, by utilizing the COBIT 2019 framework. The study specifically deep-dives into the DSS05 (Management of Security Services) and EDM03 (Ensuring Risk Optimization) domains to determine governance maturity, perform gap analysis, and formulate strategic improvements for digital business readiness. Employing an empirical, descriptive, and qualitative case study approach, data were gathered through field observations, policy document reviews, and semi-structured interviews with IT personnel, operations managers, and merchant representatives. The assessment results revealed a maturity score of 2.43 for DSS05 and 2.21 for EDM03, categorizing both at the "Managed" level. Critical gaps identified include the absence of a disaster recovery plan (DRP), inadequate risk management documentation, and a lack of continuous security monitoring. Although the platform maintained a 97.2% uptime during the study, the absence of a formal resilience strategy poses significant operational risks. Ultimately, while MedanMart possesses a functional security foundation, substantial reinforcement in risk monitoring and continuity planning is essential to satisfy COBIT 2019 standards and national personal data protection regulations.

Keywords: COBIT 2019, IT governance, data security, service continuity, MedanMart, digital MSME.

Abstrak

Platform e-commerce lokal dan UMKM digital di Indonesia saat ini menghadapi tantangan besar dalam hal tata kelola keamanan data serta keberlanjutan layanan. Penelitian ini menganalisis manajemen keamanan data dan kontinuitas layanan pada MedanMart, sebuah platform e-commerce lokal di Kota Medan, dengan mengadopsi kerangka kerja COBIT 2019. Secara khusus, studi ini menitikberatkan pada domain DSS05 (Manajemen Layanan Keamanan) dan EDM03 (Memastikan Optimalisasi Risiko) untuk mengukur kematangan tata kelola, menganalisis kesenjangan, serta merumuskan rekomendasi guna meningkatkan kesiapan bisnis digital. Dengan menggunakan pendekatan studi kasus deskriptif-kualitatif yang empiris, pengumpulan data dilakukan melalui observasi lapangan, peninjauan dokumen kebijakan, serta wawancara semi-terstruktur bersama staf TI, manajer operasional, dan perwakilan mitra penjual. Hasil penilaian kematangan menunjukkan skor 2,43 untuk DSS05 dan 2,21 untuk EDM03, yang menempatkan keduanya pada level "Terkelola". Kesenjangan utama yang ditemukan mencakup ketiadaan rencana pemulihan bencana (DRP), dokumentasi manajemen risiko yang tidak memadai, serta kurangnya pemantauan keamanan yang berkelanjutan. Meskipun waktu aktif platform mencapai 97,2% selama periode observasi, absennya strategi ketahanan formal mengindikasikan adanya risiko operasional yang potensial. Sebagai simpulan, walaupun MedanMart memiliki fondasi manajemen keamanan yang cukup baik, penguatan lebih lanjut pada aspek pemantauan risiko dan kontinuitas layanan sangat diperlukan demi mematuhi standar COBIT 2019 serta regulasi perlindungan data pribadi.

Kata Kunci: COBIT 2019, DSS05, EDM03, keamanan data, kontinuitas layanan, e-commerce lokal, tata kelola TI.

1. Pendahuluan

Pertumbuhan ekosistem e-commerce Indonesia, khususnya di Medan, telah mengalami pertumbuhan yang luar biasa, didorong oleh percepatan adopsi digital di kalangan usaha kecil dan menengah (UMKM) dan konsumen. Menurut data dari Badan Pusat Statistik (BPS, 2023) dan Kementerian Komunikasi dan Informatika (Kominfo, 2023), peningkatan pesat volume transaksi online menegaskan bahwa platform marketplace berfungsi sebagai pilar baru ekonomi lokal. Namun, pertumbuhan pesat ini seringkali menyebabkan pengabaian aspek- aspek penting: tata kelola keamanan informasi dan kontinuitas layanan. Keterbatasan sumber daya, kurangnya kesadaran strategis, dan kurangnya keahlian teknis telah menyebabkan kerentanan keamanan pada platform e- commerce lokal, mengancam integritas data pengguna dan keberlanjutan bisnis.

Kejadian pelanggaran data baru-baru ini di perusahaan e-commerce domestik besar sekali lagi menyoroti pentingnya tata kelola keamanan informasi yang sistematis. Di tingkat lokal, platform yang mendukung UMKM di Kota Medan seringkali beroperasi dengan infrastruktur keamanan minimal, sehingga sangat rentan terhadap ancaman siber dan gangguan sistem. Peraturan perundang-undangan dan regulasi yang berlaku saat ini, yaitu Keputusan Pemerintah No. 71 (2019) tentang Pengoperasian Sistem dan Transaksi Elektronik dan Undang- Undang Perlindungan Data Pribadi (UU PDP) No. 27 (2022), mewajibkan operator sistem elektronik untuk memastikan keamanan dan ketersediaan data secara mutlak.

Untuk menjembatani kesenjangan antara kebutuhan operasional dan standar keamanan, COBIT 2019 (Control Objectives for Information and Related Technologies) menyediakan metodologi tata kelola TI yang komprehensif dan adaptif. Kerangka kerja ini secara jelas memisahkan dimensi "tata kelola (EDM)" dan "manajemen (DSS)", sehingga memungkinkan penilaian kuantitatif terhadap kematangan proses suatu organisasi. Studi ini berfokus pada DSS05 (Manajemen Layanan Keamanan), yang mengelola operasi keamanan seperti manajemen identitas dan kontrol akses, dan EDM03 (Memastikan Optimalisasi Risiko), yang bertujuan untuk menjaga optimalisasi risiko TI dalam batas toleransi organisasi. Sinergi antara arah strategis EDM03 dan kontrol operasional DSS05 memberikan landasan penting untuk membangun ketahanan pada platform digital.

Sejauh ini, literatur mengenai kerangka kerja COBIT masih didominasi oleh kajian pada sektor perbankan dan Instansi pemerintahan, sehingga terdapat keterbatasan studi yang mengintegrasikan domain DSS05 dan EDM03 dalam konteks e-commerce lokal maupun UMKM digital. Secara spesifik, minimnya penelitian yang mendalami tingkat kematangan keamanan informasi pada platform marketplace di wilayah Medan menciptakan sebuah kesenjangan akademik yang perlu segera diisi. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kematangan tata kelola keamanan data pada platform "MedanMart" dengan mengadopsi domain DSS05 dan EDM03 dari COBIT 2019. Melalui analisis tersebut, penelitian ini berupaya mengidentifikasi celah antara status operasional aktual dengan praktik terbaik internasional, yang kemudian akan menjadi landasan dalam merumuskan rekomendasi strategis guna memperkuat perlindungan data, menjaga stabilitas uptime, serta mencegah risiko kebocoran data untuk mendukung responsivitas bisnis digital.

Guna menjamin akurasi serta kedalaman fokus analitis, ruang lingkup penelitian ini dibatasi pada beberapa parameter utama. Pertama, objek penelitian dikerucutkan pada satu studi kasus spesifik, yaitu "MedanMart", sebagai representasi dari sektor UMKM digital di Kota Medan. Kedua, proses evaluasi dan pengambilan kesimpulan sepenuhnya didasarkan pada data empiris yang diperoleh melalui penyebaran kuesioner, wawancara mendalam dengan pihak terkait, serta peninjauan terhadap dokumen internal perusahaan. Terakhir, cakupan evaluasi hanya akan menitikberatkan pada domain DSS05 dan EDM03 yang dianggap sebagai parameter keamanan dan risiko paling fundamental, sehingga penelitian ini tidak akan mencakup keseluruhan domain yang terdapat dalam kerangka COBIT 2019.

2. Tinjauan Pustaka

2.1. Tata Kelola TI dan COBIT 2019

COBIT 2019 merupakan evolusi signifikan dari pendahulunya, dengan penekanan lebih besar pada penyelarasan tata kelola TI dengan tujuan strategis organisasi, optimalisasi risiko, dan pemanfaatan sumber daya secara efisien (ISACA, 2019). Kerangka kerja ini secara jelas membedakan antara dimensi "Tata Kelola (EDM)", yang mencakup

evaluasi, pengarahan, dan pemantauan, dan dimensi "Manajemen", yang berfokus pada perencanaan, pembangunan, penyampaian, dan pemantauan.

Struktur COBIT 2019 menyediakan Model Kapabilitas pada skala dari Level 0 (Tidak Lengkap) hingga Level 5 (Dioptimalkan), yang memungkinkan organisasi untuk memetakan realitas mereka sendiri. Hal ini sangat penting bagi usaha kecil, menengah, dan mikro (UMKM) untuk mengidentifikasi kesenjangan tata kelola dan mengembangkan strategi peningkatan yang terukur. Seperti yang dikemukakan Sutanto & Gunawan (2020), mengadaptasi COBIT ke sektor UMKM membutuhkan penyederhanaan metrik teknis dan memungkinkan operasi berkelanjutan sambil mempertahankan prinsip-prinsip tata kelola inti.

2.2. DSS05: Mengelola Layanan Keamanan

Domain DSS05 merupakan bagian dari domain "Pengiriman, Layanan, dan Dukungan (DSS)" dan bertujuan untuk melindungi aset informasi perusahaan dan menjaga risiko keamanan yang dapat diterima (ISACA, 2019). Dalam operasi e-commerce, domain ini berfungsi sebagai lini pertahanan pertama untuk melindungi data pembeli dan penjual yang sensitif (termasuk riwayat transaksi dan informasi akun).

Subproses DSS05 meliputi anti-malware, keamanan jaringan, perlindungan titik akhir, dan manajemen identitas dan akses logis. Pratama dkk. (2023) menekankan bahwa kerentanan pada platform digital Indonesia seringkali berasal dari manajemen akses yang tidak memadai dan kurangnya pemantauan keamanan. Oleh karena itu, implementasi DSS05 yang matang tidak hanya berfungsi sebagai sarana teknis untuk mencegah pelanggaran data tetapi juga sebagai sarana untuk mendukung kepatuhan terhadap UU PDP.

2.3. EDM03: Memastikan Optimalisasi Risiko

Sebagai bagian dari fungsi tata kelolanya, EDM03 memastikan bahwa selera risiko dan batas toleransi risiko organisasi didefinisikan dengan jelas dan dikomunikasikan kepada semua tingkatan manajemen (ISACA, 2019). Fokus utamanya adalah untuk menilai apakah risiko TI selaras dengan strategi organisasi dan menetapkan mekanisme pemantauan untuk penyimpangan.

Sinergi antara EDM03 dan DSS05 menciptakan ekosistem keamanan yang komprehensif. EDM03 mendefinisikan "tingkat risiko yang dapat diterima," sementara DSS05 menerapkan kontrol keamanan di tingkat lapangan. Wibowo & Rahayu (2021) menyatakan bahwa keberadaan register risiko yang jelas berfungsi sebagai dasar untuk keputusan investasi keamanan dan prioritas respons insiden di pasar.

2.4. Keamanan Data dan Ketahanan Layanan dalam E-Commerce

Peraturan Indonesia, khususnya Peraturan Pemerintah No. 71 (2019) dan UU PDP, mewajibkan operator sistem elektronik (PSE) untuk memastikan kerahasiaan, ketersediaan, dan integritas data. Keamanan data bukan hanya masalah teknis; ini adalah parameter yang memengaruhi kepercayaan pelanggan. Selain keamanan, kontinuitas layanan, yang ditunjukkan oleh uptime dan rencana pemulihan bencana (DRP), merupakan indikator penting kematangan tata kelola. Downtime yang tidak terduga pada platform e-commerce lokal dapat merusak reputasi bisnis dan menghambat partisipasi UMKM dalam ekosistem digital.

2.5. Kesiapan Bisnis Digital

Kesiapan bisnis digital didefinisikan sebagai kemampuan organisasi untuk memanfaatkan teknologi digital secara aman dan menyelaraskannya dengan tujuan strategis. Menurut Yulianto dkk. (2024), organisasi dengan kebijakan keamanan dan manajemen risiko yang terdokumentasi cenderung lebih tangguh terhadap serangan siber dan tuntutan regulasi. Dalam konteks MedanMart, kesiapan bisnis digital diukur dari kemampuan melindungi data pengguna, stabilitas sistem, dan kepatuhan terhadap hukum dan peraturan nasional. Penilaian menggunakan domain COBIT 2019 DSS05 dan EDM03 berfungsi sebagai indikator akurat untuk mengukur kematangan keamanan dan manajemen risiko dalam kesiapan ini.

3. Metodologi Penelitian

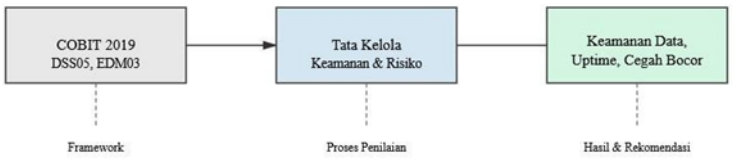
3.1. Desain dan Fokus Penelitian

Studi ini menggunakan studi kasus tunggal dengan karakteristik deskriptif dan analitis. Penelitian ini berfokus pada MedanMart, platform e-commerce lokal yang berbasis di Kota Medan. Pengambilan sampel bertujuan (purposive sampling) digunakan untuk memilih lokasi penelitian, mengingat MedanMart mewakili ekosistem digital usaha mikro, kecil, dan menengah (UMKM) lokal, mengelola sejumlah besar data pengguna (pembeli dan penjual), sangat bergantung pada ketersediaan layanan online, dan tunduk pada kepatuhan terhadap Peraturan Pemerintah No. 71 (2019) dan Undang-Undang Perlindungan Data Pribadi (UU PDP).

1. [Sisipkan diagram alur metodologi penelitian]
2. Proses penelitian dimulai dengan identifikasi masalah melalui observasi awal terhadap infrastruktur teknologi dan manajemen risiko organisasi. Selanjutnya, berdasarkan kerangka kerja COBIT 2019, kami memetakan tujuan bisnis ke tujuan TI dan mengidentifikasi DSS05 dan EDM03 sebagai domain prioritas.
3. Pengumpulan data empiris dilakukan melalui tiga metode utama.

3.2. Tahapan Prosedural

1. Wawancara semi-terstruktur: Wawancara ini dilakukan dengan pemangku kepentingan utama, termasuk staf TI, manajer operasional, dan perwakilan vendor, untuk memperoleh data kualitatif tentang praktik tata kelola di lokasi.
2. Kuesioner Penilaian Kapabilitas: Kuesioner berdasarkan aktivitas spesifik dalam domain DSS05 dan EDM03 digunakan untuk mengukur tingkat kapabilitas saat ini (As-Is).
3. Tinjauan Dokumen: Kebijakan keamanan, prosedur operasi standar (SOP), dan laporan insiden yang tersedia dianalisis.
4.
5. Data yang dikumpulkan dianalisis menggunakan analisis kesenjangan. Tujuan analisis ini adalah untuk membandingkan tingkat kapabilitas aktual dengan tingkat target yang diinginkan organisasi. Akhirnya, melalui proses ini, kami secara sistematis merumuskan rekomendasi strategis untuk mengatasi kerentanan keamanan dan meningkatkan ketahanan layanan digital di MedanMart. Kerangka kerja konseptual yang mendasari semua tahapan studi ini digambarkan secara komprehensif pada Gambar 2.



Gbr. 2. Kerangka Konseptual Penelitian

3.3. Subjek Penelitian

Populasi dan Sampel Data empiris untuk penelitian ini dikumpulkan melalui tiga metode utama:

1. Kuesioner Penilaian Kapabilitas COBIT 2019: Berdasarkan indikator proses ISACA (2019), lembar penilaian yang diadaptasi ke DSS05 (7 praktik) dan EDM03 (3 praktik) digunakan. Penilaian diukur pada skala 0 hingga 5 (0: Tidak Lengkap, 1: Awal, 2: Terkelola, 3: Terdefinisi, 4: Terkelola Secara Kuantitatif, 5: Dioptimalkan) sesuai dengan tingkat kematangan COBIT. Setiap pertanyaan dijawab berdasarkan situasi aktual di MedanMart.
2. Wawancara Semi-terstruktur: Dilakukan dengan satu manajer TI, satu manajer operasional, dan tiga perwakilan toko. Tujuannya adalah untuk mendapatkan wawasan mendalam tentang praktik keamanan, respons insiden, dan ketersediaan layanan.

3. Tinjauan dan Observasi Dokumen: Kebijakan keamanan, prosedur operasi standar (SOP), catatan insiden, dan laporan waktu aktif (uptime) ditinjau.

3.4. Teknik Pengumpulan Data

Informasi empiris dihimpun melalui tiga instrumen utama:Populasi untuk penelitian ini terdiri dari seluruh tim operasi internal MedanMart (tim TI dan operasi) dan pedagang aktif yang menggunakan platform. Sampel terdiri dari 15 individu (5 staf internal dan 10 pedagang) yang dipilih melalui pengambilan sampel bertujuan. Kriteria pemilihan sampel adalah mereka yang telah terdaftar setidaknya selama enam bulan dan mengakses platform setidaknya sekali seminggu.

3.5. Analisis Data dan Validasi

Validitas isi kuesioner diperiksa oleh seorang ahli tata kelola TI, dan uji coba awal dengan tiga responden dilakukan untuk memastikan kejelasan pertanyaan. Data yang dikumpulkan digunakan untuk menghitung skor rata-rata untuk setiap praktik dan domain dan memetakannya ke tingkat kematangan COBIT. Selain itu, data waktu aktif (uptime) diekstrak dari log server dan laporan bulanan selama enam bulan dari Januari hingga Juni 2024. Analisis Kesenjangan dilakukan untuk membandingkan skor aktual dengan nilai target Level 3 (Terdefinisi), yang merupakan standar untuk tata kelola terstandarisasi.

4. Hasil dan Diskusi

4.1. Gambaran Umum Organisasi dan Atribut Responden

MedanMart adalah pasar online yang khusus menjual produk dari usaha kecil dan menengah (UMKM) di Medan. Pasar ini memiliki sekitar 120 penjual aktif dan volume transaksi bulanan rata-rata 450-600 transaksi. Organisasi internal terdiri dari tiga staf IT dan lima staf operasional. Atribut responden yang berpartisipasi dalam penelitian ini ditunjukkan pada Tabel 1, dengan campuran seimbang antara administrator sistem dan pengguna eksternal (penjual).

Tabel 1
Profil Responden

Redox moiety	Kategori	Jumlah	Persentase (%)
Jabatan	Tim TI / Operasi	5	33,3
	Penjual (seller)	10	66,7
Lama bergabung	< 1 tahun	4	26,7
	1–2 tahun	7	46,7
	> 2 tahun	4	26,7
Frekuensi akses	Setiap hari	9	60,0
	Beberapa kali seminggu	6	40,0

4.2. Analisis Kematangan DSS05 dan EDM03

Penilaian kematangan menggunakan skala COBIT 2019 (0-5) mengungkapkan keadaan standarisasi tata kelola saat ini. Hasil survei dan penilaian wawancara dirangkum dalam Tabel 2.

Tabel 2

Profil Responden

Level	Nama	Deskripsi Singkat
0	Incomplete	Proses tidak dilaksanakan atau tidak mencapai tujuannya
1	Initial	Proses ad hoc, reaktif, bergantung pada individu
2	Managed	Proses dijalankan dan sebagian terdokumentasi
3	Defined	Proses terstandarisasi dan terdokumentasi
4	Quantitatively Managed	Proses terukur dan dikelola dengan data
5	Optimizing	Proses terus ditingkatkan berdasarkan best practice

Tabel 3

Hasil Penilaian Kematangan COBIT 2019 (DSS05 & EDM03)

Domain / Praktik	Skor Rata-Rata	Level Kematangan
DSS05 – Manage Security Services		
DSS05.01 – Perlindungan terhadap malware	2,80	Managed
DSS05.02 – Keamanan jaringan dan konektivitas	2,60	Managed
DSS05.03 – Keamanan endpoint	2,40	Managed
DSS05.04 – Identitas dan akses logika	2,53	Managed
DSS05.05 – Akses fisik aset TI	2,20	Managed
DSS05.06 – Dokumen sensitif dan output	2,33	Managed
DSS05.07 – Pemantauan kejadian keamanan	2,27	Managed
Rata-rata DSS05	2,45	Managed
EDM03 – Ensure Risk Optimization		
EDM03.01 – Evaluasi pengelolaan risiko TI	2,13	Managed
EDM03.02 – Pengarahan pengelolaan risiko	2,33	Managed
EDM03.03 – Pemantauan pengelolaan risiko	2,20	Managed
Rata-rata EDM03	2,22	Managed

4.3. Ketahanan dan Ketersediaan Layanan (Waktu Aktif)

Selama periode pengamatan dari Januari hingga Juni 2024, rata-rata ketersediaan sistem adalah 97,2%. Meskipun hal ini dianggap baik dalam skala lokal, namun masih jauh dari standar e-commerce global yaitu uptime 99,9% atau lebih tinggi. Kegagalan server menyebabkan downtime selama 24 jam pada Maret 2024

Tabel 4

Ketersediaan Layanan (Uptime) Platform MedanMart Periode Januari-Juni 2024

Bulan	Total Jam	Downtime (jam)	Uptime (%)	Keterangan
Januari 2024	744	18	97,6	Pemeliharaan terjadwal
Februari 2024	696	12	98,3	-
Maret 2024	744	24	96,8	Gangguan server 1x
April 2024	720	14	98,1	-
Mei 2024	744	22	97,0	Pemeliharaan + insiden singkat
Juni 2024	720	20	97,2	-
Rata-rata	728	18,3	97,2	-

Uptime rata-rata 97,2% menunjukkan kontinuitas layanan yang cukup baik, namun untuk layanan e-commerce yang mengandalkan transaksi real-time, target industri sering kali di atas 99%. Downtime terutama berasal dari pemeliharaan terjadwal dan satu insiden gangguan server pada Maret 2024.

4.4. Persepsi Pengguna tentang Keamanan dan Transparansi

Survei skala Likert mengungkapkan adanya perbedaan kepercayaan antara tim internal dan pedagang. Secara khusus, terkait dengan berbagi informasi pemeliharaan sistem, pedagang menilai diri mereka sendiri lebih rendah (3,00) dari pada tim TI (3,60), yang menyoroti perlunya transparansi informasi operasional kepada pengguna eksternal.

Tabel 5

Persepsi Responden terhadap Keamanan Data dan Uptime (Skala 1–5)

Pernyataan	Rata-Rata	Kategori Responden	Rata-Rata TI/Operasi	Rata-Rata Penjual
Data pribadi saya aman di platform ini	3,73	Gabungan	4,20	3,50
Platform jarang down atau tidak bisa diakses	3,67	Gabungan	3,80	3,60
Saya yakin transaksi pembayaran aman	3,87	Gabungan	4,00	3,80
Saya mendapat informasi jika ada pemeliharaan	3,20	Gabungan	3,60	3,00
Platform memiliki kebijakan privasi yang jelas	3,53	Gabungan	4,00	3,30

Persepsi keamanan data dan kepercayaan terhadap transaksi relatif positif (rata-rata 3,53–3,87), namun persepsi mengenai informasi pemeliharaan paling rendah (3,20). Penjual cenderung memberi skor lebih rendah daripada tim internal untuk hampir semua pernyataan, yang mengindikasikan bahwa komunikasi dan transparansi ke pengguna eksternal (penjual) masih perlu ditingkatkan. Temuan ini sejalan dengan gap yang teridentifikasi pada kontinuitas layanan dan dokumentasi kebijakan.

4.5. Analisis Kesenjangan dan Rekomendasi Strategis

Dengan menetapkan target Level 3 (Terdefinisi), standar minimum untuk tata kelola terstandarisasi, studi ini mengidentifikasi kesenjangan signifikan berikut:

1. Domain DSS05 (Operasi Keamanan): Skor Pemantauan Peristiwa Keamanan (DSS05.07) dan Keamanan Titik Akhir (DSS05.03) tetap di bawah 2,5. Kesenjangan utama meliputi kurangnya prosedur terdokumentasi untuk respons insiden dan tidak adanya audit keamanan reguler.
2. Domain EDM03 (Tata Kelola Risiko): Penilaian dan Pemantauan Risiko (EDM03.01 & EDM03.03) tetap reaktif. Organisasi tidak memiliki Daftar Risiko formal atau Pernyataan Selera Risiko terdokumentasi untuk memandu kebijakan keamanan. 3. Kontinuitas Layanan: Rencana pemulihan bencana (DRP) tidak ada, dan pengujian failover reguler tidak dilakukan. Selain itu, terdapat kurangnya transparansi dalam mekanisme untuk memberi tahu pengguna tentang jadwal pemeliharaan sistem.

Rincian kesenjangan dan rekomendasi untuk perbaikan dirangkum secara komprehensif dalam Tabel 5.

Kesiapan Bisnis Digital: Secara keseluruhan, tata kelola keamanan dan risiko MedanMart saat ini berada pada tahap Terkelola (Level 2). Peningkatan ke Level 3 (Terdefinisi) melalui formalisasi kebijakan dan standardisasi prosedur operasional sangat diperlukan untuk memperkuat kepercayaan pemangku kepentingan dan memenuhi persyaratan peraturan Indonesia (Peraturan Pemerintah No. 71/2019 dan UU Perlindungan Data Pribadi/UU PDP).

4.6. Strategi Pencegahan Kebocoran Data

Dalam upayanya untuk mengurangi risiko kebocoran data, MedanMart menunjukkan tingkat perhatian yang wajar terhadap aspek teknis (misalnya, enkripsi dan manajemen akses berdasarkan skor DSS05.02 dan DSS05.04). Namun, pertahanan tata kelola dan pemantauannya masih lemah. Pencegahan kebocoran data yang komprehensif memerlukan efek sinergis antara kontrol teknis (DSS05) dan pengawasan strategis (EDM03). Klasifikasi data, identifikasi aset kritis, dan pengembangan SOP respons insiden merupakan langkah-langkah penting untuk mematuhi prinsip-prinsip perlindungan informasi pribadi yang diamanatkan secara hukum.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

4.7. Diskusi Hasil Penelitian

Temuan penelitian ini konsisten dengan temuan Sutanto & Gunawan (2020), yang menemukan bahwa usaha mikro, kecil, dan menengah (UMKM) cenderung tetap berada pada tahap kematangan awal hingga terkelola, dengan tantangan utama berupa komitmen dokumentasi dan alokasi sumber daya. Namun, tidak seperti penelitian Zulkarnain & Sari (2022) yang berfokus pada e-government, penelitian tentang e-commerce lokal ini menekankan peran penjual sebagai pemangku kepentingan utama. Persepsi penjual tentang stabilitas dan keamanan sistem (Tabel 5) menunjukkan bahwa transparansi komunikasi merupakan faktor penting dalam keberlanjutan ekosistem digital Medan.

Gbr. 3. Tingkat Kematangan DSS05 dan EDM03

Tabel 6

Ringkasan Gap dan Rekomendasi

Area	Gap	Rekomendasi
Keamanan data	Pemantauan	keamanan
Manajemen risiko	Risk register dan risk appetite belum formal	Dokumentasikan risk appetite statement dan lakukan risk assessment periodik
Kontinuitas layanan	Tidak	ada

5. Kesimpulan dan Rekomendasi

5.1. Kesimpulan

Analisis tata kelola keamanan data dan keberlanjutan layanan pada platform e-commerce lokal MedanMart menggunakan kerangka kerja COBIT 2019 menunjukkan bahwa tingkat kematangan saat ini berada pada "Level 2: Terkelola". Hasil ini didasarkan pada skor kematangan domain DSS05 (Manajemen Layanan Keamanan) sebesar 2,45 dan domain EDM03 (Memastikan Optimalisasi Risiko) sebesar 2,22. Meskipun proses keamanan dan manajemen risiko telah berfungsi secara operasional, perusahaan belum mencapai "Level 3: Terdefinisi", yang menuntut adanya standardisasi di seluruh organisasi serta mekanisme pemantauan yang berbasis pada metrik yang jelas dan terukur.

Dalam hal efektivitas keamanan data, MedanMart telah menerapkan tindakan pencegahan dasar seperti enkripsi, manajemen akses, dan perlindungan terhadap malware untuk melindungi data pengguna. Namun, penelitian ini mengidentifikasi adanya kelemahan pada aspek pemantauan insiden keamanan, prosedur respons yang belum terstandardisasi, serta kurangnya audit keamanan berkala, sehingga sistem tata kelola untuk mencegah kebocoran data masih dalam tahap pengembangan. Terkait kontinuitas layanan, tercatat rata-rata uptime sebesar 97,2% selama enam bulan pengamatan, yang masih memerlukan peningkatan melalui pengembangan rencana pemulihan bencana (DRP) dan perbaikan transparansi informasi jadwal pemeliharaan kepada pengguna.

Secara keseluruhan, kesiapan bisnis digital MedanMart yang berada pada tahap "Terkelola" perlu segera ditingkatkan menuju tahap "Terdefinisi" untuk menjamin keberlanjutan operasional. Peningkatan ini sangat krusial

tidak hanya untuk memenuhi standar internasional COBIT 2019, tetapi juga untuk memastikan kepatuhan penuh terhadap regulasi nasional seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

5.2. Rekomendasi

Guna meningkatkan kualitas tata kelola di masa mendatang, manajemen MedanMart perlu mengambil langkah strategis yang diawali dengan formalisasi kebijakan tata kelola melalui dokumentasi kebijakan keamanan informasi dan privasi yang dikomunikasikan secara menyeluruh kepada seluruh pengguna. Selain itu, optimasi manajemen risiko harus dilakukan dengan merumuskan Risk Appetite Statement, memelihara register risiko, serta melaksanakan penilaian risiko secara rutin setiap tahun. Hal ini juga harus didukung dengan penetapan Prosedur Operasi Standar (SOP) yang mencakup respons insiden, jadwal audit sistem, serta penilaian ulang tingkat kematangan secara berkala. Untuk memperkuat ketahanan operasional, perusahaan disarankan merumuskan Disaster Recovery Plan (DRP) serta menguji prosedur pencadangan dan failover secara konsisten. Terakhir, aspek transparansi operasional perlu ditingkatkan melalui perencanaan pemeliharaan sistem yang diinformasikan lebih awal kepada pengguna melalui berbagai saluran komunikasi platform yang tersedia.

Di samping rekomendasi untuk pihak manajemen, penelitian di masa depan diharapkan dapat memperluas cakupan area penelitian dengan melakukan studi komparatif terhadap platform e-commerce regional lainnya di Sumatera Utara guna memetakan kematangan digital wilayah tersebut secara lebih komprehensif. Peneliti selanjutnya juga disarankan untuk mengintegrasikan aspek kepatuhan hukum dan regulasi dengan menerapkan metode penilaian kuantitatif terhadap implementasi UU PDP. Lebih lanjut, diperlukan analisis dampak yang lebih mendalam untuk menyelidiki korelasi antara peningkatan level kematangan tata kelola TI terhadap tingkat kepuasan serta niat pengguna untuk kembali menggunakan platform tersebut.

Ucapan Terima Kasih

Sebagai penutup, penulismenyampaikan rasa terima kasih dan apresiasi yang mendalam kepada seluruh pihak yang telah memberikan dukungan serta memfasilitasi terlaksananya penelitian ini. Keberhasilan dalam merumuskan kerangka transformasi tata kelola keamanan informasi ini merupakan manifestasi dari kerja keras dan kolaborasi kolektif yang solid.

Daftar Pustaka

[1] F. Harahap, "Analisis tata kelola dan evaluasi teknologi informasi menggunakan framework COBIT 2019 di Sekolah X," Jurnal Informatika, vol. 12, no. 1, pp. 45-58, 2025. doi: 10.30873/jurnalinformatika.
[2] I. Meiharsiwi, et al., "Analysis of information technology proficiency levels for academic services via COBIT 2019," Asian Journal of Social and Humanities, vol. 2, no. 12, 2024.
[3] M. K. Anam, et al., "Application of COBIT 2019 framework to analyse the security of academic information systems," DECODE, vol. 3, no. 2, pp. 120-132, 2023.
[4] A. Setiawan & D. Rahmawati, "Academic information system governance using IT Balanced Scorecard and COBIT 2019," Proc. ICITB, vol. 5, no. 1, 2023. [Online].
[5] A. Ishlahuddin, et al., "Analysing IT governance maturity level using COBIT 2019: A case study of XYZ-edu," ICISS IEEE, pp. 1-6, 2020. doi: 10.1109/IC2IE50715.2020.9274599.
[6] R. Aditya & S. Sutikno, "Evaluasi Manajemen Risiko Teknologi Informasi pada Institusi Pendidikan Menengah melalui COBIT 2019, "Jurnal Manajemen Sistem Informasi, vol. 9, no. 2, 2024.
[7] N. Fajrin & N. Santoso, "Evaluasi Tata Kelola Keamanan Informasi Berbasis COBIT 2019 pada Sekolah Menengah Kejuruan," Jurnal PTIIK, vol. 7, no. 4, 2023.
[8] U. A. Citra, et al., "Evaluasi Tata Kelola Sistem Informasi Manajemen Sekolah dan Data Peserta Didik Berdasarkan Framework COBIT 2019 di SMAN 1 Medan," ELINA: Jurnal Pengabdian Masyarakat, 2026.
[9] E. C. Aruan, et al., "Analisis Tata Kelola Keamanan Data dan Kontinuitas Layanan Berdasarkan Framework COBIT 2019 pada Platform E-Commerce Lokal," ELINA, 2026.
[10] ISACA, COBIT 2019 Framework: Governance and Management Objectives, Illinois, USA: Information Systems Audit and Control Association, 2019.