MANAJEMEN RISIKO

WARNET TERANET

Politeknik Caltex Riau

Dosen/PLP :

Mutia Sari Zulvi, S.S.T., M.M.S.I

Disusun Oleh :

Amelia Devira (2357301011)

Amelia Dhea Putri (2357301012)

Raina Fadila (2357301107)

Kelas : 2 SI C

PRODI SISTEM INFORMASI
JURUSAN TEKNOLOGI INFORMASI

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang terus berkembang pesat, kebutuhan akan akses internet menjadi sangat penting bagi masyarakat. Warnet (warung internet) masih memiliki peran strategis di beberapa daerah, khususnya di kawasan yang memiliki keterbatasan akses internet pribadi atau fasilitas digital lainnya. Salah satu contoh nyata dapat ditemukan di kota Pekanbaru, tepatnya di Jalan Sembilang, di mana masih terdapat warnet yang aktif melayani berbagai kebutuhan pengguna seperti keperluan bermain game online, mengerjakan tugas, mencetak dokumen, hingga mengakses layanan pemerintahan secara digital.

Namun, di tengah meningkatnya tuntutan efisiensi dan kenyamanan layanan, banyak warnet yang belum menerapkan sistem manajemen yang optimal. Proses reservasi komputer, pencatatan waktu penggunaan, dan pembayaran masih dilakukan secara manual, yang berisiko menyebabkan antrian panjang, kesalahan pencatatan, serta kurangnya transparansi terhadap penggunaan layanan. Selain itu, pelanggan juga tidak memiliki kemudahan dalam memesan atau memeriksa ketersediaan komputer secara online sebelum datang ke lokasi.

Permasalahan ini menjadi dasar penting dalam pengembangan sistem informasi reservasi dan manajemen operasional warnet secara digital. Dengan penerapan sistem yang terkomputerisasi, diharapkan dapat meningkatkan efisiensi pelayanan, memberikan kemudahan bagi pelanggan dalam melakukan pemesanan dan pembayaran, serta membantu pemilik warnet dalam mengelola operasional dan laporan keuangan secara lebih efektif.

1.2 Tujuan Masalah

- Mengurangi Antrian dan Kesalahan Pencatatan
  Proses pencatatan waktu penggunaan komputer dan pembayaran yang masih manual sering menyebabkan antrian panjang dan kesalahan hitung durasi. Dengan sistem digital, waktu pemakaian dan biaya dapat dicatat otomatis secara real-time dan lebih akurat.
- Mempermudah Pengelolaan oleh Pemilik Warnet
  Pemilik warnet sering kesulitan dalam memantau penggunaan komputer, pemasukan harian, serta mendeteksi komputer yang bermasalah. Tujuan ini mendorong hadirnya sistem yang dapat membantu pemilik melihat laporan operasional secara lengkap dan efisien.
- Meningkatkan Pelayanan kepada Pelanggan
  Pelanggan saat ini harus datang langsung ke warnet untuk mengecek ketersediaan komputer. Dengan sistem reservasi online dan pembayaran digital, pelanggan dapat mengakses layanan dengan lebih mudah, cepat, dan nyaman.

BAB II
LANDASAN TEORI

2.1 IT Risk Assessment

Risk assessment dalam usaha warnet adalah metode yang digunakan untuk mengenali dan meminimalkan risiko yang dapat mengganggu operasional layanan teknologi informasi, seperti gangguan pada sistem billing, koneksi internet, maupun perangkat komputer. Proses ini menjadi bagian penting dari perencanaan pemulihan ketika terjadi gangguan layanan atau kerugian operasional. Dalam operasional harian warnet, risiko dapat berupa efek negatif dari berbagai kejadian, seperti server down, serangan malware, atau human error yang dapat menimbulkan kerugian finansial dan menurunkan kepuasan pelanggan. Oleh karena itu, penting bagi pemilik usaha untuk melakukan penilaian risiko guna memastikan kontinuitas layanan dan menjaga kepercayaan pelanggan.

2.2 Tahapan Identifikasi Risk Assessment

Berikut merupakan tahapan Identifikasi Risk Assessment:

1. Mengidentifikasi Sebuah Risiko
   Langkah pertama adalah mengidentifikasi berbagai potensi risiko yang mungkin timbul dari aset-aset TI yang digunakan, seperti PC client, server, jaringan LAN, dan perangkat jaringan lainnya. Risiko bisa berasal dari dalam, seperti kerusakan hardware atau kesalahan staf, maupun dari luar seperti pemadaman listrik atau serangan siber. Identifikasi dilakukan secara menyeluruh agar semua potensi gangguan tercakup.
2. Menganalisis Sebuah Risiko
   Setelah risiko dikenali, langkah berikutnya adalah menganalisis karakteristik dari masing-masing risiko, seperti kemungkinan terjadinya, potensi dampaknya terhadap operasional layanan, dan tingkat kerentanannya. Misalnya, risiko gangguan jaringan memiliki frekuensi tinggi dan berdampak langsung pada layanan pelanggan, sehingga perlu dianalisis lebih dalam untuk mengetahui titik lemahnya.
3. Memberikan Evaluasi Terhadap Risiko
   Tahapan akhir adalah mengevaluasi setiap risiko yang telah dianalisis untuk menentukan prioritas penanganannya. Risiko dengan tingkat dampak dan kemungkinan yang tinggi akan menjadi fokus utama mitigasi, seperti menyiapkan koneksi internet cadangan, backup server, atau pelatihan staf dalam menangani gangguan teknis. Hasil evaluasi ini menjadi dasar dalam menyusun strategi manajemen risiko di warnet secara keseluruhan.

2.3 Method Failure Mode and Effects Analysis (FMEA)

Menurut Gaspersz (2002), Failure Mode and Effects Analysis (FMEA) merupakan metode analisis risiko yang digunakan untuk mengidentifikasi bagaimana komponen-komponen dalam suatu organisasi, seperti peralatan maupun sistem, dapat mengalami kegagalan operasional serta menilai dampak yang ditimbulkan akibat kegagalan tersebut.

FMEA membantu organisasi dalam memahami potensi risiko yang ada, baik dari aspek teknis maupun operasional, sehingga dapat disusun strategi pencegahan dan penanggulangan yang efektif. Hasil dari penerapan FMEA berupa rekomendasi perbaikan untuk mencegah atau meminimalisir dampak dari risiko yang mungkin terjadi. Dengan demikian, metode ini bertujuan untuk meningkatkan keselamatan dan keandalan terhadap peralatan, fasilitas, maupun sistem secara keseluruhan.

Berikut ini adalah langkah-langkah FMEA yang diterapkan dalam konteks studi kasus usaha warnet:

Langkah	Deskripsi
1	Menentukan proses yang mempunyai risiko tinggi dalam operasional warnet dan membentuk tim (Select a high-risk process and assemble a team)seperti proses billing, jaringan internet, dan proteksi sistem. Tim terdiri dari teknisi jaringan dan admin operasional
2	Menyusun diagram proses (Diagram the process) diagram mencakup alur penggunaan PC oleh pelanggan, login billing, hingga koneksi internet
3	Brainstorming potensi failure modes dan akibat-akibat yang ditimbulkan (Brainstorm potential failure modes and determine their effects) seperti billing tidak bisa login, internet mati, antivirus tidak aktif, dan komputer crash
4	Menentukan prioritas failure modes (Prioritize failure modes) dilakukan dengan menghitung Risk Priority Number (RPN). Contoh prioritas tinggi: • Deep Freeze tidak aktif (RPN: 360) • Modem tidak konek internet (RPN: 320) • Billing tidak bisa login (RPN: 315)
5	Identifikasi akar penyebab masalah dari failure modes (Identify root causes of failure modes) meliputi lisensi expired, gangguan provider, spesifikasi rendah, atau kesalahan admin
6	Membuat rancangan ulang proses (Redesign the process) seperti menambahkan SOP pengecekan lisensi, pengadaan koneksi internet cadangan, dan automasi sistem proteksi

7	Analisa dan pengujian proses baru (Analyze and test the new process) dilakukan simulasi kesalahan dan pengujian sistem baru untuk menjamin efektivitas
8	Implementasi dan monitoring rencana ulang proses (Implement and monitor the new process) melibatkan checklist harian, log sistem, dan evaluasi berkala oleh admin teknis

Tabel 1. Langkah-Langkah *Failure Mode and Effect Analysis*

BAB III
METODE PENELITIAN

3.1 Pengumpulan dan Pengolahan Data

Metode analisis risiko dalam penelitian ini menggunakan pendekatan Failure Mode and Effect Analysis (FMEA), yaitu metode yang digunakan untuk mengidentifikasi dan menganalisis potensi kegagalan pada suatu sistem atau aset teknologi informasi sebelum menimbulkan kerugian yang lebih besar. FMEA bertujuan untuk mengenali titik-titik lemah dari proses atau aset TI, serta memberikan rekomendasi perbaikan dan pencegahan terhadap potensi kegagalan tersebut.

Pengumpulan data dilakukan melalui:

- Wawancara langsung dengan pemilik dan operator Warnet Teranet yang berlokasi di Jalan Sembilang, Pekanbaru, untuk mendapatkan informasi terkait aset-aset TI yang digunakan, pengalaman kegagalan sistem, dan langkah-langkah penanganan yang telah diterapkan sebelumnya.
- Observasi lapangan untuk meninjau secara langsung kondisi perangkat keras, perangkat lunak, jaringan, serta infrastruktur fisik pendukung seperti ruang server, kabel LAN, dan sistem kelistrikan.
- Studi dokumentasi internal, termasuk daftar inventaris aset, laporan gangguan teknis, dan konfigurasi perangkat jaringan serta software billing yang digunakan dalam operasional harian.

Data-data yang diperoleh kemudian digunakan untuk menyusun daftar moda kegagalan, penyebab, serta dampak terhadap operasional warnet, yang selanjutnya dianalisis menggunakan perhitungan nilai Severity (S), Occurrence (O), dan Detection (D) untuk menghasilkan angka Risk Priority Number (RPN). Hasil perhitungan ini menjadi dasar dalam menentukan prioritas risiko serta strategi mitigasinya.

3.2 Review Proses

Pada tahapan ini dilakukan observasi langsung dan diskusi dengan operator teknis serta pengelola warnet di Jalan Sembilang, Pekanbaru untuk mengetahui kendala dan masalah utama yang sering terjadi dalam operasional harian. Berdasarkan hasil tersebut, ditemukan bahwa terdapat beberapa gangguan sistem dan infrastruktur yang berulang kali terjadi dan mempengaruhi kelancaran layanan kepada pelanggan.

Adapun daftar aset yang ada di warnet dan dijadikan sebagai aspek kritis karena perannya yang vital dalam proses operasional adalah sebagai berikut:

Aset Kritis	**Alasan**
PC Client (Komputer Pengguna)	Digunakan langsung oleh pelanggan, inti layanan warnet
PC Server / Admin	Untuk mengelola billing, kontrol jaringan dan user client
Switch	Backbone jaringan lokal, jika gagal, semua koneksi bisa terputus
Modem / ONT Internet	Penghubung ke internet, tanpa ini tidak bisa akses online
Billing Warnet Software	Mengatur waktu pemakaian, login user, tarif, dan kontrol komputer
Jaringan LAN (kabel UTP, konektor)	Menghubungkan semua perangkat client dan server
Headset / Speaker	Digunakan untuk hiburan, gaming, tidak semua pelanggan membutuhkannya
Antivirus & DeepFreeze	Penting, tapi tidak berdampak langsung dalam jangka pendek

Tabel 2. Daftar Aset Kritis Warnet Teranet

Dari aset kritis pada tabel diatas, setiap aset akan dianalisis untuk menentukan potensi kegagalan yang dapat terjadi menggunakan metode Failure Mode and Effect Analysis (FMEA). Setiap potensi kegagalan akan dinilai berdasarkan tiga parameter: Occurrence (frekuensi kejadian), Severity (tingkat keparahan), dan Detection (kemampuan mendeteksi kerusakan), yang kemudian digunakan untuk menghitung nilai Risk Priority Number (RPN) sebagai dasar prioritas penanganan risiko.

3.3 Identifikasi Potensi Failure Mode

Identifikasi failure mode atau bentuk kegagalan dilakukan berdasarkan hasil wawancara dengan pemilik dan operator Warnet Teranet, serta melalui observasi langsung terhadap infrastruktur dan aset-aset teknologi informasi yang digunakan dalam operasional harian. Tahapan ini bertujuan untuk mengenali berbagai gangguan yang pernah terjadi maupun yang berpotensi besar terjadi pada aset-aset TI yang memiliki pengaruh signifikan terhadap kelancaran layanan warnet.

Berdasarkan data yang diperoleh, beberapa contoh potensi kegagalan yang telah atau berisiko besar terjadi di Warnet Teranet antara lain:

- PC Client tidak bisa digunakan, disebabkan oleh overheat, kerusakan hardware, atau infeksi virus. Hal ini menyebabkan pelanggan tidak dapat menggunakan layanan, sehingga menurunkan pendapatan harian warnet dan menyebabkan antrian.
- Software billing error atau tidak dapat login, biasanya disebabkan oleh database corrupt atau software tidak ter-update. Dampaknya adalah proses pencatatan waktu dan tarif pelanggan menjadi kacau, bahkan berpotensi menyebabkan kehilangan data transaksi dan kerugian finansial.
- Modem atau ONT internet tidak berfungsi, akibat gangguan jaringan, kabel putus, atau kerusakan perangkat. Hal ini menyebabkan seluruh aktivitas online seperti browsing, gaming, dan pencetakan dokumen terganggu atau terhenti.
- Switch jaringan rusak atau overload, menyebabkan semua komputer client kehilangan koneksi ke server maupun internet. Hal ini secara langsung mematikan fungsi utama warnet.
- Kabel LAN longgar atau rusak, sering terjadi akibat pemasangan yang tidak rapi atau penggunaan jangka panjang tanpa pengecekan. Akibatnya adalah komputer tidak dapat terhubung ke jaringan billing dan server.
- Antivirus tidak aktif atau gagal update, karena lisensi habis, tidak adanya fitur update otomatis, atau konflik dengan software lain. Hal ini meningkatkan risiko serangan malware, pencurian data, dan kerusakan sistem.
- Tidak adanya backup berkala, yang menyebabkan data pelanggan dan log penggunaan rentan hilang saat terjadi gangguan perangkat atau sistem. Hal ini dapat menyulitkan rekap transaksi atau bukti layanan.

Setiap potensi kegagalan tersebut diidentifikasi sebagai failure mode yang akan dianalisis lebih lanjut menggunakan metode FMEA, guna menentukan tingkat keparahan, kemungkinan kejadian, dan tingkat deteksi. Hasil analisis akan digunakan untuk menyusun strategi mitigasi serta prioritas penanganan risiko berdasarkan nilai Risk Priority Number (RPN).

3.4 Penyebab Kegagalan Potensial

Beberapa penyebab utama dari potensi kegagalan sistem teknologi informasi di Warnet Teranet berhasil diidentifikasi melalui hasil wawancara dengan operator warnet serta observasi langsung terhadap infrastruktur dan perangkat yang digunakan. Adapun penyebab-penyebab kegagalan tersebut meliputi:

a. Pemakaian Perangkat yang Tidak Wajar

   Komputer client sering digunakan secara terus-menerus dalam waktu lama tanpa pendinginan atau perawatan yang memadai. Hal ini mempercepat kerusakan hardware seperti kipas prosesor, RAM, atau harddisk, yang berujung pada kerusakan total unit.

b. Kurangnya Jadwal Perawatan Rutin

   Tidak adanya jadwal maintenance berkala menyebabkan perangkat seperti switch, modem, dan kabel jaringan tidak dicek kondisinya secara rutin. Akibatnya, kerusakan ringan tidak terdeteksi lebih awal hingga mengganggu operasional.

c. Ketiadaan Proteksi Keamanan Sistem

   Banyak komputer client tidak memiliki antivirus aktif atau sistem keamanan endpoint. Hal ini menyebabkan komputer sangat rentan terhadap infeksi malware dari flashdisk, browsing tidak aman, atau file dari pelanggan.

d. Human Error oleh Operator atau Pelanggan

   Kesalahan penggunaan perangkat oleh operator atau pelanggan, seperti mencabut kabel sembarangan, membuka situs tidak aman, atau menggunakan software bajakan, menyebabkan gangguan sistem yang sering berulang.

e. Tidak Adanya Monitoring Backup dan Otomatisasi

   Sistem billing dan data pelanggan tidak memiliki mekanisme backup otomatis maupun pemantauan terhadap keberhasilan backup. Hal ini sangat berisiko jika terjadi gangguan sistem atau kerusakan perangkat, karena data tidak dapat dipulihkan.

f. Kabel dan Infrastruktur Fisik yang Tidak Rapi

   Pemasangan kabel LAN yang tidak tertata rapi dan tidak terlindungi dengan baik menyebabkan koneksi mudah terganggu, baik karena tertarik, lepas, atau rusak akibat gangguan fisik di area pelanggan.

g. Ketergantungan pada Satu Jalur Koneksi

   Tidak adanya jalur cadangan atau sistem redundansi baik untuk koneksi internet maupun switch jaringan, menyebabkan seluruh layanan terhenti saat terjadi kerusakan pada satu titik.

Penyebab-penyebab kegagalan ini menunjukkan bahwa meskipun perangkat dan sistem yang digunakan masih berfungsi, kelemahan dalam pengelolaan, perawatan, dan kebijakan operasional menjadi faktor utama yang meningkatkan risiko terjadinya gangguan sistem. Oleh karena itu, penguatan dalam kontrol dan monitoring operasional menjadi hal penting untuk ditindaklanjuti dalam proses mitigasi risiko menggunakan FMEA.

Setiap kegagalan yang terjadi pada sistem dan aset Teknologi Informasi (TI) di Warnet Teranet tentu menimbulkan dampak yang beragam, tergantung pada jenis aset yang mengalami gangguan dan peran aset tersebut dalam operasional harian. Efek dari kegagalan ini tidak hanya berdampak pada teknisi atau staf pengelola, tetapi juga langsung dirasakan oleh pelanggan, baik dalam bentuk keterlambatan layanan, gangguan akses internet, maupun ketidakpuasan secara keseluruhan. Oleh karena itu, penting untuk memahami dampak dari setiap potensi kegagalan, agar pengelola warnet dapat menyusun langkah pencegahan dan penanganan yang efektif untuk menjaga kelangsungan layanan dan reputasi usaha

3.5 Identifikasi Effect Kegagalan Potensial

Adapun beberapa contoh efek atau dampak potensial dari kegagalan sistem TI di Warnet Teranet antara lain:

1. Terganggunya layanan pelanggan
   Jika komputer client tidak dapat digunakan karena rusak atau sistem billing tidak berjalan, maka pelanggan tidak dapat mengakses layanan. Hal ini dapat menyebabkan antrian panjang dan pelanggan beralih ke tempat lain.
2. Kehilangan data transaksi dan penggunaan waktu
   Gagalnya software billing atau tidak berfungsinya backup menyebabkan hilangnya data lama dan log pemakaian, yang berakibat pada kesalahan dalam penagihan dan pengelolaan laporan keuangan.
3. Terputusnya koneksi internet secara keseluruhan
   Jika modem, ONT, atau switch mengalami gangguan, maka semua komputer dalam jaringan tidak akan bisa mengakses internet. Dampaknya adalah seluruh operasional layanan terhenti, termasuk browsing, gaming, atau pencetakan dokumen.
4. Penurunan performa sistem secara menyeluruh
   Kabel LAN yang rusak, spesifikasi komputer yang tidak memadai, serta virus yang tersebar pada client akan menyebabkan sistem berjalan lambat, tidak responsif, dan menurunkan kepuasan pelanggan.
5. Gangguan pada koordinasi antar staf
   Jika jaringan internal terganggu atau komputer admin tidak dapat diakses, maka operator tidak bisa melakukan kontrol terhadap billing, status komputer client, dan pencatatan data operasional.
6. Meningkatnya keluhan pelanggan dan hilangnya kepercayaan
   Gangguan berulang tanpa penanganan yang tepat akan menyebabkan pelanggan merasa kecewadan berpotensi tidak kembali menggunakan layanan warnet tersebut.

Dampak-dampak di atas menunjukkan bahwa setiap kegagalan pada sistem TI memiliki konsekuensi yang dapat memengaruhi langsung keberlangsungan usaha. Oleh karena itu, pengelolaan risiko dan sistem deteksi dini sangat diperlukan untuk memastikan layanan berjalan optimal dan pelanggan tetap puas.

3.6 Menentukan Seferity dan Rating Keparahan

Berdasarkan hasil observasi dan diskusi dengan salah satu staf teknis di warnet, maka ditentukan tingkat keparahan atau severity dari setiap potensi kegagalan yang terjadi pada sistem operasional. Penilaian ini dilakukan menggunakan skala ordinal 1 hingga 10, di mana semakin besar dampak dari suatu kegagalan terhadap kelangsungan layanan, maka semakin tinggi pula nilainya.
Berikut ini merupakan hasil penilaian rating keparahan dari masing-masing potensi kegagalan yang dirangkum dalam Tabel 2:

Tabel 2. Hasil Severity

No	Potensi Kegagalan	Severity atau Rating Keparahan
1	PC tidak bisa dihidupkan	3
2	PC Admin hang / lambat	7
3	Printer hasil cetak buram / tidak bisa cetak	6
4	Headset suara tidak keluar / rusak	5
5	Modem / ONT Internet tidak konek internet	7
6	Switch port tidak berfungsi	7
7	Billing Software tidak bisa login / error	8
8	Antivirus / Deep Freeze tidak aktif / update	9
9	Office tidak bisa dibuka / crash	5
10	Staff salah input / tidak hadir	6

Dilihat pada tabel 2, potensi kegagalan dengan tingkat keparahan tertinggi adalah tidak aktif atau tidak ter-updatenya antivirus, dengan nilai severity 9, karena dapat menyebabkan kerusakan sistem yang meluas, serangan virus, bahkan kehilangan data penting. Disusul oleh kegagalan sistem billing akibat lisensi yang tidak aktif (severity 8) yang menghambat proses transaksi

pelanggan. Selain itu, kerusakan pada perangkat jaringan seperti modem, switch, dan komputer admin juga memiliki severity tinggi (**7**) karena secara langsung mengganggu aktivitas pelanggan dan berdampak pada pendapatan usaha. Sementara itu, masalah seperti headset rusak atau aplikasi tidak terbuka berada pada tingkat keparahan menengah karena meskipun mengganggu, tidak langsung menghentikan proses utama. Oleh karena itu, risiko-risiko dengan severity tinggi harus menjadi prioritas dalam penanganan dan pencegahan agar tidak mengganggu kelangsungan operasional warnet secara keseluruhan.

3.7 Menentukan Occurant atau Rating Kejadian

Kuisioner telah disebarkan kepada 2 orang staf untuk menghitung nilai *occurrent* terhadap masing-masing potensial.

Tabel 3. Hasil Occurent

No	Potensi Kegagalan	Penyebab Kegagalan	*Occurent*
1	PC tidak bisa hidup	Terlalu banyak aplikasi	3
		Crash akibat overheat	3
2	PC Admin hang / lambat	Spesifikasi rendah	2
		Terlalu banyak task berjalan	2
3	Printer hasil buram / tidak jelas	Tinta habis	1
		Kertas macet	1
		Tinta kering	1
4	Headset tidak keluar suara	Kabel rusak	5
		Jack audio longgar / putus	5
5	Modem tidak konek internet	Gangguan provider	5
		Kabel rusak / port ONT bermasalah	5
6	Switch tidak berfungsi	Port rusak	1
		Tidak ada port cadangan	1

7	Billing tidak bisa login	Lisensi expired	5
		Monitoring lisensi tidak dilakukan	5
8	Deep Freeze tidak aktif	Dimatikan / di-nonaktifkan manual	5
		Lupa update	5
9	Office tidak terbuka / crash	Software corrupt	5
		Tidak update otomatis	5
10	Staff tidak hadir / salah input	Sakit atau cuti mendadak	6
		Kurang pelatihan sistem billing	6

Berdasarkan Tabel 3, nilai *occurrence* tertinggi terdapat pada potensi kegagalan modem tidak konek internet**,** billing tidak bisa login**,** deep freeze tidak aktif**,** office tidak terbuka, dan headset tidak berfungsi, yang semuanya memiliki skor sebesar 5. Gangguan pada komponen-komponen ini dapat langsung menghambat layanan warnet, seperti akses internet terputus, sistem transaksi tidak berjalan, hingga kerusakan sistem akibat proteksi yang tidak aktif. Oleh karena itu, risiko-risiko ini perlu menjadi prioritas penanganan.

3.8 Identifikasi Pencegahan Yang Telah Dilakukan

Berdasarkan hasil wawancara terhadap 2 orang staf, diperoleh informasi pencegahan yang telah dilakukan terhadap kegagalan, yaitu:

Tabel 4. Identifikasi Pencegahan

No	Potensi Kegagalan	Penyebab Kegagalan	Identifikasi pencegahan saat ini
1	PC tidak bisa dihidupkan	Terlalu banyak aplikasi, Virus	Pengurangan aplikasi berjalan dan pemasangan antivirus & deep freeze
2	PC Admin hang / lambat	Spesifikasi rendah, Terlalu banyak proses	Upgrade spesifikasi & pembatasan aplikasi berjalan
3	Printer hasil cetak buram / tidak bisa mencetak	Tinta habis, Kertas macet	Pengecekan dan perawatan rutin pada tinta dan kertas
4	Headset tidak keluar suara / rusak	Kabel rusak, Kualitas rendah	Pemeriksaan koneksi & penggantian headset secara berkala
5	Modem / ONT tidak konek internet	Gangguan provider, Kabel longgar	Koordinasi dengan provider & pengecekan koneksi fisik secara berkala
6	Switch port tidak berfungsi	Port rusak, Sambungan tidak stabil	Gunakan port cadangan dan pastikan koneksi LAN stabil
7	Billing Software tidak bisa login / error	Lisensi expired, Sistem tidak update	Monitoring masa aktif lisensi & update berkala

8	Antivirus / Deep Freeze tidak aktif / update	Dimatikan manual, Lupa update	Proteksi admin dan update berkala oleh admin
9	Office tidak bisa dibuka / crash	Aktivasi gagal, Aplikasi corrupt	Lakukan update otomatis dan pengecekan instalasi
10	Staff salah input / tidak hadir	Kurang pelatihan, Sakit	Pelatihan rutin dan sistem pengganti saat staf berhalangan

Berdasarkan tabel 4 identifikasi pencegahan, sebagian besar potensi kegagalan telah memiliki upaya pencegahan, seperti pemasangan antivirus, pembatasan aplikasi, dan pelatihan staf. Namun, beberapa masih belum optimal, misalnya update antivirus yang tidak rutin, lisensi software yang tidak terpantau, serta kesalahan input akibat kurangnya pelatihan. Hal ini menunjukkan perlunya peningkatan pada sistem pemantauan, pemeliharaan rutin, dan SOP operasional harian.

3.9 Identifikasi Metode Deteksi

Kuisioner telah disebarkan kepada 2 orang staf untuk menghitung nilai *occurrent* terhadap masing-masing potensial. Detail perhitungan dapat dilihat pada lampiran. sedangkan untuk hasil *Occurent* dapat dilihat pada tabel dibawah ini.

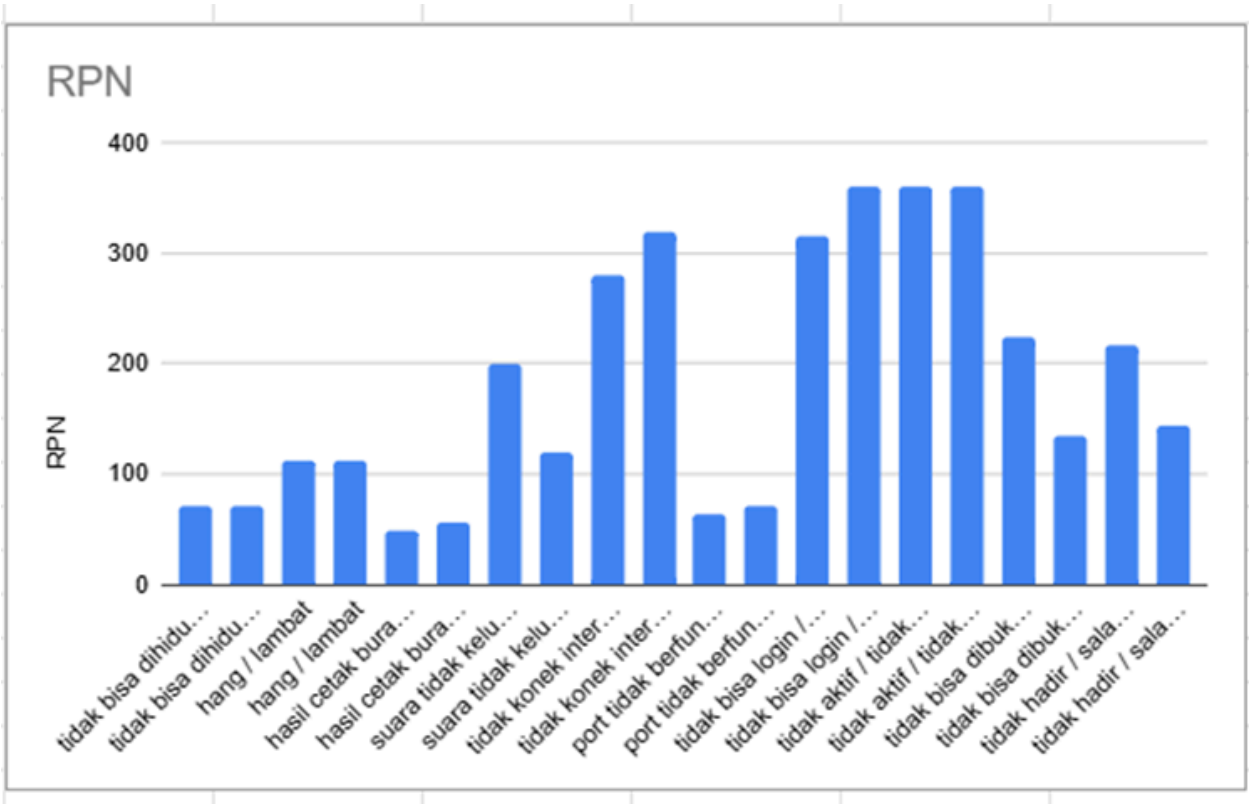
Tabel 5. Hasil Deteksi

No	Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan Saat Ini	Deteksi
1	PC tidak bisa dihidupkan	Terlalu banyak aplikasi dan infeksi virus	Aplikasi dibatasi, antivirus & Deep Freeze diaktifkan	8
2	PC Admin hang / lambat	Spesifikasi rendah, Terlalu banyak proses	Upgrade spesifikasi & pembatasan aplikasi berjalan	8
3	Printer hasil cetak buram / tidak bisa	Tinta habis, Kertas macet	Pengecekan dan perawatan rutin pada	8

	mencetak		tinta dan kertas	
4	Headset tidak keluar suara / rusak	Kabel Rusak, Kualitas rendah	Pemeriksaan koneksi & pengganti headset secara berkala	8
5	Modem / ONT tidak konek internet	Gangguan provider, Kabel longgar	Koordinasi dengan provider & pengecekan koneksi fisik secara berkala	8
6	Switch port tidak berfungsi	Port rusak, Sambungan tidak stabil	Gunakan port cadangan dan pastikan koneksi LAN stabil	9
7	Billing Software tidak bisa login / error	Lisensi expired, Sistem tidak update	Monitoring masa aktif lisensi & update berkala	9
8	Antivirus / Deep Freeze tidak aktif / update	Dimatikan manual, Luoa update	Proteksi admin dan update berkala oleh admin	8
9	Office tidak bisa dibuka / crash	Aktivasi gagal, Aplikasi corrupt	Lakukan update otomatis dan pengecekan instalasi	9
10	Staff salah input / tidak hadir	Kurang pelatihan, Sakit	Pelatihan rutin dan sistem pengganti saat staff berhalangan	6

3.10 Menghitung Risk Priority Number (RPN)

Setelah kita menganalisa nilai keparahan, kegagalan, dan deteksi, maka tahapan selanjutnya adalah menentukan nilai Risk Priority Number (RPN). Nilai RPN ini menjadi dasar untuk mengetahui potensi risiko mana yang harus diprioritaskan dalam penanganan.
Nilai RPN yang tinggi menunjukkan bahwa potensi kegagalan tersebut memiliki dampak besar, sering terjadi, dan sulit terdeteksi. Oleh karena itu, diperlukan penanganan segera agar tidak mengganggu kelangsungan operasional



Gambar 2. Grafik RPN tertinggi

3.11 Prioritas Risiko Dari RPN

Setelah dilakukan perhitungan RPN, maka tahap selanjutnya dilakukan memprioritaskan risiko berdasarkan RPN yang didapatkan. Berikut ini daftar RPN yang diurutkan dari besar dan kecil. Dan RPN terbesar / high akan diprioritaskan terlebih dahulu karena akan menimbulkan kerugian yang besar.

Tabel 6. Prioritas Risiko dari RPN

No	Potensi Kegagalan	Penyebab Kegagalan	RPN	
1	Antivirus / Deep Freeze Tidak aktif / tidak update	Dimatikan / lupa update	360	*High* (Tinggi)
2	Billing Tidak bisa login / error	Lisensi expired	360	*High* (Tinggi)
3	Modem / ONT Internet Tidak konek internet	Gangguan provider	320	*High* (Tinggi)
4	Office Tidak bisa dibuka / crash	Aktivasi gagal / corrupt	225	*Moderate* (Sedang)

5	Staff Tidak hadir / salah input	Sakit / kurang pelatihan	216	*Moderate* (Sedang)
6	Headset Suara tidak keluar / rusak	Kabel rusak / kualitas rendah	200	*Moderate* (Sedang)
7	PC Admin Hang / lambat	Spesifikasi rendah	112	*Moderate* (Sedang)
8	PC Tidak bisa dihidupkan	Terlalu banyak aplikasi	72	*Low* (Rendah)
9	Switch Port tidak berfungsi	Port rusak	72	*Low* (Rendah)
10	Printer Tidak bisa cetak / hasil buram	Tinta habis / kertas macet	56	*Low* (Rendah)

3.12 Analysis FMEA (Action Plane)

Dari hasil observasi dan wawancara yang dilakukan di lokasi warnet, ditemukan beberapa potensi kegagalan yang dapat mengganggu proses operasional. Beberapa potensi kegagalan tersebut antara lain: PC tidak dapat digunakan, PC admin hang, billing software tidak dapat digunakan, internet tidak terhubung, suara headset tidak keluar, port switch tidak berfungsi, antivirus / deep freeze tidak aktif aplikasi office tidak terbuka, hingga staf yang melakukan kesalahan input. Potensi-potensi ini dapat menghambat pelayanan kepada pelanggan secara langsung. Oleh karena itu, perlu dilakukan analisis risiko menggunakan metode FMEA untuk membantu pengelola dalam meminimalisir potensi kegagalan. Berikut ini adalah penjelasan proses analisis:

1. PC Tidak Bisa Dihidupkan, menyebabkan pelanggan tidak dapat menggunakan layanan komputer secara langsung, sehingga berdampak pada pendapatan harian.

    a. Terlalu banyak aplikasi berjalan. Rekomendasi yang dapat digunakan adalah membatasi aplikasi berjalan saat startup serta memperkuat sistem antivirus agar kinerja komputer lebih stabil.

    b. Virus atau malware. Penggunaan antivirus harus dioptimalkan dan dilakukan update secara rutin agar risiko serangan sistem dapat diminimalisir. Nilai RPN sebesar 72, tergolong risiko rendah namun tetap perlu diperhatikan untuk mencegah kerusakan menyebar.

2. PC Admin Hang atau Lambat, berisiko mengganggu kelancaran operasional seperti pencatatan transaksi, laporan harian, dan aktivitas administratif lainnya.

    a. Spesifikasi perangkat rendah. Rekomendasi yang dapat diberikan adalah melakukan upgrade perangkat admin dengan spesifikasi yang sesuai kebutuhan operasional, serta

membatasi aplikasi yang berjalan di latar belakang. RPN sebesar 112, termasuk risiko sedang yang penting untuk segera ditindaklanjuti.

3. Printer Tidak Bisa Cetak , menghambat pencetakan dokumen pelanggan seperti bukti pembayaran.

   a. Tinta habis atau kertas macet. Rekomendasi: lakukan pengecekan rutin dan sediakan cadangan tinta/kertas. Nilai RPN: 56 masuk kategori risiko rendah, namun perlu diperhatikan karena berkaitan dengan layanan pelanggan.

4. Headset Rusak atau Tidak Bersuara , menurunkan kenyamanan pelanggan saat menggunakan komputer untuk hiburan.

   a. Kabel rusak atau kualitas rendah. Rekomendasi: lakukan pengecekan berkala dan gunakan headset standar minimal. Nilai RPN: 200 risiko sedang, sering dikeluhkan pelanggan.

5. Modem / ONT Tidak Terkoneksi Internet , menyebabkan seluruh komputer tidak dapat digunakan karena bergantung pada koneksi online.

   a. Gangguan provider. Rekomendasi: gunakan dua ISP dan fitur failover otomatis. Nilai RPN: 320 termasuk risiko tinggi, berdampak besar pada keseluruhan operasional.

6. Port Switch Tidak Berfungsi , menyebabkan beberapa komputer tidak dapat mengakses jaringan.
   a. Port rusak atau longgar. Rekomendasi: sediakan switch cadangan dan gunakan port alternatif. Nilai RPN: 72 termasuk risiko rendah, tetapi jika tidak segera ditangani dapat menyebar ke lebih banyak unit.
7. Billing Software Tidak Bisa Digunakan , membuat proses transaksi tidak dapat berjalan.

   a. Lisensi expired. Rekomendasi: pantau masa aktif lisensi dan backup rutin sistem. Nilai RPN: 360 termasuk risiko sangat tinggi, harus menjadi prioritas utama.

8. Antivirus dan Deep Freeze Tidak Aktif , menjadikan sistem rentan terhadap virus dan malware.
   a. Lupa update atau dinonaktifkan. Rekomendasi: aktifkan proteksi admin dan lakukan update otomatis. Nilai RPN: 360 risiko sangat tinggi, dapat menyebabkan kerusakan menyeluruh.

9. Office Tidak Bisa Dibuka , mengganggu aktivitas staf admin seperti mengetik laporan dan pengolahan data.

   a. Gagal aktivasi atau file corrupt. Rekomendasi: aktifkan update otomatis dan pastikan lisensi aktif. Nilai RPN: 225 termasuk risiko sedang, perlu diperbaiki agar efisiensi kerja meningkat.

10. Staf Tidak Hadir atau Salah Input , menyebabkan gangguan operasional dan kesalahan pada data transaksi.

   a. Kurangnya pelatihan atau kondisi kesehatan. Rekomendasi: berikan pelatihan rutin dan buat SOP pengganti staf. Nilai RPN: 216 termasuk risiko sedang**,** berkaitan langsung dengan kualitas layanan.

BAB IV
HASIL dan PEMBAHASAN

Kesimpulan

Daftar Pustaka