Analisis Risiko Penggunaan Aplikasi Shopee Menggunakan Metode Failure Mode and Effect Analysis Berdasarkan Data Scrapping

Novan Setyawan[1], Zeny Zanuba Arifah[2], Mastuty Ayu Ningtyas[3]
Fakultas Informatika, Universitas Telkom, Surabaya
novansetyawan@student.telkomuniversity.ac.id[1], zenyzanubaarifah@student.telkomuniversity.ac.id[2]
mastutyayu@telkomuniversity.ac.id[3]

Abstrak

Penelitian ini mengkaji risiko penggunaan aplikasi Shopee melalui metode Failure Mode and Effect Analysis (FMEA) dan standar ISO 27001 tahun 2022, berdasarkan data yang diperoleh melalui teknik data scrapping. Analisis ini mengidentifikasi berbagai mode kegagalan yang dialami pengguna, termasuk masalah teknis seperti bug, crash aplikasi, kesulitan dalam proses pembayaran, keterlambatan pengiriman barang, serta masalah keamanan data dan privasi pengguna. Hasil penilaian menunjukkan beberapa risiko dengan nilai Risk Priority Number (RPN) sangat tinggi di setiap kategori aset, di kategori informasi/data dengan nilai 378 terkait kurangnya perhatian akan stock barang, pada kategori people dengan nilai 320 terkait user salah dan tidak mengingat alamat tujuan, kategori hardware dengan nilai 252 terkait jaringan yang tidak stabil menyebabkan aplikasi berjalan tidak baik, dan pada kategori terakhir yaitu software dengan nilai 240 terkait kesalahan input pengguna dalam informasi pembayaran. Hasil penilaian tersebut menandakan perlunya tindakan mitigasi segera. Implementasi langkah-langkah mitigasi yang diusulkan bertujuan untuk meningkatkan kualitas dan keandalan aplikasi Shopee, terbukti efektif dalam meningkatkan pengalaman pengguna dan menurunkan insiden kegagalan. Penelitian ini memberikan kontribusi signifikan dalam pemahaman dan pengelolaan risiko aplikasi e-commerce, menawarkan analisis komprehensif dan berbasis data nyata yang dapat digunakan oleh pengembang Shopee untuk perbaikan aplikasi.

Kata kunci: Analisis Risiko, Shopee, Failure Mode and Effect Analysis (FMEA), data scrapping.

PENDAHULUAN

Di era digital saat ini, e-commerce telah menjadi bagian integral dari kehidupan sehari-hari masyarakat. Salah satu platform e-commerce yang populer di Asia Tenggara, termasuk Indonesia, adalah Shopee. Shopee menawarkan berbagai kemudahan dalam berbelanja online, mulai dari beragam produk hingga berbagai metode pembayaran yang aman dan nyaman. Namun, seiring dengan peningkatan penggunaan aplikasi Shopee, muncul berbagai risiko yang dapat mempengaruhi pengalaman pengguna dan keamanan data.

Analisis risiko menjadi penting untuk mengidentifikasi dan mengelola potensi masalah yang mungkin timbul dalam penggunaan aplikasi Shopee. Salah satu metode yang efektif untuk melakukan analisis risiko adalah Failure Mode and Effect Analysis (FMEA). FMEA adalah pendekatan sistematis yang digunakan untuk mengidentifikasi potensi kegagalan dalam suatu sistem, produk, atau proses, dan menilai dampaknya terhadap keseluruhan operasi. Dengan menggunakan FMEA, perusahaan dapat mengidentifikasi area kritis yang memerlukan perhatian khusus dan merancang strategi mitigasi yang efektif. (Munaroh, 2020).

Pada penelitian ini, analisis risiko penggunaan aplikasi Shopee dilakukan dengan metode FMEA yang didukung oleh data yang diperoleh melalui teknik data scrapping. Data scrapping adalah proses otomatisasi pengambilan data dari berbagai sumber di internet, yang memungkinkan

pengumpulan informasi yang relevan dan aktual. Data ini mencakup berbagai ulasan pengguna, laporan bug, dan insiden lain yang berkaitan dengan penggunaan aplikasi Shopee.

Pendekatan ini memberikan gambaran yang lebih komprehensif tentang risiko yang dihadapi pengguna aplikasi Shopee. Dengan memanfaatkan data scraping, analisis risiko menjadi lebih akurat dan berdasarkan fakta lapangan. Hasil analisis ini diharapkan dapat membantu pengembang aplikasi Shopee dalam meningkatkan kualitas dan keandalan aplikasi, serta memberikan pengalaman yang lebih baik dan aman bagi pengguna. (Haekal ,2021).

Pada akhirnya, penelitian ini bertujuan untuk mengidentifikasi dan mengelola risiko-risiko utama dalam penggunaan aplikasi Shopee melalui metode FMEA, serta menyarankan langkah-langkah mitigasi yang dapat diimplementasikan. Dengan demikian, diharapkan dapat tercipta lingkungan berbelanja online yang lebih aman dan terpercaya bagi pengguna Shopee.

TINJAUAN PUSTAKA

Risiko

Risiko dapat didefinisikan sebagai kemungkinan terjadinya suatu kejadian atau situasi yang tidak diharapkan akan terjadi yang dapat menyebabkan kegagalan. Konsep ini membahas kemungkinan hasil tindakan tertentu yang dapat terjadi saat ini atau di masa depan apakah berdampak menguntungkan atau tidak. Karakteristik dari risiko sendiri adalah ketidakpastian dan mengandung unsur kerugian. (Stamatis, 2019).

Manajemen Risiko

Manajemen risiko dalam manajemen teknologi informasi adalah proses yang membantu mengelola biaya operasional dan ekonomi yang terkait dengan sistem TI. Manajemen risiko melibatkan penilaian risiko dan analisis sistematis terhadap potensi risiko yang dapat berdampak pada profitabilitas bisnis atau organisasi (Atmojo, 2020).

Tujuan manajemen risiko adalah untuk meningkatkan kinerja, mendorong inovasi, dan mendukung pencapaian tujuan perusahaan. Manajemen risiko membentuk landasan untuk mengelola risiko, dan prinsip-prinsip ini harus dipertimbangkan saat menetapkan proses dan kerangka kerja manajemen risiko.

Proses Manajemen Risiko

Proses manajemen risiko meliputi berbagai tahapan (Novianti, 2019), yaitu:

1. **Identifikasi Risiko**: Pertama, kita perlu menemukan, mengenali, dan memahami risiko yang dapat mempengaruhi proyek atau hasil proyek. Ada beberapa metode berbeda untuk mengidentifikasi risiko, seperti membuat daftar risiko.
2. **Analisis Risiko**: Setelah kita mengidentifikasi risiko, langkah selanjutnya adalah mencari tahu seberapa besar kemungkinan risiko tersebut terjadi dan apa dampaknya. Hal ini membantu kami memahami sifat dan potensi risiko terhadap tujuan proyek.
3. **Evaluasi atau Pemeringkatan Risiko**: Kami kemudian mengevaluasi atau memberi peringkat risiko berdasarkan seberapa signifikan risiko tersebut. Kami melakukan ini dengan mempertimbangkan seberapa besar kemungkinan hal tersebut terjadi dan apa konsekuensinya. Hal ini membantu kami memutuskan apakah risiko tersebut dapat diterima, dapat dikelola, atau sebaiknya ditolak.

4. **Mitigasi Risiko**: Juga dikenal sebagai rencana respons risiko. Pada tahap ini, kita menilai risiko tertinggi dan mengembangkan rencana untuk mengatasi atau memodifikasi risiko tersebut hingga mencapai tingkat yang dapat diterima. Hal ini mencakup strategi untuk meminimalkan kemungkinan risiko negatif dan memaksimalkan peluang yang ada, serta merumuskan strategi mitigasi risiko, rencana pencegahan, dan rencana darurat.
5. **Pemantauan Risiko**: Tahap ini melibatkan penggunaan daftar risiko proyek untuk mengawasi, melacak, dan meninjau risiko yang ada.

E-Commerce

Commerce atau e-commerce adalah suatu proses terjadinya transaksi jual beli yang dalam prakteknya dilakukan secara online melalui media elektronik. Menurut Laudon & Laudon, e commerce adalah transaksi business to business yang terjadi dengan perantara jaringan internet. Dalam dunia perdagangan, e-commerce menawarkan banyak perubahan. Proses jual beli tidak lagi membutuhkan pertemuan tatap muka seperti pada toko konvensional. Penjual dan pembeli hanya perlu melakukan proses transaksi online. (Rehatalanit, Y. L. R. , 2021).

Analisis Risiko dalam E-commerce

Analisis risiko adalah proses sistematis untuk mengidentifikasi, menilai, dan mengelola risiko yang mungkin mempengaruhi keberhasilan suatu proyek atau operasional bisnis. Menurut Kerzner (2017), analisis risiko penting untuk memastikan bahwa potensi masalah dapat diidentifikasi lebih awal dan langkah-langkah mitigasi dapat diimplementasikan untuk mengurangi dampak negatifnya. Dalam konteks e-commerce, risiko dapat berkisar dari masalah teknis seperti bug dan downtime, hingga risiko keamanan seperti kebocoran data dan penipuan online (Turban et al., 2020).

Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) adalah proses terstruktur yang menggunakan pendekatan top-down untuk mengidentifikasi dan mengevaluasi potensi risiko dalam suatu produk. FMEA dapat dijadikan sebagai *tools* yang berguna untuk menilai tingkat evaluasi kualitas produk serta kemungkinan mode kegagalan dan dampaknya (Kartikasari, 2019). Terdapat 3 variabel utama pembuatan FMEA yaitu:

1. Severity merupakan rating yang menunjukkan seberapa serius dampak yang muncul sebagai akibat dari *potensial failure mode.*
2. Occurance adalah rating yang menunjukkan seberapa sering terjadi kecacatan atau *bug* pada produk.
3. Detection adalah proses kontrol yang menemukan secara khusus sumber utama kegagalan.

Menurut (Stamatis, 2019), langkah-langkah dalam proses FMEA yaitu:

1. Tinjau teknik/prosedurnya.
2. Identifikasi potensi kegagalan teknik yang ditinjau.
3. Menganalisis dampak yang mungkin timbul dari kegagalan ini.
4. Menilai seberapa parah kegagalan yang mungkin terjadi.
5. Identifikasi apa yang dapat menyebabkan kegagalan tersebut.
6. Tentukan seberapa sering kegagalan ini terjadi.
7. Evaluasi pengendalian yang ada untuk mencegah kegagalan ini.
8. Menilai seberapa baik pengendalian dapat mendeteksi atau menghindari kegagalan.

9. Hitung Angka Prioritas Risiko (RPN) dengan mengalikan tingkat keparahan, kejadian, dan deteksi (RPN = S*O*D). Angka ini menunjukkan betapa seriusnya potensi kegagalan.
10. Memberikan rekomendasi untuk memperbaiki kegagalan yang paling serius.

RPN membantu tim fokus pada kegagalan paling kritis dan memutuskan tindakan pencegahan atau perbaikan.

Data Scrapping

Data scrapping adalah teknik pengumpulan data otomatis dari berbagai sumber online menggunakan perangkat lunak khusus. Menurut Mitchell (2015), data scrapping memungkinkan pengambilan informasi yang besar dan beragam dari website, yang dapat digunakan untuk berbagai analisis termasuk analisis risiko. Dalam penelitian ini, data scrapping digunakan untuk mengumpulkan ulasan pengguna, laporan bug, dan insiden lain yang terkait dengan penggunaan aplikasi Shopee. Teknik ini memungkinkan pengumpulan data yang real-time dan berbasis fakta, sehingga analisis risiko yang dilakukan menjadi lebih akurat dan relevan.

Keamanan Informasi

Keamanan informasi merupakan upaya perlindungan data dari serangan seperti virus dan peretas, yang menjamin keberlangsungan bisnis, mengurangi risiko bisnis, meningkatkan keuntungan investasi, dan meningkatkan peluang bisnis (Aprianti, 2023). Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu:

1. Confidentiality (kerahasiaan) merupakan aspek yang memastikan bahwa data dan informasi hanya dapat diakses oleh individu yang berwenang dengan tetap menjaga kerahasiaannya.
2. Integrity (Integritas) merupakan aspek untuk memastikan bahwa data tidak diubah tanpa izin, menjaga keakuratan dan integritasnya.
3. Availability (Ketersediaan) merupakan aspek yang memastikan bahwa data dan informasi disediakan sesuai kebutuhan, memungkinkan pengguna yang berwenang untuk mengakses informasi dan alat yang relevan.

METODE

Metode penelitian yang digunakan pada penelitian ini adalah metode kualitatif. Pendekatan ini digunakan untuk memahami resiko pada aplikasi berdasarkan pengalaman pengguna dalam penggunaan aplikasi shopee. Alat yang digunakan dalam penelitian ini mencakup kumpulan pertanyaan. Data utama untuk penelitian berasal dari pengguna aplikasi Shopee di Indonesia. Metode pengumpulan data yang digunakan adalah kuisioner atau survei, dimana untuk prosesnya dengan cara mendistribusikan kuisioner atau survei tersebut secara online. Proses analisis data meliputi langkah-langkah seperti pengelompokan data, identifikasi data, dan penentuan tindak lanjut dari hasil data tersebut.

HASIL DAN PEMBAHASAN

A. Identifikasi Aset Kritis

Daftar aset kritis yang dimiliki aplikasi Shopee didapatkan melalui data scrapping dari ulasan pengguna di play store. Berikut merupakan tabel dari hasil identifikasi aset Kritis.

Tabel 1.1 Identifikasi Aset Kritis

No.	Kategori	Aset
1	Hardware	Server

2		Router
3		Smartphone
6	Software	Konfigurasi
7		Bug
8		Interface
11	People	Admin
12		User
13		Interface
16	Data/Informasi	Informasi Data
17		Keamanan Data
18		Ketersediaan Informasi

Sumber: hasil olah data penulis

B. Identifikasi Risiko

Pada tahap identifikasi risiko, dapat dilihat dari dua aspek utama yaitu kemungkinan resiko aplikasi serta kerentanan yang dimiliki oleh aplikasi tersebut. Hasil identifikasi risiko dapat dilihat pada tabel berikut.

Tabel 1.2 Identifikasi Risiko

No.	Jenis Risiko	Risiko
1.	Perangkat Keras (Hardware)	1. Keterbatasan memori internal/eksternal untuk update 2. Adanya kerusakan pada sensor fingerprint perangkat user 3. Kinerja perangkat yang kurang untuk menggunakan aplikasi baik dari spesifikasi maupun system operasi 4. Jaringan yang tidak stabil menyebabkan aplikasi tidak dapat berjalan dengan baik 5. spesifikasi maupun sistem operasi device user tidak memenuhi syarat minimum
2.	Perangkat Lunak (Software)	1. Keterbatasan layanan operator dengan aplikasi yang mengalami gangguan/keterlambatan dalam pengiriman kode otp 2. Saat membuka bagian saldo shopeepay tidak menampilkan nominal hanya blank 3. Perubahan antarmuka dan fitur yang kurang sesuai dengan aplikasi 4. Gangguan login karena faktor seperti kualitas kamera yg rendah, sensor cahaya , jarak, dll 5. Sistem tidak memberikan verifikasi pembayaran
3.	Data/Informasi	1. Kebocoran data akibat tingkat proteksi data yang kurang dari aplikasi

		2. Kurangnya update informasi stock barang 3. Kesalahan input pengguna took 4. Konten yang tidak sesuai dengan kebijakan 5. Informasi proses pengembalian yang tidak valid pada sistem
4.	Sumber Daya Manusia (People)	1. user tidak dapat mengingat password untuk akun shopee 2. user salah memasukkan dan tidak mengingat alamat tujuan pengiriman 3. Kurir tidak memiliki moral & integritas serta tanggung jawab 4. Admin shopee kurang memahami cara kerja sistem pesanan dalam aplikasi 5. Tidak adanya panduan pengguna seputar antarmuka dan fitur

Sumber: hasil olah data penulis

C. Penilaian Risiko

Penilaian risiko dilakukan dengan menggunakan metode FMEA (Failure Mode and Effect Analysis) berdasarkan framework ISO 27001 tahun 2022. Dalam penilaian ini, setiap risiko dinilai berdasarkan tiga faktor utama: Severity (tingkat keparahan), Occurrence (kemungkinan terjadinya), dan Detection (kemampuan deteksi). Hasil penilaian ini kemudian digunakan untuk menghitung Risk Priority Number (RPN).

D. Hasil Perhitungan RPN

Hasil perhitungan RPN memberikan gambaran mengenai prioritas risiko yang perlu segera ditangani. Berikut adalah hasil perhitungan RPN untuk beberapa risiko yang diidentifikasi:

Tabel 1.3 Tabel Perhitungan RPN

Rank	Asset	Identifikasi Risiko	Severity	Occurrence	Detection	RPN	Level
1	*Information/Data*	Kurang perhatian akan pengecekan atau update jumlah stock di toko online	7	6	9	378	Very High
2	*People*	User salah memasukkan dan tidak mengingat alamat tujuan untuk pengiriman	10	4	8	320	Very High

3	*Hardware*	Jaringan yang tidak stabil menyebabkan aplikasi tidak dapat berjalan dengan baik	9	7	4	252	Very High
4	*Information/Data*	Informasi proses pengembalian yang tidak valid pada sistem	10	5	5	250	Very High
5	*Information/Data*	kesalahan input pengguna toko seperti alamat, no telepon dll	10	4	6	240	Very High
6	*Information/Data*	Kebocoran data akibat tingkat proteksi data yang kurang dari aplikasi	10	4	6	240	Very High
7	*Software*	Kesalahan input pengguna dalam segi memasukkan informasi pembayaran	10	6	4	240	Very High
8	*People*	User tidak dapat mengingat password untuk akun shopee	10	4	6	240	Very High
9	*Software*	Keterbatasan layanan operator dengan aplikasi yang mengalami gangguan/keterlambatan dalam pengiriman kode otp	8	4	6	192	High
10	*Hardware*	Kinerja perangkat yang kurang untuk menggunakan aplikasi, dari segi	7	4	4	112	Medium

		ram, chipset maupun sistem operasi					
11	*Software*	Perubahan antarmuka dan fitur yang kurang sesuai dengan aplikasi	7	5	3	105	Medium
12	*People*	Kurir tidak memiliki moral & integritas serta tanggung jawab, serta kurangnya tanggung jawab dari pihak shopee	10	1	9	90	Medium
13	*Hardware*	Adanya eror atau kerusakan pada sensor fingerprint perangkat user	7	3	4	84	Medium
14	*People*	Admin shopee kurang memahami cara kerja sistem pesanan dalam aplikasi	8	5	2	80	Medium
15	*Software*	Saat membuka bagian saldo shopeepay tidak menampilkan nominal hanya blank	5	3	5	75	Low
16	*People*	Tidak adanya panduan pengguna seputar antarmuka dan fitur, serta susunan fitur yang rumit	6	5	2	60	Low
17	*Information/Data*	Konten yang tidak sesuai dengan kebijakan atau	5	4	2	40	Low

		pedoman yang ada pada aturan aplikasi					
18	*Software*	Gangguan login karena faktor seperti kualitas kamera yg rendah, sensor cahaya , jarak, dll	10	1	3	30	Low
19	*Hardware*	Spesifikasi maupun sistem operasi device user tidak memenuhi syarat minimum	4	1	6	24	Low
20	*Hardware*	Kapasitas memori tidak cukup atau keterbatasan memori internal/eksternal untuk update	5	1	4	20	Low

Sumber: hasil olah data penulis

E. Mitigasi Risiko

Berdasarkan hasil perhitungan RPN, langkah-langkah mitigasi risiko dirancang untuk mengurangi dampak negatif dari risiko yang diidentifikasi. Berikut adalah beberapa tindakan mitigasi yang disarankan:

Tabel 1.4 Tabel Tindak Lanjut Risiko

No.	Asset	Identifikasi Risiko	Annex	Tindak Lanjut
1	*Information /Data*	Kurang perhatian akan pengecekan atau update jumlah stock di toko online	5.9	Meningkatkan proses pengecekan dan pembaruan stok secara teratur dalam sistem toko online. Dengan memelihara inventaris yang akurat dan terkini, pelanggan akan mendapatkan visibilitas yang lebih baik terhadap ketersediaan barang, mengurangi kebingungan dan meningkatkan kepuasan pelanggan.
2	*People*	User salah memasukkan dan tidak mengingat alamat tujuan untuk pengiriman	5.9	Memastikan bahwa platform atau aplikasi, seperti Shopee, memiliki sistem yang efektif untuk mengelola dan memvalidasi alamat pengiriman yang dimasukkan oleh pengguna
3	*Hardware*	Jaringan yang tidak stabil menyebabkan aplikasi tidak dapat	8.16	Kegiatan pemantauan akan dilakukan untuk jaringan yang tidak stabil. Ini mencakup

		berjalan dengan baik		pemantauan terus-menerus terhadap perilaku jaringan untuk mendeteksi anomali dan gangguan yang dapat memengaruhi kinerja aplikasi.
4	*Information/ Data*	Informasi proses pengembalian yang tidak valid pada sistem	5.10	Meningkatkan kejelasan dan pemahaman tentang proses pengembalian barang yang valid dalam sistem. Hal ini dapat dilakukan melalui penyediaan panduan yang komprehensif dan pembaruan kebijakan yang menjelaskan prosedur yang harus diikuti untuk melakukan pengembalian barang secara sah
5	*Information/ Data*	kesalahan input pengguna toko seperti alamat, no telepon dll	5.10	Memastikan bahwa para pengguna toko diberikan pelatihan dan pemahaman yang cukup tentang kebijakan penggunaan yang diterima, serta prosedur untuk memastikan bahwa informasi yang dimasukkan oleh pengguna toko, seperti alamat dan nomor telepon, diverifikasi dengan benar sebelum disimpan dalam sistem
6	*Information/ Data*	Kebocoran data akibat tingkat proteksi data yang kurang dari aplikasi	5.34	Memperkuat tingkat proteksi data dalam aplikasi dengan menerapkan langkah-langkah perlindungan yang sesuai, seperti enkripsi data, pengaturan akses yang ketat, dan pemantauan keamanan secara teratur. Dengan meningkatkan proteksi data, risiko kebocoran informasi yang sensitif dapat dikurangi secara signifikan.
7	*Software*	Kesalahan input pengguna dalam segi memasukkan informasi pembayaran	8.12	Memperkuat tingkat proteksi data dalam aplikasi dengan menerapkan langkah-langkah perlindungan yang sesuai, seperti enkripsi data, pengaturan akses yang ketat, dan pemantauan keamanan secara teratur. Dengan meningkatkan proteksi data, risiko kebocoran informasi yang sensitif dapat dikurangi secara signifikan.
8	*People*	User tidak dapat mengingat password untuk akun shopee	6.8	Memastikan bahwa Shopee memiliki mekanisme yang memungkinkan pengguna untuk melaporkan masalah lupa password secara cepat dan efisien.
9	*Software*	Keterbatasan layanan operator dengan aplikasi yang mengalami gangguan/keterlambatan dalam pengiriman kode otp	5.29	Mengidentifikasi dan merencanakan strategi untuk mengatasi situasi darurat seperti gangguan layanan operator atau keterlambatan dalam pengiriman kode OTP. Ini mungkin melibatkan penggunaan alternatif untuk verifikasi identitas, seperti kode cadangan atau metode otentikasi yang tidak bergantung pada layanan operator.

10	*Hardware*	Kinerja perangkat yang kurang untuk menggunakan aplikasi, dari segi ram, chipset maupun sistem operasi	8.6	Manajemen kapasitas akan memantau dan menyesuaikan penggunaan sumber daya sesuai dengan kebutuhan saat ini dan yang diharapkan. Dengan melakukan manajemen kapasitas yang efektif, organisasi dapat mengidentifikasi perangkat yang ku
11	*Software*	Perubahan antarmuka dan fitur yang kurang sesuai dengan aplikasi	8.33	Meningkatkan uji coba sebelum peluncuran perubahan antarmuka dan fitur baru. Hal ini dapat mencakup pengujian regresi yang menyeluruh untuk memastikan bahwa perubahan tersebut tidak mempengaruhi fungsionalitas yang ada, serta pengujian sistematis untuk mengidentifikasi dan memperbaiki bug sebelum aplikasi diluncurkan ke pengguna akhir.
12	*People*	Kurir tidak memiliki moral & integritas serta tanggung jawab, serta kurangnya tanggung jawab dari pihak shopee	6.3	Menyelenggarakan pelatihan yang mengarah pada peningkatan kesadaran moral, integritas, dan tanggung jawab bagi para kurir. Juga harus memastikan bahwa pihak pengiriman yang mereka rekrut memiliki kebijakan yang jelas dan tegas terkait tanggung jawab mereka dalam mengatasi kasus pencurian barang.
13	*Hardware*	Adanya eror atau kerusakan pada sensor fingerprint perangkat user	8.16	kegiatan pemantauan akan dilakukan secara terus-menerus terhadap perilaku anomali pada sistem, termasuk sensor fingerprint. Dengan melakukan pemantauan yang cermat, manajemen sistem dapat mendeteksi segera adanya masalah pada sensor fingerprint dan mengambil tindakan korektif untuk untuk memperbaikinya, sehingga proses pembayaran pelanggan tidak terganggu.
14	*People*	Admin shopee kurang memahami cara kerja sistem pesanan dalam aplikasi	6.3	Meningkatkan kesadaran, pendidikan, dan pelatihan mengenai cara kerja sistem pesanan dalam aplikasi Shopee bagi admin Shopee yang bertanggung jawab menangani masalah pesanan. Pelatihan yang ditingkatkan akan membantu admin Shopee memahami sistem dengan lebih baik, mempercepat proses penanganan masalah pesanan, dan meningkatkan efisiensi operasional secara keseluruhan
15	*Software*	Saat membuka bagian saldo shopeepay tidak menampilkan nominal hanya blank	5.24	Menginformasikan kepada pihak IT atau keamanan informasi tentang masalah ini untuk memulai proses penanganan. Mereka akan mengevaluasi penyebab masalah, mengambil tindakan perbaikan yang diperlukan, dan memulihkan fungsi normal dari saldo ShopeePay.

16	*People*	Tidak adanya panduan pengguna seputar antarmuka dan fitur, serta susunan fitur yang rumit	6.3	Menyediakan panduan pengguna yang lengkap dan mudah dipahami tentang antarmuka dan fitur aplikasi. Melalui pelatihan dan pendidikan yang memadai, pengguna baru akan lebih mudah memahami cara menggunakan aplikasi, mengurangi kesulitan dalam navigasi, dan mempercepat adaptasi mereka terhadap fitur-fitur yang tersedia
17	*Information/ Data*	Konten yang tidak sesuai dengan kebijakan atau pedoman yang ada pada aturan aplikasi	5.10	Memastikan bahwa setiap konten yang diunggah sesuai dengan kebijakan dan pedoman yang ada, sehingga mengurangi risiko konten yang tidak sesuai dan kesulitan dalam proses unggahan foto/video.
18	*Software*	Gangguan login karena faktor seperti kualitas kamera yg rendah, sensor cahaya , jarak, dll	8.5	Mengimplementasikan metode autentikasi yang lebih fleksibel atau memperkenalkan opsi alternatif untuk login, seperti penggunaan kata sandi sebagai cadangan jika autentikasi biometrik gagal karena faktor-faktor seperti kualitas kamera yang rendah atau kondisi lingkungan yang tidak mendukung.
19	*Hardware*	Spesifikasi maupun sistem operasi device user tidak memenuhi syarat minimum	8.4	Akses terhadap kode sumber, alat pengembangan, dan perpustakaan perangkat lunak akan dikelola dengan baik. Hal ini akan memungkinkan organisasi untuk melakukan penyesuaian
20	*Hardware*	Kapasitas memori tidak cukup atau keterbatasan memori internal/eksternal untuk update	8.6	Pengelolaan kapasitas akan memantau dan menyesuaikan penggunaan sumber daya sesuai dengan kebutuhan kapasitas saat ini dan yang diharapkan. memastikan bahwa kapasitas memori yang cukup tersedia untuk melakukan pembaruan dengan efektif dan mengurangi risiko kegagalan pembaruan karena keterbatasan kapasitas memori.

Sumber: hasil olah data penulis

KESIMPULAN

Penelitian ini bertujuan untuk menganalisis risiko penggunaan aplikasi Shopee dengan menggunakan metode Failure Mode and Effect Analysis (FMEA) serta ISO 27001 tahun 2022 berdasarkan data yang diperoleh melalui teknik data scrapping. Melalui teknik data scrapping, penelitian ini berhasil mengidentifikasi berbagai mode kegagalan yang sering dialami oleh pengguna aplikasi Shopee. Risiko utama yang ditemukan termasuk masalah teknis seperti bug dan crash aplikasi, kesulitan dalam proses pembayaran, dan keterlambatan dalam pengiriman barang. Selain itu, masalah keamanan data dan privasi pengguna juga menjadi perhatian penting. Hasil penilaian menunjukkan beberapa risiko dengan nilai Risk Priority Number (RPN) sangat tinggi di setiap kategori aset, di kategori informasi/data dengan nilai 378 terkait kurangnya perhatian akan stock barang, pada kategori people dengan nilai 320 terkait user salah dan tidak mengingat alamat tujuan, kategori hardware dengan nilai 252 terkait jaringan yang tidak stabil

menyebabkan aplikasi berjalan tidak baik, dan pada kategori terakhir yaitu software dengan nilai 240 terkait kesalahan input pengguna dalam informasi pembayaran. Mengindikasikan bahwa risiko tersebut perlu mendapatkan perhatian khusus dan tindakan mitigasi yang segera. Implementasi langkah-langkah mitigasi yang diusulkan diharapkan dapat meningkatkan kualitas dan keandalan aplikasi Shopee. Evaluasi terhadap efektivitas mitigasi melalui survei pengguna dan analisis tren data menunjukkan adanya peningkatan dalam pengalaman pengguna dan penurunan insiden kegagalan. enelitian ini memberikan kontribusi signifikan dalam pemahaman dan pengelolaan risiko aplikasi e-commerce. Dengan menggabungkan metode FMEA dan teknik data scrapping, penelitian ini mampu memberikan analisis yang lebih komprehensif dan berbasis data nyata. Hasilnya dapat digunakan oleh pengembang Shopee untuk meningkatkan kualitas aplikasi dan memberikan pengalaman yang lebih baik dan aman bagi pengguna.

DAFTAR PUSTAKA

Munaroh, L., Amrozi, Y., & Nurdian, R. A. (2020) "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013", *Technomedia Journal*, *5*(2 Februari), 167–181. https://doi.org/10.33050/tmj.v5i2.1377

Haekal, B. V., Ernawati, I., & Chamidah, N. (2021) "Klasifikasi kepuasan pengguna layanan aplikasi shopee menggunakan metode decision tree C4.5", *Informatik : Jurnal Ilmu Komputer*, *17*(3), 188. https://doi.org/10.52958/iftk.v17i3.3648

Stamatis, D.H. (2019) "Risk Management Using Failure Mode and Effect Analysis (FMEA)"

Novianti, D. (2019) "PENGEMBANGAN KERANGKA MANAJEMEN RISIKO PADA PERBANKAN SYARIAH," *Asy Syar'iyyah: Jurnal Ilmu Syari'ah dan Perbankan Islam*, 4(1), pp. 46–67.

Rehatalanit, Y. L. R. "Peran e-commerce dalam pengembangan bisnis." *Jurnal Teknologi Industri* 5 (2021).

Atmojo, S.A. and Manuputty, A.D. (2020) "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," Jurnal Teknik Informatika dan Sistem Informasi, 7(3), pp. 546–558. Available at: http://jurnal.mdp.ac.id.

Pangestuti, D.C., Nastiti, H. and Husniaty, R. (2022) "Analisis Risiko Operasional Dengan Metode FMEA," *Jurnal Akuntansi, Ekonomi dan Manajemen Bisnis*, 10(2), pp. 177–186.

Kartikasari, V. and Romadhon, H. (2019) "Analisa Pengendalian dan Perbaikan Kualitas Proses Pengalengan Ikan Tuna Menggunakan Metode Failure Mode And Effect Analysis (FMEA) dan Fault Tree Analysis (FTA) Studi kasus di PT XXX Jawa Timur," *Journal of Industrial View*, 1(1), pp. 1–10.

Aprianti, S., Sari, R.P. and Rusi, I. (2023) "Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013," *Jurnal Buana Informatika*, 14(1), pp. 50–59.

Anshori, F.A., Suprapto and Reza Perdanakusuma, A. (2019) "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 3(2), pp. 1701–1707. Available at: http://j-ptiik.ub.ac.id.