

# ANALISIS MANAJEMEN RISIKO DALAM PENERAPAN ENTERPRISE RESOURCE PLANNING (ERP) DENGAN METODE FMEA PADA PT XYZ

Dewi Shafitri RP Santosa<sup>1</sup>, Ghea Sekar Palupi<sup>2</sup>

<sup>1,2</sup> Jurusan Teknik Informatika/Program Studi S1 Sistem Informasi, Universitas Negeri Surabaya

<sup>1</sup>[dewi.20033@mhs.unesa.ac.id](mailto:dewi.20033@mhs.unesa.ac.id)

<sup>2</sup>[gheapalupi@unesa.ac.id](mailto:gheapalupi@unesa.ac.id)

**Abstrak—** *Dinamika bisnis modern yang cepat dan kompleks menuntut strategi manajemen risiko yang efektif untuk mendukung keberhasilan penerapan teknologi. Penelitian mengkaji penggunaan Failure Mode and Effect Analysis (FMEA) dalam manajemen risiko selama implementasi Enterprise Resource Planning (ERP) di PT XYZ, sebuah perusahaan peralatan kesehatan di Surabaya. Tujuan penelitian ini adalah untuk mengidentifikasi risiko operasional potensial dan merumuskan rekomendasi strategis untuk mitigasi risiko tersebut secara efektif. Metode penelitian ini meliputi analisis kualitatif yang berbasis wawancara mendalam dan evaluasi dokumentasi terkait. Hasil penelitian mengidentifikasi berbagai risiko dengan kategori yang berbeda-beda, yaitu risiko tinggi, sedang, dan rendah, yang masing-masing memerlukan tindakan mitigasi spesifik. Penelitian ini menemukan bahwa integrasi FMEA dan ISO 31000:2018 mampu memperkuat proses identifikasi, evaluasi, dan pengelolaan risiko secara sistematis dan terstruktur. Penelitian ini menegaskan bahwa sistem ERP, meskipun sangat penting untuk integrasi dan otomatisasi proses bisnis, tetap mengandung risiko signifikan yang memerlukan pendekatan manajemen yang cermat. Penelitian ini berkontribusi pada literatur manajemen risiko dalam implementasi ERP dan mengusulkan kerangka kerja manajemen risiko yang komprehensif untuk mengoptimalkan efisiensi organisasi dan mengurangi potensi kegagalan. Rekomendasi untuk penelitian lanjutan dan praktek industri disajikan, dengan fokus pada evaluasi risiko yang kontinu dan adaptasi kerangka kerja manajemen risiko yang efektif.*

**Kata Kunci—** *Manajemen Risiko, Failure mode and effect analysis(FMEA), Enterprise resource planning (ERP), Mitigasi risiko, Analisis kualitatif.*

## I. PENDAHULUAN

Saat ini, dunia bisnis menghadapi perubahan cepat dengan kompetisi yang semakin sengit dan perubahan dalam permintaan pelanggan, peraturan, dan teknologi. Salah satu strategi untuk menghadapi tantangan ini adalah penerapan sistem Enterprise Resource Planning (ERP), yang meningkatkan efisiensi operasional dan kesiapan organisasi. ERP adalah perangkat lunak terintegrasi yang mengelola proses bisnis dan mengotomatisasi berbagai fungsi seperti keuangan, persediaan, produksi, dan SDM, serta memberikan visibilitas data secara real-time.[1]

Penerapan ERP dapat meningkatkan performa perusahaan, namun juga menghadirkan risiko operasional yang perlu dikelola. Penelitian menunjukkan bahwa kegagalan ERP, seperti yang dialami Foxmeyer Drugs dengan SAP R/3, sering kali disebabkan oleh kurangnya pengukuran aspek kualitas

dan kinerja, integrasi, kesesuaian dengan proses bisnis, serta risiko dan keamanan[2]. Oleh karena itu, manajemen risiko sangat penting dalam memastikan keberhasilan implementasi ERP.

Manajemen risiko melibatkan identifikasi dan penilaian risiko, serta penggunaan kebijakan dan metode untuk mengelola risiko[3]. Dalam kasus PT XYZ, perusahaan alat kesehatan di Surabaya yang menerapkan ERP sejak 2022, muncul risiko terkait transaksi seperti kesalahan pembuatan PO akibat ketidaksesuaian persediaan[4]. Manajemen risiko yang tepat, berdasarkan standar internasional seperti ISO 31000, sangat penting untuk menjaga efisiensi proses bisnis dan mengurangi kesalahan.

ISO 31000 memberikan panduan untuk identifikasi dan penanganan risiko, membantu perusahaan menganalisis risiko dan menyusun rekomendasi pengelolaan risiko. Standar ini menekankan pada penciptaan dan perlindungan nilai, serta fleksibilitas untuk berbagai jenis organisasi. Metode pengendalian risiko seperti FMEA (*Failure Mode and Effect Analysis*) dapat digunakan untuk mengurangi kegagalan penerapan ERP dengan mengidentifikasi dan mengatasi masalah yang ada maupun yang potensial[5]. Dengan menerapkan ISO 31000:2018 dan FMEA, PT XYZ dapat mengelola risiko teknologi informasi dengan lebih efisien dan efektif, mengoptimalkan operasional, dan mencapai keunggulan kompetitif.

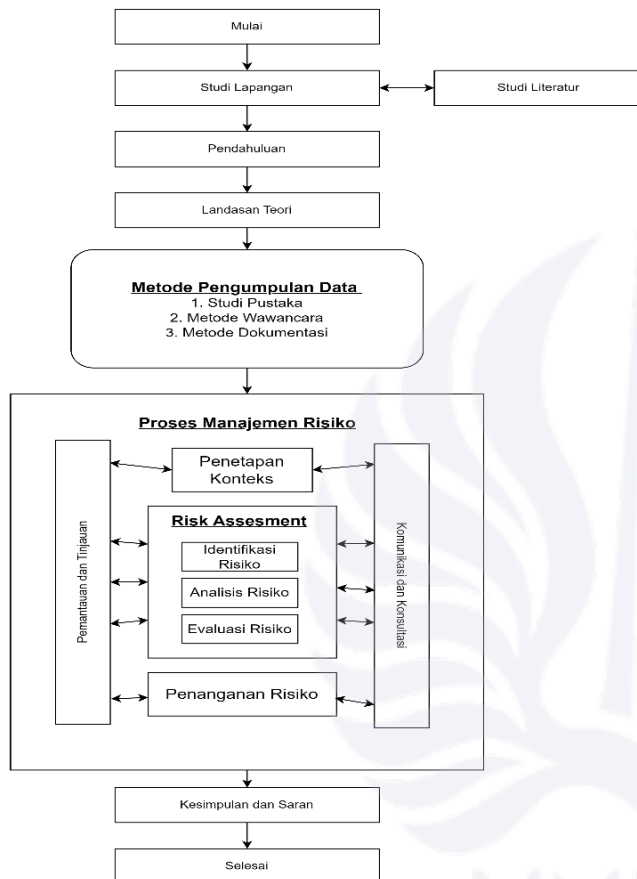
Penelitian ini bertujuan untuk mengidentifikasi risiko-risiko operasional potensial yang dapat menghambat keberhasilan penerapan ERP. Dengan mengetahui risiko-risiko tersebut, penelitian ini kemudian merumuskan rekomendasi strategis yang dapat digunakan untuk mitigasi risiko secara efektif. Pendekatan yang digunakan adalah mengintegrasikan metode Failure Mode and Effect Analysis (FMEA) dengan standar ISO 31000:2018. FMEA membantu dalam mengidentifikasi dan memprioritaskan risiko berdasarkan tingkat keparahan, frekuensi, dan kemampuan deteksi, sedangkan ISO 31000:2018 menyediakan proses yang sistematis untuk manajemen risiko.

## II. METODOLOGI PENELITIAN

Metodologi penelitian merupakan suatu tahap - tahap yang harus ditetapkan terlebih dahulu sebelum melakukan pemecahan suatu masalah yang akan dilakukan dalam melakukan suatu penelitian, sehingga penelitian dapat

dilakukan dengan terarah dan mempermudah dalam melakukan analisa permasalahan yang akan dilakukan dalam penelitian tersebut. Tahapan yang ada dalam penelitian ini antara lain yaitu langkah penelitian, flowchart penelitian, jenis penelitian, jenis data, dan teknik pengumpulan data.

Untuk memecahkan suatu masalah dalam melakukan penelitian, langkah-langkah sistematis diperlukan agar pendekatan dan model dari permasalahan tersebut dapat diuraikan. Langkah-langkah tersebut adalah sebagai berikut



Gbr. 1 Langkah Penelitian.

Uraian lankah penelitian ini adalah sebagai berikut :

1) *Studi Lapangan*, pada tahap ini dilakukan pengamatan pada perusahaan dengan cara interview seorang pekerjanya untuk mengetahui proses penggunaan sistem ERP dan mengetahui upaya pengendalian kualitasnya yang dilakukan perusahaan.

2) *Studi Literatur*, mengumpulkan referensi dan teori-teori yang relevan sebagai landasan penelitian.

3) *Pengumpulan Data*, Mengumpulkan data melalui wawancara mendalam dan evaluasi dokumentasi yang relevan.

4) *Proses Manajemen Risiko*, Proses manajemen risiko mengacu pada ISO 31000:2018. Untuk *risk assessment* sepenuhnya menggunakan metode *Failure Mode and Effect Analysis* (FMEA).

5) *Kesimpulan dan Saran*, Menafsirkan hasil analisis untuk mengidentifikasi risiko dan menyusun rekomendasi strategi mitigasi risiko.

#### A. Analisis Data

Data yang terkumpul dianalisis dengan menggunakan metode *Failure Mode and Effect Analysis* (FMEA), yang melibatkan langkah-langkah sebagai berikut :

1) *Identifikasi Risiko*, Mengidentifikasi potensi risiko yang dapat terjadi selama implementasi ERP, dengan fokus pada risiko teknis, operasional, dan manajerial.

2) *Penilaian Risiko*, Menilai setiap risiko berdasarkan tiga kriteria utama: tingkat keparahan (*severity*), frekuensi kejadian (*occurrence*), dan kemampuan deteksi (*detection*). Setiap kriteria diberi skor dari 1 hingga 10.

3) *Prioritas Risiko*, Menghitung *Risk Priority Number* (RPN) dengan mengalikan skor dari tiga kriteria.  $RPN = Severity(S) \times Occurrence(O) \times Detection(D)$ . Risiko dengan RPN tertinggi diberi prioritas untuk mitigasi.

4) *Mitigasi Risiko*, Mengembangkan dan merekomendasikan langkah-langkah mitigasi untuk mengurangi atau mengelola risiko yang teridentifikasi. Strategi mitigasi disesuaikan dengan panduan dari standar ISO 31000:2018.

#### B. Validasi Data

Untuk memastikan validitas data, teknik triangulasi digunakan dengan menggabungkan hasil wawancara, analisis dokumen, dan observasi. Diskusi dan konfirmasi dengan informan kunci juga dilakukan untuk memastikan keakuratan dan relevansi temuan[6].

#### C. Penyajian Data

Data yang telah dianalisis akan disajikan dalam bentuk naratif deskriptif yang menggambarkan temuan penelitian secara komprehensif, dilengkapi dengan tabel dan grafik untuk mendukung penjelasan.

### III. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan menganalisis manajemen risiko dalam penerapan sistem ERP di PT XYZ dengan metode FMEA dan proses manajemen risiko sesuai ISO 31000:2018. Hasilnya mencakup identifikasi aset kritis, risiko, penyebab, dampak, pencegahan saat ini, analisis risiko, dan rekomendasi mitigasi.

#### A. Identifikasi Aset Krtis PT XYZ

Identifikasi aset ini dilakukan dengan pendekatan yang sistematis dan terstruktur, melibatkan berbagai departemen dan unit kerja yang terkait. Hasilnya menunjukkan bahwa proses bisnis telah diidentifikasi sebagai aset secara umum dapat dilihat pada Tabel II.

TABEL I  
IDENTIFIKASI ASET KRITIS PT XYZ

| No | Kategori Aset | Aset Kritis                                                                              | Deskripsi                                                                                                                         |
|----|---------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1. | Informasi     | Data pembelian                                                                           | Data ini digunakan oleh direktur untuk melakukan proses validasi data pada setiap user atau staff bagian.                         |
|    |               | Data penjualan                                                                           |                                                                                                                                   |
|    |               | Data pengembalian                                                                        |                                                                                                                                   |
|    |               | Data penggantian                                                                         |                                                                                                                                   |
|    |               | Data keuangan                                                                            |                                                                                                                                   |
|    |               | Data daily report                                                                        |                                                                                                                                   |
|    |               | Data stok                                                                                |                                                                                                                                   |
| 2. | Hardware      | Komputer/Laptop                                                                          | digunakan untuk membantu setiap staff dalam melakukan proses bisnis seperti memasukkan data, mengirimkan data, dan mengolah data. |
|    |               | Hardware pendukung :<br>- Printer<br>- Scanner                                           |                                                                                                                                   |
| 3. | Jaringan      | Jaringan internet (wifi)                                                                 | Digunakan untuk mendukung jaringan yang digunakan dalam sistem agar dapat melakukan komunikasi dan proses bisnis.                 |
|    |               | EERP (Edison ERP)                                                                        |                                                                                                                                   |
| 4. | Software      | Sistem Operasi Windows                                                                   | Digunakan sebagai software untuk mendukung sistem ini di bagian sistem operasi                                                    |
|    |               | Direktur<br>Sekretaris<br>Finance<br>Pembelian<br>Admin<br>HRD-GA<br>Marketing<br>Gudang |                                                                                                                                   |

### B. Identifikasi Risiko

Pengelolaan risiko dalam penerapan sistem ERP di PT XYZ penting. Tabel berikut menunjukkan risiko yang teridentifikasi selama implementasi, membantu PT XYZ memahami tantangan dan mengambil langkah-langkah tepat. Risiko terhadap aset kritis PT XYZ juga tercantum, berdasarkan wawancara pengguna, penelitian sebelumnya, dan analisis mendalam.

TABEL III  
IDENTIFIKASI RISIKO

| Kategori Aset Kritis | Aset Kritis    | Risiko          | Kode Risiko |
|----------------------|----------------|-----------------|-------------|
|                      | Data pembelian | Kehilangan data | R-01        |

| Kategori Aset Kritis | Aset Kritis                                                                                                   | Risiko                                  | Kode Risiko |
|----------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------|
| Informasi            | Data penjualan<br>Data pengembalian<br>Data penggantian<br>Data keuangan<br>Data daily report<br>Data stok.   | Kebocoran data                          | R-02        |
|                      |                                                                                                               | Human error                             | R-03        |
| Hardware             | Komputer/Laptop                                                                                               | Kerusakan komputer/laptop               | R-04        |
|                      |                                                                                                               | Kehilangan/pencurian                    | R-05        |
|                      |                                                                                                               | Backup data gagal                       | R-06        |
|                      |                                                                                                               | Virus                                   | R-07        |
|                      |                                                                                                               | Kegagalan perangkat keras               | R-08        |
|                      |                                                                                                               | Human error                             | R-09        |
|                      |                                                                                                               | Bencana alam, seperti banjir dan gempa) | R-10        |
|                      |                                                                                                               | kebakaran                               | R-11        |
|                      |                                                                                                               | Kehilangan fungsi                       | R-12        |
|                      |                                                                                                               | Kerusakan printer/scanner               | R-13        |
| Jaringan             | Jaringan internet (wifi)                                                                                      | Human error                             | R-14        |
|                      |                                                                                                               | Akses tidak sah                         | R-15        |
| Software             | EERP (Edison ERP)                                                                                             | Penyusupan jaringan                     | R-16        |
|                      |                                                                                                               | Jaringan down                           | R-17        |
|                      |                                                                                                               | Human error                             | R-18        |
|                      |                                                                                                               | Sistem error                            | R-19        |
|                      |                                                                                                               | Ketergantungan pihak ketiga             | R-20        |
|                      |                                                                                                               | Ketidaksesuaian dengan kebutuhan bisnis | R-21        |
|                      |                                                                                                               | Kegagalan Integrasi modul               | R-22        |
|                      |                                                                                                               | Kegagalan sistem operasi                | R-23        |
|                      |                                                                                                               | Kegagalan update                        | R-24        |
|                      |                                                                                                               | Turnover karyawan tinggi                | R-25        |
| People               | Direktur<br>Sekretaris<br>Finance<br>Pembelian<br>Regulatory affair<br>Admin<br>HRD-GA<br>Marketing<br>Gudang | Kurangnya pelatihan                     | R-26        |
|                      |                                                                                                               | Pelanggaran terhadap peraturan          | R-27        |

### C. Identifikasi Penyebab Risiko

Berikut adalah penyebab risiko dalam implementasi sistem ERP, didasarkan pada wawancara pengguna, penelitian sebelumnya, dan analisis mendalam penulis, yang tercantum dalam Tabel III.

TABEL IIIII  
IDENTIFIKASI PENYEBAB RISIKO

| Aset Kritis                                                   | Risiko          | Penyebab Risiko                            | Code penyebab risiko |
|---------------------------------------------------------------|-----------------|--------------------------------------------|----------------------|
| Data pembelian<br>Data penjualan<br>Data pengembalian<br>Data | Kehilangan data | Bencana alam, seperti banjir dan kebakaran | R-01.1               |
|                                                               |                 | Kerusakan perangkat keras/lunak            | R-01.2               |
|                                                               |                 | Kegagalan backup                           | R-01.3               |

| Aset Kritis                                                  | Risiko                                  | Penyebab Risiko                                                                    | Code penyebab risiko |
|--------------------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------|----------------------|
| penggantian Data keuangan<br>Data daily report<br>Data stok. | Kebocoran data                          | Staf yang memberikan hak aksesnya kepada orang lain                                | R-02.1               |
|                                                              |                                         | User yang tidak berkepentingan berhasil login dan melakukan perubahan data         | R-02.2               |
|                                                              |                                         | karyawan yang tidak puas atau mantan karyawan yang memiliki akses ke data sensitif | R-02.3               |
|                                                              | Human error                             | Salah input                                                                        | R-03.1               |
|                                                              |                                         | Lupa password                                                                      | R-03.2               |
|                                                              |                                         | Password masing-masing staff jarang diganti                                        | R-03.3               |
| Komputer/<br>Laptop                                          | Kerusakan komputer/<br>laptop           | Terkena cairan                                                                     | R-04.1               |
|                                                              |                                         | Usia perangkat                                                                     | R-04.2               |
|                                                              | Kehilangan /<br>pencurian               | Korupsi internal                                                                   | R-05.1               |
|                                                              |                                         | Kurangnya inventarisasi                                                            | R-05.2               |
|                                                              | Backup data gagal                       | Disk error/Disk full                                                               | R-06.1               |
|                                                              | Virus                                   | Penggunaan perangkat lunak yang diperoleh dari sumber yang tidak resmi             | R-07.1               |
|                                                              |                                         | Pemakaian USB atau perangkat eksternal yang tidak aman                             | R-07.2               |
|                                                              |                                         | Tidak terinstall anti virus                                                        | R-07.3               |
|                                                              | Kegagalan perangkat keras               | Penggunaan lisensi perangkat lunak telah melewati jangka waktu yang ditentukan.    | R-08.1               |
|                                                              | Human error                             | Pemakaian tidak sesuai prosedur                                                    | R-09.1               |
|                                                              |                                         | Klik tautan berbahaya                                                              | R-09.2               |
|                                                              | Bencana alam, seperti banjir dan gempa) | Perubahan iklim, factor alam                                                       | R-10.1               |
|                                                              |                                         | kebakaran                                                                          | R-11.1               |
| Hardware pendukung :<br>Printer<br>Scanner                   | Kehilangan fungsi                       | Maintenance tidak teratur                                                          | R-12.1               |
|                                                              |                                         | Penggunaan berlebihan                                                              | R-12.2               |
|                                                              | Kerusakan printer/scanner               | Maintenance tidak teratur                                                          | R-13.1               |
|                                                              |                                         | Penggunaan berlebihan                                                              | R-13.2               |
|                                                              | Human error                             | Pemakaian tidak sesuai prosedur                                                    | R-14.1               |
|                                                              |                                         | Kesalahan dalam mengoperasikan atau memasang bahan cetak                           | R-14.2               |
| Jaringan internet (wifi)                                     | Akses tidak sah                         | Jaringan tidak dilindungi dengan baik                                              | R-15.1               |
|                                                              | Penyusupan jaringan                     | Adanya peretas yang dapat mengakses sistem melalui kerentanan dalam                | R-16.1               |

| Aset Kritis                                                                                                   | Risiko                                | Penyebab Risiko                                             | Code penyebab risiko |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------|-------------------------------------------------------------|----------------------|
| Sistem EERP (Edison ERP)                                                                                      | Jaringan down                         | penggunaan internet                                         |                      |
|                                                                                                               |                                       | Banyak pengguna terhubung ke jaringan wifi                  | R-17.1               |
|                                                                                                               | Human error                           | Kurang pelatihan pengguna                                   | R-18.1               |
|                                                                                                               |                                       | Input data yang tidak akurat                                | R-18.2               |
|                                                                                                               | Sistem Error                          | Tidak melakukan perpanjangan lisensi                        | R-19.1               |
|                                                                                                               |                                       | Software masih terdapat celah keamanan                      | R-19.2               |
|                                                                                                               | Ketergantungan pihak ketiga           | Bergantung pada pihak ketiga untuk hosting dan pengembangan | R-20.1               |
|                                                                                                               | Ketidaksuaian dengan kebutuhan bisnis | Keterbatasan fitur tertentu                                 | R-21.1               |
|                                                                                                               | Kegagalan Integrasi sistem            | Data tidak sinkron antara departemen                        | R-22.1               |
|                                                                                                               |                                       |                                                             |                      |
| Sistem Operasi Windows                                                                                        | Kegagalan sistem operasi              | Kesalahan melakukan prosedur penggunaan sistem              | R-23.1               |
|                                                                                                               | Kegagalan update                      | Jaringan down                                               | R-23.2               |
| Direktur<br>Sekretaris<br>Finance<br>Pembelian<br>Regulatory affair<br>Admin<br>HRD-GA<br>Marketing<br>Gudang | Turnover karyawan tinggi              | Karyawan tidak kompeten                                     | R-25.1               |
|                                                                                                               |                                       | Ketidakpuasan karyawan                                      | R-25.2               |
|                                                                                                               | Human error                           | Karyawan/User tidak paham sistem                            | R-26.1               |
|                                                                                                               | Pelanggaran terhadap peraturan        | Kurangnya sosialisasi peraturan terhadap karyawan           | R-27.1               |
|                                                                                                               |                                       |                                                             |                      |

#### D. Identifikasi Dampak Risiko

Berikut adalah identifikasi dampak risiko yang muncul, didasarkan pada wawancara pengguna, penelitian sebelumnya, dan analisis mendalam penulis, yang tercantum dalam Tabel IV.

TABEL IVV  
IDENTIFIKASI DAMPAK RISIKO

| Risiko          | Code penyebab risiko | Penyebab Risiko                            | Dampak dari Risiko                                                |
|-----------------|----------------------|--------------------------------------------|-------------------------------------------------------------------|
| Kehilangan data | R-01.1               | Bencana alam, seperti banjir dan kebakaran | Aset – asset IT rusak, Proses bisnis terhenti, Kerugian financial |
|                 | R-01.2               | Kerusakan perangkat keras/lunak            | Kehilangan data, Proses bisnis terganggu, Kerugian financial      |
|                 | R-01.3               | Kegagalan backup                           | Kehilangan rekam jejak, gagal menyimpan data, Proses bisnis       |

| Risiko                    | Code penyebab risiko | Penyebab Risiko                                                                    | Dampak dari Risiko                                                                |
|---------------------------|----------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|                           |                      |                                                                                    | terganggu                                                                         |
| Kebocoran data            | R-02.1               | Staf yang memberikan hak aksesnya kepada orang lain                                | Penyebaran informasi perusahaan                                                   |
|                           | R-02.2               | User yang tidak berkepentingan berhasil login dan melakukan perubahan data         | Manipulasi data, penyebaran informasi perusahaan,                                 |
|                           | R-02.3               | karyawan yang tidak puas atau mantan karyawan yang memiliki akses ke data sensitif | kebocoran informasi perusahaan                                                    |
| Human error               | R-03.1               | Salah input                                                                        | Proses bisnis terganggu, pekerjaan terhambat                                      |
|                           | R-03.2               | Lupa password                                                                      | Proses bisnis terganggu, pekerjaan terhambat                                      |
|                           | R-03.3               | Password masing-masing staff jarang diganti                                        | Proses bisnis terganggu, pekerjaan terhambat                                      |
| Kerusakan komputer/laptop | R-04.1               | Terkena cairan                                                                     | Aset – aset IT rusak, Kehilangan data, Proses bisnis terhenti, Kerugian finansial |
|                           | R-04.2               | Usia perangkat                                                                     | Kegiatan operasional terganggu                                                    |
| Kehilangan /pencurian     | R-05.1               | Korupsi internal                                                                   | Kerugian finansial                                                                |
|                           | R-05.2               | Kurangnya inventarisasi                                                            | Kegiatan operasional terganggu                                                    |
| Backup data gagal         | R-06.1               | Disk error/Disk full                                                               | Gagal menyimpan data. Kehilangan data, Proses bisnis terganggu                    |
| Virus                     | R-07.1               | Penggunaan perangkat lunak yang diperoleh dari sumber yang tidak resmi             | Kegiatan operasional terganggu                                                    |
|                           | R-07.2               | Pemakaian USB atau perangkat eksternal yang tidak aman                             | Gangguan fungsionalitas                                                           |
|                           | R-07.3               | Tidak terinstall anti virus                                                        | Kehilangan produktivitas, corrupt, Proses bisnis terganggu                        |
| Kegagalan perangkat keras | R-08.1               | Penggunaan lisensi perangkat lunak telah melewati jangka waktu yang ditentukan.    | Kerugian finansial                                                                |
| Human error               | R-09.1               | Pemakaian tidak sesuai prosedur                                                    | Kegiatan operasional terganggu                                                    |
|                           | R-09.2               | Klik tautan berbahaya                                                              | Gangguan produktivitas                                                            |

| Risiko                                  | Code penyebab risiko | Penyebab Risiko                                                                         | Dampak dari Risiko                                                                 |
|-----------------------------------------|----------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|                                         |                      |                                                                                         | pengguna, terserang malware/virus                                                  |
| Bencana alam, seperti banjir dan gempa) | R-10.1               | Perubahan iklim, factor alam                                                            | Aset – aset IT rusak, Proses bisnis terhenti, Kerugian finansial                   |
| kebakaran                               | R-11.1               | Hubungan arus pendek                                                                    | Kehilangan aset – aset dan mengganggu proses bisnis                                |
| Kehilangan fungsi                       | R-12.1               | Maintenance tidak teratur                                                               | Proses bisnis terganggu, pekerjaan terhambat                                       |
|                                         | R-12.2               | Penggunaan berlebihan                                                                   | Gangguan fungsionalitas                                                            |
| Kerusakan printer/scan ner              | R-13.1               | Maintenance tidak teratur                                                               | Kerugian finansial, Proses bisnis terganggu, pekerjaan terhambat                   |
|                                         | R-13.2               | Penggunaan berlebihan                                                                   | Gangguan fungsionalitas                                                            |
| Human error                             | R-14.1               | Pemakaian tidak sesuai prosedur                                                         | Alat Error, kegiatan operasional terganggu                                         |
|                                         | R-14.2               | Kesalahan dalam mengoperasikan atau memasang bahan cetak                                | Kerusakan perangkat                                                                |
| Akses tidak sah                         | R-15.1               | Jaringan tidak dilindungi dengan baik                                                   | Gangguan fungsionalitas                                                            |
| Penyusupan jaringan                     | R-16.1               | Adanya peretas yang dapat mengakses sistem melalui kerentanan dalam penggunaan internet | Gangguan operasional                                                               |
| Jaringan down                           | R-17.1               | Banyak pengguna terhubung ke jaringan wifi                                              | Gangguan kinerja jaringan                                                          |
| Human error                             | R-18.1               | Kurang pelatihan pengguna                                                               | Gangguan operasional, Pekerjaan terhambat                                          |
|                                         | R-18.2               | Input data yang tidak akurat                                                            | Gangguan operasional                                                               |
| Sistem Error                            | R-19.1               | Tidak melakukan perpanjangan lisensi                                                    | Kerugian finansial                                                                 |
|                                         | R-19.2               | Software masih terdapat celah keamanan                                                  | Terserang malware, data di curi                                                    |
| Ketergantungan pihak ketiga             | R-20.1               | Bergantung pada pihak ketiga untuk hosting dan pengembangan                             | Kerugian finansial                                                                 |
| Ketidaksuaian dengan kebutuhan bisnis   | R-21.1               | Keterbatasan fitur tertentu                                                             | Perusahaan harus mencari solusi tambahan, menambah sistem lain, Kerugian finansial |

| Risiko                         | Code penyebab risiko | Penyebab Risiko                                   | Dampak dari Risiko                  |
|--------------------------------|----------------------|---------------------------------------------------|-------------------------------------|
| Kegagalan Integrasi sistem     | R-22.1               | Data tidak sinkron antara departemen              | Kesalahan atau ketidaksesuaian data |
| Kegagalan sistem operasi       | R-23.1               | Kesalahan melakukan prosedur penggunaan sistem    | Kegiatan operasional terganggu      |
| Kegagalan update               | R-23.2               | Jaringan down                                     | Kegiatan operasional terganggu      |
| Turnover karyawan tinggi       | R-25.1               | Karyawan tidak kompeten                           | Pekerjaan tidak optimal             |
|                                | R-25.2               | Ketidakpuasan karyawan                            | Gangguan operasional                |
| Human error                    | R-26.1               | Karyawan/User tidak paham sistem                  | Pekerjaan terhambat, sistem error   |
| Pelanggaran terhadap peraturan | R-27.1               | Kurangnya sosialisasi peraturan terhadap karyawan | Kerja tidak optimal                 |

#### E. Identifikasi Pencegahan Saat Ini

Berikut adalah upaya pencegahan risiko yang dilakukan perusahaan, berdasarkan wawancara pengguna, penelitian sebelumnya, dan analisis mendalam penulis.

TABEL V  
IDENTIFIKASI PENCEGAHAN SAAT INI

| Risiko          | Code penyebab risiko | Penyebab Risiko                                                                    | Identifikasi Pencegahan Saat ini                                |
|-----------------|----------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Kehilangan data | R-01.1               | Bencana alam, seperti banjir dan kebakaran                                         | Menyiapkan peralatan pemadam kebakaran (APAR).                  |
|                 | R-01.2               | Kerusakan perangkat keras/lunak                                                    | Melakukan pemeliharaan rutin terhadap perangkat keras dan lunak |
|                 | R-01.3               | Kegagalan backup                                                                   | Melakukan pemantauan jaringan secara teratur.                   |
| Kebocoran data  | R-02.1               | Staf yang memberikan hak aksesnya kepada orang lain                                | Memberlakukan sanksi terhadap pelanggaran hak akses.            |
|                 | R-02.2               | User yang tidak berkepentingan berhasil login dan melakukan perubahan data         | Memberlakukan sanksi terhadap pelanggaran hak akses.            |
|                 | R-02.3               | Karyawan yang tidak puas atau mantan karyawan yang memiliki akses ke data sensitif | Memantau aktivitas pengguna secara teratur                      |
| Human error     | R-03.1               | Salah input                                                                        | Mengurangi penggunaan input manual dalam sistem.                |
|                 | R-03.2               | Lupa password                                                                      | Tidak mengganti                                                 |

| Risiko                                 | Code penyebab risiko | Penyebab Risiko                                                                 | Identifikasi Pencegahan Saat ini                                                                   |
|----------------------------------------|----------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
|                                        | R-03.3               | Password masing-masing staff jarang diganti                                     | Mengingatkan pengguna untuk memperbarui kata sandi secara teratur.                                 |
| Kerusakan komputer/ laptop             | R-04.1               | Terkena cairan                                                                  | Diberikan kebijakan perusahaan tentang larangan mengkonsumsi minuman di dekat perangkat elektronik |
|                                        | R-04.2               | Usia perangkat                                                                  | Pengadaan penggantian hardware                                                                     |
| Kehilangan / pencurian                 | R-05.1               | Korupsi internal                                                                | Melakukan audit rutin untuk memverifikasi keberadaan dan kondisi perangkat                         |
|                                        | R-05.2               | Kurangnya inventarisasi                                                         | Melakukan pengecekan dan pembaruan inventaris secara berkala                                       |
| Backup data gagal                      | R-06.1               | Disk error/Disk full                                                            | Memantau ruang penyimpanan yang tersedia secara berkala                                            |
| Virus                                  | R-07.1               | Penggunaan perangkat lunak yang diperoleh dari sumber yang tidak resmi          | Melakukan pengecekan terhadap hardware                                                             |
|                                        | R-07.2               | Pemakaian USB atau perangkat eksternal yang tidak aman                          | Melakukan pengecekan terhadap hardware                                                             |
|                                        | R-07.3               | Tidak terinstall anti virus                                                     | Install dan update anti virus secara berkala                                                       |
| Kegagalan perangkat keras              | R-08.1               | Penggunaan lisensi perangkat lunak telah melewati jangka waktu yang ditentukan. | Melakukan pengecekan terhadap hardware                                                             |
| Human error                            | R-09.1               | Pemakaian tidak sesuai prosedur                                                 | Memberikan pengenalan terhadap hardware yang digunakan.                                            |
|                                        | R-09.2               | Klik tautan berbahaya                                                           | Menggunakan perangkat lunak keamanan yang dapat mendeteksi                                         |
| Bencana alam, seperti banjir dan gempa | R-10.1               | Perubahan iklim, factor alam                                                    | Menempatkan infrastruktur dan fasilitas penting di lokasi yang aman                                |
| kebakaran                              | R-11.1               | Hubungan arus pendek                                                            | Menyiapkan peralatan pemadam kebakaran (APAR).                                                     |
| Kehilangan fungsi                      | R-12.1               | Maintenance tidak teratur                                                       | Menjadwalkan perawatan rutin.                                                                      |
|                                        | R-12.2               | Penggunaan                                                                      | Seluruh hardware                                                                                   |

| Risiko                    | Code penyebab risiko | Penyebab Risiko                                                                         | Identifikasi Pencegahan Saat ini                        |
|---------------------------|----------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------|
|                           |                      | berlebihan                                                                              | dioperasikan saat jam kerja                             |
| Kerusakan printer/scanner | R-13.1               | Maintenance tidak teratur                                                               | Menjadwalkan perawatan rutin.                           |
|                           | R-13.2               | Penggunaan berlebihan                                                                   | Diberikan jadwal penggunaan                             |
| Human error               | R-14.1               | Pemakaian tidak sesuai prosedur                                                         | Memberikan pengenalan terhadap hardware yang digunakan. |
|                           | R-14.2               | Kesalahan dalam mengoperasikan atau memasang bahan cetak                                | Memiliki prosedur standar yang jelas dan terdokumentasi |
| Akses tidak sah           | R-15.1               | Jaringan tidak dilindungi dengan baik                                                   | Melakukan pemindaian keamanan secara teratur            |
| Penyusupan jaringan       | R-16.1               | Adanya peretas yang dapat mengakses sistem melalui kerentanan dalam penggunaan internet | Melakukan pemantauan aktivitas jaringan secara aktif    |
| Jaringan down             | R-17.1               | Banyak pengguna terhubung ke jaringan wifi                                              | Menyediakan beberapa jaringan (wifi)                    |
| Human error               | R-18.1               | Kurang pelatihan pengguna                                                               | Memberikan pengenalan terhadap sistem yang digunakan.   |
|                           | R-18.2               | Input data yang tidak akurat                                                            | Mengimplementasikan proses verifikasi dan validasi data |
| Sistem Error              | R-19.1               | Tidak melakukan perpanjangan lisensi                                                    | Melakukan pengecekan terhadap software                  |

| Risiko                                  | Code penyebab risiko | Penyebab Risiko                                             | Identifikasi Pencegahan Saat ini                        |
|-----------------------------------------|----------------------|-------------------------------------------------------------|---------------------------------------------------------|
|                                         | R-19.2               | Software masih terdapat celah keamanan                      | Melakukan audit keamanan secara berkala                 |
| Ketergantungan pihak ketiga             | R-20.1               | Bergantung pada pihak ketiga untuk hosting dan pengembangan | Melakukan pengecekan terhadap software                  |
| Ketidaksesuaian dengan kebutuhan bisnis | R-21.1               | Keterbatasan fitur tertentu                                 | Melakukan evaluasi menyeluruh terhadap kebutuhan bisnis |
| Kegagalan Integrasi sistem              | R-22.1               | Data tidak sinkron antara departemen                        | Melakukan audit data reguler                            |
| Kegagalan sistem operasi                | R-23.1               | Kesalahan melakukan prosedur penggunaan sistem              | Memberikan pengenalan terhadap sistem yang digunakan.   |
| Kegagalan update                        | R-23.2               | Jaringan down                                               | Melakukan pemantauan jaringan secara teratur.           |
| Turnover karyawan tinggi                | R-25.1               | Karyawan tidak kompeten                                     | Diberikan pelatihan di awal bekerja                     |
|                                         | R-25.2               | Ketidakpuasan karyawan                                      | Menyesuaikan kondisi kerja, kompensasi, dan kebijakan   |
| Human error                             | R-26.1               | Karyawan/User tidak paham sistem                            | Memberikan pengenalan terhadap sistem yang digunakan.   |
| Pelanggaran terhadap peraturan          | R-27.1               | Kurangnya sosialisasi peraturan terhadap karyawan           | Mensosialisasikan perubahan peraturan kepada pengguna.  |

## F. Penilaian Risiko

Penilaian risiko ini bertujuan untuk menentukan prioritas risiko menggunakan metode FMEA yang diterapkan dalam penelitian ini. Berdasarkan penilaian yang diberikan oleh responden, diperoleh nilai S (severity), O (occurrence), dan D (detection) untuk setiap kegagalan seperti yang tercantum dalam tabel VII.

TABEL VI  
PENILAIAN RISIKO

| Codep  | Process Function | Potencial Failure Modes | Potential Effect(s) of Failure                                        | S | Potential Cause(s) of Failure                       | O | Current Process Controls                                            | D | RPN |
|--------|------------------|-------------------------|-----------------------------------------------------------------------|---|-----------------------------------------------------|---|---------------------------------------------------------------------|---|-----|
| R-01.1 | Informasi        | Kehilangan data         | Aset – asset IT rusak, Proses bisnis terhenti, Kerugian financial     | 5 | Bencana alam, seperti banjir dan kebakaran          | 2 | Menyiapkan peralatan pemadam kebakaran (APAR).                      | 7 | 70  |
| R-01.2 | Informasi        | Kehilangan data         | Kehilangan data, Proses bisnis terganggu, Kerugian financial          | 5 | Kerusakan perangkat keras/lunak                     | 3 | Melakukan pemeliharaan rutin terhadap perangkat keras dan lunak     | 4 | 60  |
| R-01.3 | Informasi        | Kehilangan data         | Kehilangan rekam jejak, gagal menyimpan data, Proses bisnis terganggu | 2 | Kegagalan backup                                    | 6 | Melakukan pemantauan jaringan secara teratur.                       | 4 | 48  |
| R-02.1 | Informasi        | Kebocoran data          | Penyebaran informasi perusahaan                                       | 6 | Staf yang memberikan hak aksesnya kepada orang lain | 3 | Memantau secara berkala siapa yang memiliki akses ke data sensitif. | 4 | 72  |

| Codep  | Process Function | Potencial Failure Modes    | Potential Effect(s) of Failure                                                     | S | Potential Cause(s) of Failure                                                      | O | Current Process Controls                                                                           | D | RPN |
|--------|------------------|----------------------------|------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------|---|----------------------------------------------------------------------------------------------------|---|-----|
| R-02.2 | Informasi        | Kebocoran data             | Manipulasi data, penyebaran informasi perusahaan,                                  | 6 | User yang tidak berkepentingan berhasil login dan melakukan perubahan data         | 2 | Melakukan audit rutin terhadap aktivitas login                                                     | 4 | 48  |
| R-02.3 | Informasi        | Kebocoran data             | Data disalahgunakan                                                                | 6 | Mantan karyawan atau karyawan yang tidak puas yang memiliki akses ke data sensitif | 2 | Memantau aktivitas pengguna secara teratur                                                         | 4 | 48  |
| R-03.1 | Informasi        | Human error                | Proses bisnis terganggu, pekerjaan terhambat                                       | 3 | Salah input                                                                        | 5 | Mengurangi penggunaan input manual dalam sistem.                                                   | 2 | 30  |
| R-03.2 | Informasi        | Human error                | Proses bisnis terganggu, pekerjaan terhambat                                       | 3 | Lupa password                                                                      | 2 | Tidak mengganti password yang susah                                                                | 3 | 18  |
| R-03.3 | Informasi        | Human error                | Proses bisnis terganggu, pekerjaan terhambat                                       | 4 | Password masing-masing staff jarang diganti                                        | 4 | Mengingatkan pengguna untuk memperbarui kata sandi secara teratur.                                 | 2 | 32  |
| R-04.1 | Hardware         | Kerusakan komputer/laptop  | Aset – asset IT rusak, Kehilangan data, Proses bisnis terhenti, Kerugian financial | 6 | Terkena cairan                                                                     | 1 | Diberikan kebijakan perusahaan tentang larangan mengkonsumsi minuman di dekat perangkat elektronik | 4 | 24  |
| R-04.2 | Hardware         | Kerusakan komputer/ laptop | Kegiatan operasional terganggu                                                     | 5 | Usia perangkat                                                                     | 3 | Pengadaan penggantian hardware                                                                     | 4 | 60  |
| R-05.1 | Hardware         | Kehilangan/pencurian       | Kerugian financial                                                                 | 5 | Korupsi internal                                                                   | 3 | Melakukan audit rutin untuk memverifikasi keberadaan dan kondisi perangkat                         | 4 | 60  |
| R-05.2 | Hardware         | Kehilangan/pencurian       | Kegiatan operasional terganggu                                                     | 5 | Kurangnya inventarisasi                                                            | 3 | Melakukan pengecekan dan pembaruan inventaris secara berkala                                       | 4 | 60  |
| R-06.1 | Hardware         | Backup data gagal          | Gagal menyimpan data. Kehilangan data, Proses bisnis terganggu                     | 5 | Disk error/Disk full                                                               | 2 | Memantau ruang penyimpanan yang tersedia secara berkala                                            | 4 | 40  |
| R-07.1 | Hardware         | Virus                      | Kegiatan operasional terganggu                                                     | 6 | Penggunaan perangkat lunak yang diperoleh dari sumber yang tidak resmi             | 3 | Melakukan pengecekan terhadap hardware                                                             | 4 | 72  |
| R-07.2 | Hardware         | Virus                      | Gangguan fungsionalitas                                                            | 6 | Pemakaian USB atau perangkat eksternal yang tidak aman                             | 4 | Melakukan pengecekan terhadap hardware                                                             | 2 | 48  |
| R-07.3 | Hardware         | Virus                      | Kehilangan produktivitas, corrupt, Proses bisnis terganggu                         | 6 | Tidak terinstall anti virus                                                        | 2 | Install dan update anti virus secara berkala                                                       | 2 | 24  |
| R-08.1 | Hardware         | Kegagalan perangkat keras  | Kerugian finansial                                                                 | 6 | Penggunaan lisensi perangkat lunak telah melewati jangka waktu yang ditentukan.    | 1 | Melakukan pengecekan terhadap hardware                                                             | 2 | 12  |
| R-09.1 | Hardware         | Human error                | Kegiatan operasional terganggu                                                     | 6 | Pemakaian tidak sesuai prosedur                                                    | 1 | Memberikan pengenalan terhadap hardware yang digunakan.                                            | 2 | 12  |
| R-09.2 | Hardware         | Human error                | Gangguan produktivitas pengguna, terserang malware/virus                           | 5 | Klik tautan berbahaya                                                              | 2 | Menggunakan perangkat lunak keamanan yang dapat mendeteksi                                         | 5 | 50  |
| R-10.1 | Hardware         | Bencana alam,              | Aset – asset IT                                                                    | 5 | Perubahan iklim,                                                                   | 2 | Menempatkan                                                                                        | 8 | 80  |

| Codep  | Process Function                      | Potencial Failure Modes                 | Potential Effect(s) of Failure                                                     | S | Potential Cause(s) of Failure                                                           | O | Current Process Controls                                | D | RPN |
|--------|---------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------|---|---------------------------------------------------------|---|-----|
|        |                                       | seperti banjir dan gempa)               | rusak, Proses bisnis terhenti, Kerugian financial                                  |   | factor alam                                                                             |   | infrastruktur dan fasilitas penting di lokasi yang aman |   |     |
| R-11.1 | Hardware                              | kebakaran                               | Kehilangan asset – asset dan mengganggu proses bisnis                              | 8 | Hubungan arus pendek                                                                    | 3 | Menyiapkan peralatan pemadam kebakaran (APAR).          | 4 | 96  |
| R-12.1 | Hardware pendukung : Printer/ scanner | Kehilangan fungsi                       | Proses bisnis terganggu, pekerjaan terhambat                                       | 4 | Maintenance tidak teratur                                                               | 3 | Menjadwalkan perawatan rutin.                           | 2 | 24  |
| R-12.2 | Hardware pendukung : Printer/ scanner | Kehilangan fungsi                       | Gangguan fungsionalitas                                                            | 4 | Penggunaan berlebihan                                                                   | 3 | Seluruh hardware dioperasikan saat jam kerja            | 2 | 24  |
| R-13.1 | Hardware pendukung : Printer/ scanner | Kerusakan printer/scanner               | Kerugian finansial, Proses bisnis terganggu, pekerjaan terhambat                   | 5 | Maintenance tidak teratur                                                               | 3 | Menjadwalkan perawatan rutin.                           | 2 | 30  |
| R-13.2 | Hardware pendukung : Printer/ scanner | Kerusakan printer/scanner               | Gangguan fungsionalitas                                                            | 4 | Penggunaan berlebihan                                                                   | 3 | Diberikan jadwal penggunaan                             | 3 | 36  |
| R-14.1 | Hardware pendukung : Printer/ scanner | Human error                             | Alat Error, kegiatan operasional terganggu                                         | 4 | Pemakaian tidak sesuai prosedur                                                         | 3 | Memberikan pengenalan terhadap hardware yang digunakan. | 3 | 36  |
| R-14.2 | Hardware pendukung : Printer/ scanner | Kerusakan perangkat                     | Proses bisnis terhambat                                                            | 5 | Kesalahan dalam mengoperasikan atau memasang bahan cetak                                | 4 | Memiliki prosedur standar yang jelas dan terdokumentasi | 2 | 40  |
| R-15.1 | Jaringan                              | Akses tidak sah                         | Gangguan fungsionalitas                                                            | 5 | Jaringan tidak dilindungi dengan baik                                                   | 5 | Melakukan pemindaian keamanan secara teratur            | 3 | 75  |
| R-16.1 | Jaringan                              | Penyusupan jaringan                     | Gangguan operasional                                                               | 5 | Adanya peretas yang dapat mengakses sistem melalui kerentanan dalam penggunaan internet | 4 | Melakukan pemantauan aktivitas jaringan secara aktif    | 3 | 60  |
| R-17.1 | Jaringan                              | Jaringan down                           | Gangguan kinerja jaringan                                                          | 5 | Banyak pengguna terhubung ke jaringan wifi                                              | 8 | Menyediakan beberapa jaringan (wifi)                    | 3 | 120 |
| R-18.1 | Software                              | Human error                             | Gangguan operasional, Pekerjaan terhambat                                          | 5 | Kurang pelatihan pengguna                                                               | 3 | Memberikan pengenalan terhadap sistem yang digunakan.   | 2 | 30  |
| R-18.2 | Software                              | Human error                             | Gangguan operasional                                                               | 4 | Input data yang tidak akurat                                                            | 3 | Mengimplementasikan proses verifikasi dan validasi data | 2 | 24  |
| R-19.1 | Software                              | Sistem Error                            | Kerugian finansial                                                                 | 6 | Tidak melakukan perpanjangan lisensi                                                    | 5 | Melakukan pengecekan terhadap software                  | 2 | 60  |
| R-19.2 | Software                              | Sistem Error                            | Terserang malware, data di curi                                                    | 9 | Software masih terdapat celah keamanan                                                  | 4 | Melakukan audit keamanan secara berkala                 | 4 | 144 |
| R-20.1 | Software                              | Ketergantungan pihak ketiga             | Kerugian finansial                                                                 | 8 | Bergantung pada pihak ketiga untuk hosting dan pengembangan                             | 5 | Melakukan pengecekan terhadap software                  | 2 | 80  |
| R-21.1 | Software                              | Ketidaksesuaian dengan kebutuhan bisnis | Perusahaan harus mencari solusi tambahan, menambah sistem lain, Kerugian finansial | 7 | Keterbatasan fitur tertentu                                                             | 1 | Melakukan evaluasi menyeluruh terhadap kebutuhan bisnis | 2 | 14  |
| R-22.1 | Software                              | Kegagalan Integrasi sistem              | Kesalahan atau ketidaksesuaian data                                                | 6 | Data tidak sinkron antara departemen                                                    | 4 | Melakukan audit data reguler                            | 2 | 48  |
| R-23.1 | Software                              | Kegagalan sistem                        | Kegiatan                                                                           | 7 | Kesalahan                                                                               | 4 | Memberikan                                              | 3 | 84  |

| Codep  | Process Function | Potencial Failure Modes        | Potential Effect(s) of Failure    | S | Potential Cause(s) of Failure                     | O | Current Process Controls                               | D | RPN |
|--------|------------------|--------------------------------|-----------------------------------|---|---------------------------------------------------|---|--------------------------------------------------------|---|-----|
|        |                  | operasi                        | operasional terganggu             |   | melakukan prosedur penggunaan sistem              |   | pengenalan terhadap sistem yang digunakan.             |   |     |
| R-23.2 | Software         | Kegagalan update               | Kegiatan operasional terganggu    | 4 | Jaringan down                                     | 5 | Melakukan pemantauan jaringan secara teratur.          | 3 | 60  |
| R-25.1 | People           | Turnover karyawan tinggi       | Pekerjaan tidak optimal           | 5 | Karyawan tidak kompeten                           | 4 | Diberikan pelatihan di awal bekerja                    | 4 | 80  |
| R-25.2 | People           |                                | Gangguan operasional              | 5 | Ketidakpuasan karyawan                            | 3 | Menyesuaikan kondisi kerja, kompensasi, dan kebijakan  | 4 | 60  |
| R-26.1 | People           | Human error                    | Pekerjaan terhambat, sistem error | 5 | Karyawan/User tidak paham sistem                  | 4 | Memberikan pengenalan terhadap sistem yang digunakan.  | 4 | 80  |
| R-27.1 | People           | Pelanggaran terhadap peraturan | Kerja tidak optimal               | 7 | Kurangnya sosialisasi peraturan terhadap karyawan | 4 | Mensosialisasikan perubahan peraturan kepada pengguna. | 3 | 84  |

### G. Penentuan Level Risiko

Setelah melakukan perhitungan RPN, dilakukan memprioritaskan berdasarkan nilai RPN yang telah dihitung. Berikut adalah daftar RPN yang diurutkan dari nilai tertinggi ke terendah.

TABEL VII  
PENENTUAN LEVEL RISIKO

| Code   | Potencial Failure Modes                | Potential Cause(s) of Failure                               | RPN | Level Risiko |
|--------|----------------------------------------|-------------------------------------------------------------|-----|--------------|
| R-19.2 | Sistem Error                           | Software masih terdapat celah keamanan                      | 144 | High         |
| R-17.1 | Jaringan Down                          | Banyak pengguna terhubung ke jaringan wifi                  | 120 | High         |
| R-11.1 | kebakaran                              | Hubungan arus pendek                                        | 96  | Medium       |
| R-21.1 | Kegagalan sistem operasi               | Kesalahan melakukan prosedur penggunaan sistem              | 84  | Medium       |
| R-25.1 | Pelanggaran terhadap peraturan         | Kurangnya sosialisasi peraturan terhadap karyawan           | 84  | Medium       |
| R-10.1 | Bencana alam, seperti banjir dan gempa | Perubahan iklim, factor alam                                | 80  | Medium       |
| R-20.1 | Ketergantungan pihak ketiga            | Bergantung pada pihak ketiga untuk hosting dan pengembangan | 80  | Medium       |
| R-23.1 | Turnover karyawan tinggi               | Karyawan tidak kompeten                                     | 80  | Medium       |
| R-24.1 | Human error                            | Karyawan/User tidak paham sistem                            | 80  | Medium       |

| Code   | Potencial Failure Modes   | Potential Cause(s) of Failure                                                           | RPN | Level Risiko |
|--------|---------------------------|-----------------------------------------------------------------------------------------|-----|--------------|
| R-15.1 | Akses tidak sah           | Jaringan tidak dilindungi dengan baik                                                   | 75  | Low          |
| R-02.1 | Kebocoran data            | Staf yang memberikan hak aksesnya kepada orang lain                                     | 72  | Low          |
| R-07.1 | Virus                     | Penggunaan perangkat lunak yang diperoleh dari sumber yang tidak resmi                  | 72  | Low          |
| R-01.1 | Kehilangan data           | Bencana alam, seperti banjir dan kebakaran                                              | 70  | Low          |
| R-01.2 | Kehilangan data           | Kerusakan perangkat keras/lunak                                                         | 60  | Low          |
| R-04.2 | Kerusakan komputer/laptop | Usia perangkat                                                                          | 60  | Low          |
| R-05.1 | Kehilangan/pencurian      | Korupsi internal                                                                        | 60  | Low          |
| R-05.2 | Kehilangan/pencurian      | Kurangnya inventarisasi                                                                 | 60  | Low          |
| R-16.1 | Penyusupan jaringan       | Adanya peretas yang dapat mengakses sistem melalui kerentanan dalam penggunaan internet | 60  | Low          |

| Code   | Potencial Failure Modes    | Potential Cause(s) of Failure                                                 | RPN | Level Risiko |
|--------|----------------------------|-------------------------------------------------------------------------------|-----|--------------|
| R-19.1 | Sistem Error               | Tidak melakukan perpanjangan lisensi                                          | 60  | Low          |
| R-22.1 | Kegagalan update           | Jaringan down                                                                 | 60  | Low          |
| R-23.2 | Turnover karyawan tinggi   | Ketidakpuasan karyawan                                                        | 60  | Low          |
| R-09.2 | Human error                | Klik tautan berbahaya                                                         | 50  | Low          |
| R-01.3 | Kehilangan data            | Kegagalan backup                                                              | 48  | Low          |
| R-02.2 | Kebocoran data             | User yang tidak berkepentingan berhasil login dan melakukan perubahan data    | 48  | Low          |
| R-02.3 | Kebocoran data             | Mantan karyawan atau karyawan yang tidak puas memiliki akses ke data sensitif | 48  | Low          |
| R-07.2 | Virus                      | Pemakaian USB atau perangkat eksternal yang tidak aman                        | 48  | Low          |
| R-22.1 | Kegagalan Integrasi sistem | Data tidak sinkron antara departemen                                          | 48  | Low          |
| R-06.1 | Backup data gagal          | Disk error/Disk full                                                          | 40  | Low          |
| R-14.2 | Human error                | Kesalahan dalam mengoperasikan atau memasang bahan cetak                      | 40  | Low          |
| R-13.2 | Kerusakan printer/scanner  | Penggunaan berlebihan                                                         | 36  | Low          |
| R-14.1 | Human error                | Pemakaian tidak sesuai prosedur                                               | 36  | Low          |
| R-03.3 | Human error                | Password masing-masing staff jarang diganti                                   | 32  | Low          |
| R-03.1 | Human error                | Salah input                                                                   | 30  | Low          |
| R-13.1 | Kerusakan printer/scanner  | Maintenance tidak teratur                                                     | 30  | Low          |

| Code   | Potencial Failure Modes                 | Potential Cause(s) of Failure | RPN | Level Risiko |
|--------|-----------------------------------------|-------------------------------|-----|--------------|
| R-18.1 | Human error                             | Kurang pelatihan pengguna     | 30  | Low          |
| R-04.1 | Kerusakan komputer/laptop               | Terkena cairan                | 24  | Low          |
| R-07.3 | Virus                                   | Tidak terinstall anti virus   | 24  | Low          |
| R-12.1 | Kehilangan fungsi                       | Maintenance tidak teratur     | 24  | Low          |
| R-12.2 | Kehilangan fungsi                       | Penggunaan berlebihan         | 24  | Low          |
| R-18.2 | Human error                             | Input data yang tidak akurat  | 24  | Low          |
| R-03.2 | Human error                             | Lupa password                 | 18  | Low          |
| R-21.1 | Ketidaksesuaian dengan kebutuhan bisnis | Keterbatasan fitur tertentu   | 14  | Low          |

#### H. Perlakuan Risiko

Rencana mitigasi untuk sembilan risiko yang menjadi fokus PT XYZ adalah sebagai berikut.

TABEL VIII  
PERLAKUAN RISIKO

| Code   | Langkah Mitigasi                                                                                                                                                                                                                                                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R-19.2 | <ul style="list-style-type: none"> <li>- Melakukan pembaruan perangkat lunak secara berkala untuk memperbaiki celah keamanan yang diketahui.</li> <li>- Melakukan pemindaian keamanan rutin untuk mengidentifikasi celah keamanan baru[7].</li> <li>- Menggunakan firewall dan solusi keamanan lainnya untuk melindungi sistem dari serangan.</li> </ul> |
| R-17.1 | <ul style="list-style-type: none"> <li>- Menerapkan kebijakan manajemen kapasitas untuk mengelola jumlah pengguna yang terhubung secara bersamaan.</li> <li>- Diperlukanya pengecekan jaringan secara berkala dan menambahkan router penguat sinyal agar sistem dapat diakses[8].</li> </ul>                                                             |
| R-11.1 | <ul style="list-style-type: none"> <li>- Memasang sistem deteksi asap dan pencegah kebakaran yang memadai[8].</li> <li>- Menjalankan pelatihan keselamatan kebakaran secara berkala kepada staf.</li> </ul>                                                                                                                                              |

| Code   | Langkah Mitigasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>- Melakukan inspeksi dan perawatan rutin terhadap instalasi listrik untuk mencegah kegagalan dan hubungan pendek.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| R-21.1 | <ul style="list-style-type: none"> <li>- Melakukan pemeliharaan rutin pada sistem operasi dan perangkat keras[9].</li> <li>- Memiliki perjanjian dukungan teknis dengan vendor untuk mendapatkan bantuan dalam penyelesaian masalah.</li> <li>- Menyiapkan sistem cadangan yang dapat diaktifkan dengan cepat jika diperlukan.</li> </ul>                                                                                                                                                                                                              |
| R-25.1 | <ul style="list-style-type: none"> <li>- Memiliki kebijakan dan prosedur yang jelas terkait dengan kepatuhan peraturan.</li> <li>- Memberikan pelatihan kepada karyawan tentang kepatuhan peraturan dan konsekuensinya[10].</li> <li>- Melakukan audit kepatuhan secara berkala untuk memastikan bahwa perusahaan mematuhi semua peraturan yang berlaku.</li> </ul>                                                                                                                                                                                    |
| R-10.1 | <ul style="list-style-type: none"> <li>- Evaluasi risiko untuk mengidentifikasi daerah rentan.</li> <li>- Pilih lokasi yang aman dan kuatkan struktur bangunan.</li> <li>- Pasang sistem proteksi terhadap air dan pemantauan peringatan dini.</li> <li>- Siapkan rencana evakuasi dan pemulihan yang terstruktur.</li> <li>- Pertimbangkan asuransi properti dan simpan cadangan data dengan aman.</li> </ul>                                                                                                                                         |
| R-20.1 | <ul style="list-style-type: none"> <li>- Perusahaan perlu melakukan monitoring berkala kepada penyedia jasa hosting. Mengingat pentingnya website EERP, maka perusahaan perlu mempunyai server tersendiri yang lebih handal dan lebih menjaga keamanan data.</li> <li>- Menerapkan kontrak layanan yang jelas dan memperhatikan persyaratan keamanan dalam perjanjian dengan pihak ketiga.</li> <li>- Mencadangkan data secara teratur dan memiliki rencana pemulihan bencana untuk mengantisipasi kemungkinan kegagalan dari pihak ketiga.</li> </ul> |
| R-23.1 | <ul style="list-style-type: none"> <li>- Menerapkan proses rekrutmen yang lebih selektif untuk memastikan karyawan yang direkrut memiliki keterampilan dan kecocokan yang tepat[11].</li> <li>- Menyediakan pelatihan dan pengembangan karir untuk meningkatkan kompetensi karyawan yang ada.</li> </ul>                                                                                                                                                                                                                                               |
| R-24.1 | <ul style="list-style-type: none"> <li>- Menyediakan pelatihan yang memadai kepada karyawan baru untuk memastikan pemahaman yang baik tentang sistem dan prosedur kerja[12].</li> <li>- Memiliki dokumentasi yang jelas dan mudah diakses tentang prosedur dan kebijakan perusahaan.</li> <li>- Menerapkan verifikasi ganda atau pemeriksaan ulang untuk tugas-tugas kritis untuk mengurangi risiko human error.</li> </ul>                                                                                                                            |

#### IV. KESIMPULAN

Berdasarkan analisis manajemen risiko dalam penerapan ERP di PT XYZ dengan metode FMEA, terdapat 44 risiko yang teridentifikasi dengan kategori risiko tinggi 2, risiko sedang 7, dan risiko rendah 35. Risiko utama yang perlu perhatian meliputi sistem *error* akibat celah keamanan (RPN 144), jaringan *down* karena banyaknya pengguna (RPN 120), kebakaran akibat hubungan arus pendek (RPN 96), kegagalan sistem karena kesalahan prosedur (RPN 84), pelanggaran peraturan akibat kurangnya sosialisasi (RPN 84), bencana alam seperti banjir dan gempa (RPN 80), ketergantungan pihak ketiga karena tidak perpanjangan lisensi (RPN 80), turnover karyawan tinggi akibat ketidakkompetenan (RPN 80), dan human error karena ketidakpahaman sistem (RPN 80).

Strategi mitigasi mencakup kombinasi kebijakan, prosedur, pelatihan, dan teknologi, keamanan perangkat lunak dan jaringan; pelatihan karyawan, kepatuhan aturan, teknologi tepat guna, serta perencanaan dan pengelolaan risiko proaktif.

Mengintegrasikan strategi ini dalam praktik bisnis sehari-hari dapat mengurangi kerugian dan meningkatkan keberhasilan jangka panjang, dengan membangun fondasi kuat untuk keberhasilan perusahaan.

#### V. SARAN

Penelitian ini memberikan beberapa rekomendasi untuk meningkatkan keberlanjutan penelitian dan memberikan arahan untuk studi selanjutnya:

- Evaluasi efektivitas penerapan kerangka FMEA dalam manajemen risiko yang disesuaikan dengan kebutuhan PT XYZ.
- Evaluasi manajemen risiko ERP menggunakan kerangka FMEA yang disesuaikan oleh staf dan pemangku kepentingan PT XYZ.

Diharapkan rekomendasi ini dapat berkontribusi pada pengembangan praktik manajemen risiko yang lebih baik di PT XYZ dan memberikan wawasan yang berguna untuk penelitian mendatang di bidang ini..

#### REFERENSI

- [1] C. Goldsberry, "Enterprise resource planning," *Weld. Des. Fabr.*, vol. 82, no. 3, 2009.
- [2] D. Margareth, "Kesuksesan dan kegagalan implementasi enterprise resource planning (ERP) dan contoh studi kasus PT Semen Gresik & Fox Meyer," *Mib-Pib*, vol. E-48, pp. 1–26, 2013, [Online]. Available: <https://d1wqtxts1xzle7.cloudfront.net/36938075/KESUKSESAN-DAN-KEGAGALAN-IMPLEMENTASI-ENTERPRISE-RESOURCE-PLANNING-ERP-PADA-PERUSAHAAN-DAN-CONTOH-STUDI-KASUS-with-cover-page-v2.pdf?Expires=1643298037&Signature=QReGGVWVd4kbmb-8-cOo5XQq~Usl3SeUT~FeuY3XOCJBfC>

- [3] U. Hasdiana, No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title, vol. 11, no. 1. 2018. [Online]. Available: <http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/>
- [4] “KESUKSESAN DAN KEGAGALAN IMPLEMENTASI SISTEM ERP: APAKAH KESALAHAN PERANTI LUNAK? Wahyu Agus Winarno\*,” pp. 36–49, 2007.
- [5] A. Alijoyo, Q. B. Wijaya, and I. Jacob, “Failure Mode Effect Analysis Analisis Modus Kegagalan dan Dampak RISK EVALUATION RISK ANALYSIS: Consequences Probability Level of Risk,” *Crms*, p. 19, 2020, [Online]. Available: [www.lspmks.co.id](http://www.lspmks.co.id)
- [6] S. Haryoko, Bahartiar, and F. Arwadi, *Analisis Data Penelitian Kualitatif (Konsep, Teknik, & Prosedur Analisis)*. 2020.
- [7] P. Hanifah and J. S. Suroso, “Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA,” *J. Komput. Terap.*, vol. 6, no. Vol. 6 No. 2 (2020), pp. 210–221, 2020, doi: 10.35143/jkt.v6i2.3728.
- [8] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000,” *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.
- [9] A. Wicaksono, H. H. Mulyo, and I. E. Riantono, “Analisis Dampak Penerapan Sistem ERP terhadap Kinerja Pengguna,” *Binus Bus. Rev.*, vol. 6, no. 1, p. 25, 2015, doi: 10.21512/bbr.v6i1.985.
- [10] A. P. Aisyah and L. Dahlia, “Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti,” *J. Akunt. dan Manaj.*, vol. 19, no. 02, pp. 78–90, 2022, doi: 10.36406/jam.v19i02.483.
- [11] L. Ferreira and C. Almeida, “Employee Turnover and Organizational Performance: a Study of the Brazilian Retail Sector,” *Brazilian Bus. Rev.*, vol. 12, no. 4, pp. 27–56, 2015, doi: 10.15728/bbr.2015.12.4.2.
- [12] D. N. Safitri, R. F. Sari, Y. S. Dharmawan, S. Informasi, U. Internasional, and S. Indonesia, “Analisis Manajemen Risiko Sistem Enterprise Resource Planning Menggunakan Kerangka Kerja Iso 31000 Pada Pt . Xyz,” *Aisyah J. Informatics Electr. Eng.*, vol. 3, no. 1, pp. 58–67, 2021.