# MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN *FRAMEWORK* ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR

**Diky Yudha Andika[1], Agustinus Fritz Wijaya[2]**
[1,2] Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
*agustinus.wijaya@uksw.edu*

**ABSTRAK**

Peranan teknologi informasi begitu penting bagi kemajuan suatu perusahaan, dengan menggunakan teknologi informasi pasti selalu terdapat kemungkinan risiko baik itu yang sudah ada maupun risiko risiko yang beum teridentifikasi. PT. Trust Lerinvital Timur merupakan salah satu perusahaan transportasi yang menyadari betapa pentingnya pengelolaan risiko dalam suatu perusahaan. Dalam menunjang proses bisnis yang berjalan di perusahaan, perusahaan memiliki aplikasi ERP yang membantu jalanya proses bisnis. Aplikasi ini merupakan aplikasi yang saling terintregasi antar divisi, seperti penggajian, stok kendaraan, , data pemasok, dan lain sebagainya. Namun tidak dapat dipungkiri banyak kemungkinan risiko yang menggangu jalannya aplikasi ERP ini, salah satunya seperti internet service yang sering tiba-tiba mati. Dengan menggunakan framework ISO 31000:2018, diharapkan dapat meminimalisir kemungkinan risiko SI/TI perusahaan, sehingga hasil dari penelitian ini berupa rekomendasi-rekomendasi dari analisis risiko untuk melakukan pengendalian risiko. Sehingga usulan tindakan risiko yang sesuai dapat membantu perusahaan dalam menjaga kualitas perusahaan dari segi SI/TI perusahaan. Selain itu, dihasilkan pula usulan penanganan risiko yang dapat dijadikan acuan oleh PT. Trust Lerinvital Timur untuk meminimalkan kerugian yang diakibatkan oleh risiko tersebut.

**Keyword :** *analisis risiko, ERP, ISO 31000, manajemen risiko*

## 1. PENDAHULUAN

Perkembangan teknologi merupakan hal yang sangat penting dalam dunia bisnis, setiap perusahaan yang bergerak dibidang manapun pasti memerlukan wawasan mengenai teknologi informasi, sehingga banyak perusahaan yang bersaing tidak hanya melulu dari segi bisnis, namun juga bersaing dalam hal teknologi informasi[1]. Cara perusahaan mengembangkan teknologi SI/TI nya dengan mengoptimalkan perkembangan SI/TI perusahaan, sehingga perusahaan tersebut mampu bersaing dengan para kompetitornya. Namun, semakin tinggi teknologi SI/TI perusahaan, maka semakin rentan juga ancaman risiko teknologi informasi pada perusahaan tersebut, sebaik apapun sistem informasi pada suatu perusahaan selalu diikuti dengan kemungkinan risiko yang mampu mengancam sistem tersebut, sehingga sangat diperlukan manajemen risiko yang tepat bagi sebuah perusahaan[2].

Tidak dapat dipungkiri bahwa penggunaan teknologi informasi di perusahaan memiliki berbagai tantangan dan kemungkinan risiko yang terjadi. Risiko merupakan suatu kemungkinan yang dapat menimbulkan bahaya, yang mengakibatkan tidak optimalnya proses bisnis perusahaan. Berdasarkan kemungkinan risiko yang ada, maka perlu adanya manajemen risiko di bidang teknologi informasi guna meminimalisir kemungkinan dan dampak yang akan ditimbulkan.

Manajemen risiko suatu perusahaan menjadikan sebuah aset SI/TI tersebut menjadi lebih berguna serta lebih fungsional bagi perusahaan, meskipun risiko tersebut tidak dapat di eliminasi, namun setidaknya risiko SI/TI mampu diminimalisir, sehingga manfaat dari pengelolaan risiko ini mampu membuat proses bisnis yang berjalan pada perusahaan menjadi lebih efektif dan efesien. Perusahaan yang maju, pasti menyadari bahwa betapa pentingnya pengelolaan risiko yang terkait dengan perencanaan serta penerapan SI/TI perusahaan, sehingga tidak hanya terpaku pada satu sektor tertentu saja, melainkan dari berbagai sektor juga memerlukan risiko SI/TI dengan baik[3].

PT. Trust LerinVital Timur merupakan sebuah perusahaan jasa yang bergerak dibidang jasa transportasi, perusahaan ini terletak di Pondok Mitra Lestari, Jakarta Selatan. PT. Trust Lerinvital Timur ini merupakan perusahaan yang sedang berkembang dalam bidang jasa transportasi bagi perusahaan lain, beberapa kegiatan perusahaan ini antara lain menyiapkan cargo untuk muatan barang pabrik, pengantaran cargo menuju pabrik, setiap pemesanan jasa transportasi lain bagi perusahaan lain dalam kegiatan di bidang produksi. Dalam kegiatan manajemen di PT. Trust Lerinvital Timur memiliki sistem ERP yang digunakan perusahaan dalam mendata transportasi apa saja yang digunakan, perusahaan apa saja yang menggunakan jasa PT. Trust Lerinvital Timur, alamat tujuan cargo, surat jalan kendaraan, stok kendaraan yang tersedia, uang masuk, uang keluar, hingga kepada absensi perusahaan. Namun aplikasi ERP ini banyak ditemukan risiko SI/TI yang mengancam, hingga kemungkinan potensial risiko yang mampu mengganggu bahkan menghambat aktivitas proses bisnis yang berjalan. Sehingga, perlu dilakukan manajemen risiko yang tepat untuk meminimalisir ancaman risiko SI/TI[4].

Manajemen risiko di PT. Trust Lerinvital Timur ini dapat dilakukan dengan menggunakan framework ISO 31000:2018 mengenai *risk management*. Manajemen risiko tersebut dapat dilakukan dengan cara melakukan identifikasi aset dan kemungkinan risiko, analisis risiko, hingga evaluasi risiko[5]. Dimana kegiatan manajemen risiko ini merupakan usaha manajemen untuk mengendalikan risiko kegiatan operasional perusahaan dengan melakukan analisis, evaluasi, hingga rencana mitigasi risiko[6].

Tujuan dari penelitian ini adalah membantu perusahaan dalam hal manajemen risiko, seperti meminimalisir risiko, serta kemungkinan-kemungkinan risiko, dan juga memberikan rekomendasi yang tepat bagi PT. Trust Lerinvital Timur terhadap risiko risiko yang telah diidentifikasi maupun risiko risiko yang sewaktu-waktu dapat muncul membahayakan sistem kerja ERP perusahaan. Analisis risiko ini dilakukan dengan pendekatan menggunakan metode ISO 31000:2018. ISO 31000:2018 merupakan pedoman standar bagi sebuah organisasi maupun perusahaan untuk membangun sebuah pondasi bagi suatu proses menejemen risiko[7]. Pondasi ini meliputi perencanaan, akuntabilitas dari para karyawan, aset serta aktivitas yang digunakan untuk mengelola risiko di PT. Trust Lerinvital Timur dalam pengelolaan risiko. Dalam manajemen risiko ini diperlukan risk assesment yang sudah diatur dalam ISO 31000:2018 agar mampu melihat risk value dari setiap risiko yang sudah teridentifikasi[8].

## 2. TINJAUAN PUSTAKA

Pada penelitian sebelumnya membahas tentang ISO 31000 dilakukan oleh Andi Novia Rilyani yang berjudul "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000" pada tahun 2016. Fokus dari penelitian ini tertuju pada *i-Gracias* (*Integrated Academic Information System*), yaitu sebuah aplikasi yang dapat diakses oleh dosen, mahasiswa, dan staf yang ada di Telkom University. Penelitian tersebut membahas tentang analisis risiko pada aset-aset SI/TI yang terintegrasi dengan sistem *i-Gracias*. Pada penelitian ini menghasilkan bahwa risiko yang memiliki nilai risiko paling tinggi adalah Database crash. Selain itu memiliki 30 risiko yang berada pada kuadran risiko menengah dan terdapat 12 risiko yang berada pada kuadran risiko. Penanganan risiko difokuskan pada aset yang memiliki risiko tinggi dengan mengidentifikasi penyebab dan mencari solusi yang tepat[9].

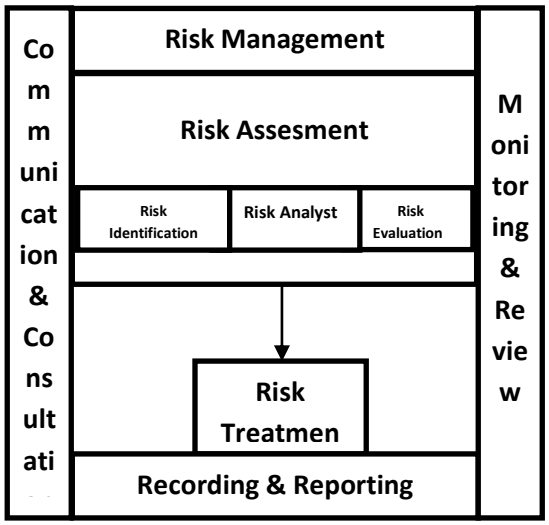
Penelitian berikutnya dengan topik tentang ISO 31000 yang memiliki judul "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada website SWIFTS menggunakan ISO 31000" di tulis oleh Francisca Lady Nice pada tahun 2016. Fokus dari penelitian ini terarah kepada website SWIFTS. Hasil dari penelitian ini adalah tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi, baik itu data perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait pada sistem SWIFTS sehingga memiliki potensi untuk dapat mengganggu jalanya kegiatan proses bisnis LAPAN itu sendiri. Maka dari itu diperlukan peninjauan kembali oleh pihak kepala Divisi IT LAPAN dan penerapan pada perlakuan risiko yang disarankan[10].

Selain itu, penilitian dengan judul "Analisis Risiko Teknologi Informasi pada program HRMS" oleh Stefan Agustinus pada tahun 2017. Pada penelitian tersebut memiliki topik tentang penilaian risiko terhadap aset-aset yang ada di dalam maupun diluar perusahaan yang berhubungan atau terintegrasi dengan program HRMS. Dalam hasil penelitian, ditemukan 2 kemungkinan risiko memiliki tingkatan high kemudian 18 kemungkinan risiko dengan tingkatan medium yang dapat mengganggu kinerja perusahaan. Dengan adanya penilaian risiko, diharapkan mampu meminimalkan kerugian yang dialami perusahaan[8].

## 3. METODE PENELITIAN

Penelitian mengenai manajemen risiko di PT. Trust Lerinvital Timur ini disajikan menggunakan metode *case study research*, dimana metode ini hanya fokus pada satu objek, yaitu aplikasi ERP di PT. Trust Lerinvital Timur, selain itu peneliti juga melakukan pendekatan kualitatif sehingga peneliti dapat terjun langsung di lapangan dalam hal melakukan observasi lapang untuk mendapatkan data yang bersifat asli dan dapat dipertanggung jawabkan[11].

Metode penelitian yang digunakan pada kasus manajemen risiko pada sistem ERP di PT. Trust Lerinvital Timur ini menggunakan kerangka kerja ISO 31000:2018, dimana prinsip dan pedoman dari ISO 31000 sangat cocok digunakan dan telah diakui secara internasional. Mulai dari proses identifikasi risiko, analisis risiko, hingga evaluasi risiko dapat menghasilkan rekomendasi pengelolaan risiko yang tepat bagi perusahaan[12]. Berikut ini tahap manajemen risiko yang digunakan tergambar pada gambar 1.




Gambar 1. Metode Penelitian

Pada tahap pertama dilakukan penilaian risiko yang sistematis guna menghasilkan hasil yang menentukan apakah aplikasi ERP ini memiliki risiko yang dapat diterima atau tidak[13]. Terdapat beberapa tahapan dalam melakukan penilaian risiko ini. Tahapan tahapan tersebut sebagai berikut.

1. *Risk Identification* (Identifikasi Risiko)
   Pada tahap ini dilakukan dengan mengumpulkan informasi yang berguna untuk mengetahui risiko apa saja yang memiliki kemungkinan muncul dalam kegiatan operasional perusahaan[14].
2. *Risk Analyst* (Analisis Risiko)
   Tahap selanjutnya dilakukan analisis risiko dengan melakukan pendataan serta analisis yang berupa faktor-faktor yang mempengaruhi penilaian, karakterisasi, serta manajemen risiko yang berguna dengan insfrastruktur SI/TI perusahaan[15].
3. *Risk Evaluation* (Evaluasi Risiko)
   Tahap terakhir melakukan evaluasi risiko, dengan cara membandingkan risiko mana saja yang memiliki antara level risiko yang terendah hingga risiko yang paling membahayakan atau paling tinggi, sehingga mampu dilakukan analisis berupa pengelompokkan risiko berdasarkan dengan level risiko yang sesuai. Tujuan dari evaluasi risiko ini adalah untuk mendapatkan proses pengambilan risiko berdasarkan hasil analisis risiko[16].

Hingga pada tahap terakhir yaitu *Risk Treatment* (Perlakuan Risiko) dapat ditemukan pemilihan satu atau lebih pilihan dalam hal menanggulangi risiko dan menerapkan penanganan risiko yang mampu meminimalisir risiko[5].

Pada tahap pengambilan data-data perusahaan yang diperlukan dalam melakukan penelitian manajemen risiko di PT. Trust Lerinvital Timur dilakukan dengan cara melakukan wawancara dengan salah satu manajer di perusahaan, wawancara ini bertujuan untuk mengetahui masalah-masalah serta kendala apa saja yang terjadi mengenai aplikasi ERP. Sehingga dapat dilakukan penelitian lebih lanjut mengenai manajemen risiko pada sistem aplikasi ERP, selain itu juga dilakukan metode observasi agar mengetahui secara langsung bagaimana proses bisnis yang diterapkan dalam sistem ERP[17].

## 4. HASIL DAN PEMBAHASAN

### 4.1. Identifikasi Risiko

#### a. Penilaian Risiko

- **Identifikasi Aset**

Tahap ini dilakukan identifikasi mengenai aset aplikasi atau sistem ERP yang meliput set data, aset software, hingga aset hardware perusahaan.

Tabel 1. Identifikasi Aset Pada Aplikasi ERP

| Komponen SI/TI | Aset |
|---|---|
| **Data** | 1. Data Kendaraan<br>2. Data Perusahaan<br>3. Data Absensi<br>4. Data Pemasok<br>5. Data Customer<br>6. Data Pengiriman |
| **Software** | Aplikasi ERP |
| **Hardware** | Device (PC) |

Tabel 1 menunjukkan aset SI/TI yang berupa hardware, software, serta data yang digunakan dalam penggunaan aplikasi ERP

- **Identifikasi Kemungkinan Risiko**

Setelah melakukan identifikasi aset pada aplikasi ERP di perusahaan PT. Trust Lerivital Timur, langkah berikutnya, dilakukan identifikasi kemungkinan risiko, dilakukan dengan cara mengelompokkan berdasarkan faktor-faktor yang muncul seperti pada faktor alam atau lingkungan, faktor SDM, dan juga faktor sistem dan infrastruktur.

Tabel 2. Identifikasi Kemungkinan Risiko

| Faktor | Id | Kemungkinan Risiko |
|---|---|---|
| **Alam atau Lingkungan** | R01 | Banjir |
| | R02 | Gempa Bumi |
| | R03 | Petir |
| | R04 | Kebakaran |
| | R05 | Listrik Padam |
| **Manusia** | R06 | Human Error |
| | R07 | Data dan Informasi diakses oleh pihak yang tidak berwenang |
| | R08 | Penyalahgunaan hak akses |
| | R09 | Vandalisme |
| | R10 | Cybercrime |
| **Sistem dan Insfrastruktur** | R11 | Server down |
| | R12 | Backup Failure |
| | R13 | Overhead |
| | R14 | Data corrupt |
| | R15 | Overcapacity |
| | R16 | Overload |

| Faktor | Id | Kemungkinan Risiko |
|---|---|---|
| | R17 | Web service mati secara tiba-tiba |
| | R18 | Koneksi jaringan terputus |
| | R19 | Koneksi jaringan tidak stabil |
| | R20 | Sistem Crash |
| | R21 | Gagal update |
| | R22 | Memori penuh |
| | R23 | Kegagalan software |
| | R24 | Kegagalan hardware |
| | R25 | Serangan virus |
| | R26 | Proses maintenance tidak terjadwal |

- **Identifikasi Dampak Risiko**

Tahap berikutnya dilakukan tahap identifikasi risiko, dengan mencari dampak-dampak yang dihasilkan dari kemungkinan risiko yang telah di temukan dari risiko yang telah diidentifikasi sebelumnya.

Tabel 3. Identifikasi Dampak Risiko

| Id | Kemungkinan Risiko | Dampak |
|---|---|---|
| R01 | Banjir | Terjadi kerusakan infrastruktur dan menghambat aktivitas bisnis Perusahaan |
| R02 | Gempa Bumi | Terjadi kerusakan insfrastruktur dan proses bisnis Perusahaan terhenti |
| R03 | Petir | Mengalami kerusakan infrastrutur pada perusahaan dan mengalami kerugian secara finansial. |
| R04 | Kebakaran | Terjadi kerusakan infrastruktur perusahaan, proses bisnis terhenti, instansi mengalami kerugian secara finansial. |
| R05 | Listrik Padam | Seluruh akifitas pada perusahaan terhenti |
| R06 | Human Error | Proses layanan pada pengoroman data tidak berjalan secara optimal |
| R07 | Data dan Informasi diakses oleh pihak yang tidak berwenang | Mengakibatkan kebocoran informasi data an memungkinkan manipulasi data |
| R08 | Penyalahgunaan hak akses | Mengakibatkan kebocoran informasi data an memungkinkan manipulasi data |
| R09 | Vandalisme | Dapat mengakibatkan kerusakan pada hardware maupun perangkat lainya |
| R10 | Cybercrime | Adanya manipulasi data serta pencurian data |
| R11 | Server down | Kegagalan dalam melakukan akses ke server |
| R12 | Backup Failure | Meningkatkan risiko kehilangan data |
| R13 | Overhead | Kinerja hardware kurang maksimal, karena rusaknya hardware yang harus menanggung suhu panas yang terus menerus |
| R14 | Data corrupt | Dapat mengalami kehilangan daata |
| R15 | Overcapacity | Kapasitas memori penuh sehingga database tidak dapat menampung data berlebih |
| R16 | Overload | Kehilangan data dan proses loading terhambat karena log database, log temp dan log temp database terisi penuh |
| R17 | Web service mati secara tiba-tiba | Aplikasi ERP tidak bisa dibuka |
| R18 | Koneksi jaringan terputus | Kegagalan dalam melakukan akses ke aplikasi ERP |
| R19 | Koneksi jaringan tidak stabil | Kegiatan yang memerlukan akses internet menjadi sangat lambat |
| R20 | Sistem crash | Kerusakan sistem yang menyebabkan aplikasi ERP tidak dapat diakses dalam jangka waktu sementara |
| R21 | Gagal update | Kegagalan dalam melakukan update aplikasi setelah dilakukan maintenence |
| R22 | Memori penuh | Data tidak bisa tersimpan dalam komputer |
| R23 | Kegagalan software | Software tidak bisa berjalan |
| R24 | Kegagalan hardware | Hardware mengalami kerusakan dan tidak bisa di fungsikan |
| R25 | Serangan virus | Komputer terserang virus malware atau sebagainya sehingga proses bisnis terganggu |
| R26 | Proses maintenance tidak terjadwal | Menyebabkan sering terjadinya error pada aplikasi ERP |

### 4.2. Analisis Risiko

Tahap berikutnya dilakukan proses analisis risiko dengan menentukan nilai kemungkinan risiko yang sudah diidentifikasi, sehingga dapat di kategorikan kedalam tabel kriteria *likelihood* yang berdasarkan frekuensi kejadianya, serta impact atau dampak yang terjadi. Tabel *likelihood* dapat dilihat pada tabel 4.

Tabel 4. Tabel Nilai Pada *Likelihood*

| Likelihood | | Deskripsi | Frekuensi Kejadian |
|---|---|---|---|
| Nilai | Kriteria | | |
| 1 | *Rare* | Risiko sangat jarang terjadi | >2 tahun |
| 2 | *Unlikely* | Risiko jarang terjadi | 1 - 2 tahun |
| 3 | *Possible* | Risiko cukup sering terjadi | 7 - 12 bulan |
| 4 | *Likely* | Risiko sering terjadi | 4 - 6 bulan |
| 5 | *Certain* | Risiko selalu terjadi | 1 - 6 bulan |

Setelah dilakukan tahap ini, maka dapat menentukan bagaimana nilai dari dampak atau impact yang akan terjadi pada objek kasus terhadap kemungkinan risiko, pada kriteria penilaian dampak atau impact ini dibedakan berdasarkan seberapa besar dampak yang akan ditimbulkan untuk mempengaruhi kinerja dari aplikasi ERP. Nilai dari dampak ini dapat dilihat di tabel impact pada Tabel 5.

Tabel 6. Penilaian *Likelihood* dan *Impact*

| ***Impact*** | | **Deskripsi** |
|---|---|---|
| **Nilai** | **Kriteria** | |
| 1 | *Insignificant* | Risiko tidak menganggu aktivitas dan proses bisnis pada instansi |
| 2 | *Minor* | Aktivitas pada instansi sedikit terhambat, namun tidak menganggu aktivitas inti pada instansi |
| 3 | *Moderate* | Risiko tersebut menganggu jalannya proses bisnis pada instansi, sehingga aktivitas bisnis sedikit terhambat |
| 4 | *Major* | Risiko tersebut menghambat hampir seluruh jalannya proses bisnis pada instansi |
| 5 | *Catastrophic* | Risiko mengganggu jalannya proses bisnis yang ada secara menyeluruh dan menghentikan aktivitas instansi secara total |

Dari kriteria *Likelihood* pada tabel 4 dan kriteria impact pada tabel 5. Berikutnya memberikan penilaian pada terhadap kemungkinan risiko berdasarkan tabel 4 dan 5.

Tabel 5. Tabel Nilai Kriteria *Impact*

| ***Id*** | ***Kemungkinan Risiko*** | ***Likelihood*** | ***Impact*** |
|---|---|---|---|
| **R01** | Banjir | **1** | **3** |
| **R02** | Gempa Bumi | **2** | **4** |
| **R03** | Petir | **2** | **3** |
| **R04** | Kebakaran | **1** | **5** |
| **R05** | Listrik Padam | **3** | **3** |
| **R06** | Human Error | **4** | **3** |
| **R07** | Data dan Informasi diakses oleh pihak yang tidak berwenang | **2** | **2** |
| **R08** | Penyalahgunaan hak akses | **2** | **2** |
| **R09** | Vandalisme | **1** | **3** |
| **R10** | Cybercrime | **1** | **3** |
| **R11** | Server down | **4** | **s4** |
| **R12** | Backup Failure | **1** | **2** |
| **R13** | Overheat | **3** | **1** |
| **R14** | Data corrupt | **1** | **4** |
| **R15** | Overcapacity | **2** | **1** |
| **R16** | Overload | **3** | **2** |
| **R17** | Web service mati secara tiba-tiba | **4** | **4** |
| **R18** | Koneksi jaringan terputus | **4** | **4** |
| **R19** | Koneksi jaringan tidak stabil | **3** | **3** |
| **R20** | Sistem crash | **4** | **3** |
| **R21** | Gagal update | **3** | **4** |
| **R22** | Memori penuh | **1** | **2** |
| **R23** | Kegagalan software | **3** | **3** |
| **R24** | Kegagalan hardware | **2** | **3** |
| **R25** | Serangan virus | **1** | **3** |
| **R26** | Proses maintenance tidak terjadwal | **2** | **3** |

Dari tabel 6 di atas, ditemukan nilai-nilai *likelihood* dan *impact* terhadap kemungkinan risiko yang telah teridentifikasi. Hingga kemudian akan ditemukan nilai dari *Likelihood* dan *Impact*, setelah itu dilakukan evaluasi risiko.

### 4.3. Evaluasi Risiko

Tahap terakhir adalah evaluasi risiko, yaitu dilakukan proses evaluasi terhadap segala kemungkinan risiko yang tadinya sudah dilakukan analisis pada tahapan sebelumnya. Hingga kemudian menghasilkan analisis risiko untuk dapat dikategorikan menjadi 3 level risiko yaitu : *Low*, *Medium*, dan *High*.

Tabel 7. *Matrix* Evaluasi Risiko

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| *Likelihood* | Certain | 5 | Medium | Medium | High | High | High |
| | Likely | 4 | Medium | Medium | Medium | High | High |
| | Possible | 3 | Low | Medium | Medium | Medium | High |
| | Unlikely | 2 | Low | Low | Medium | Medium | Medium |
| | Rare | 1 | Low | Low | Low | Medium | Medium |
| | *Impact* | | 1 | 2 | 3 | 4 | 5 |
| | | | Insigficant | Minor | Moderate | Major | Catastrophic |

Rasio pengelompokan berdasarkan level risiko atau *risk level* dimulai dari yang tertinggi hingga terendah, hal tersebut dijelaskan pada tabel 7

Hingga nantinya setiap Id dari kemungkinan risiko akan dimasukkan kedalam matiks evaluasi risiko sesuai dengan kriteria *Likelihood* dan kriteria *Impact*.

Tabel 8. Matrix Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact*

| *Likelihood* | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Certain | 5 | | | | | |
| | Likely | 4 | | | R06 R20 | R11 R17 R18 | |
| | Possible | 3 | R13 | R16 | R05 R19 R23 | R21 | |
| | Unlikely | 2 | R15 | R08 R07 | R03 R24 R26 | R02 | |
| | Rare | 1 | | R09 R12 R22 | R01 R10 R25 | R14 | R04 |
| | Impact | | 1 | 2 | 3 | 4 | 5 |
| | | | Insigficant | Minor | Moderate | Major | Catastrophic |

Pada tabel 8 dihasilkan perhitungan *Likelihood* dan *Impact* terdapat 26 kemungkinan risiko yang dapat dikategorikan dengan rasio.

setelahnya akan dikelompokkan sesuai dengan tingkatan 26 kemungkinan risiko tersebut kedalam tingkatan level *high*, *medium* dan *low.*

Tabel 9. Pengelompokkan Risiko Berdasarkan Tingkatan

| Id | Kemungkinan Risiko | *Likelihood* | *Impact* | *Risk Level* |
|---|---|---|---|---|
| R11 | Server down | 4 | 4 | ***High*** |
| R17 | Web service mati secara tiba-tiba | 4 | 4 | ***High*** |
| R18 | Koneksi jaringan terputus | 4 | 4 | ***High*** |
| R21 | Gagal update | 3 | 4 | ***Medium*** |
| R06 | Human Error | 4 | 3 | ***Medium*** |
| R20 | Sistem crash | 4 | 3 | ***Medium*** |
| R05 | Listrik Padam | 3 | 3 | ***Medium*** |
| R19 | Koneksi jaringan tidak stabil | 3 | 3 | ***Medium*** |
| R23 | Kegagalan software | 3 | 3 | ***Medium*** |
| R02 | Gempa Bumi | 2 | 4 | ***Medium*** |
| R16 | Overload | 3 | 2 | ***Medium*** |
| R03 | Petir | 2 | 3 | ***Medium*** |
| R24 | Kegagalan hardware | 2 | 3 | ***Medium*** |
| R26 | Proses maintenance tidak terjadwal | 2 | 3 | ***Medium*** |
| R04 | Kebakaran | 1 | 5 | ***Medium*** |
| R14 | Data corrupt | 1 | 4 | ***Medium*** |
| R08 | Penyalahgunaan hak akses | 2 | 2 | ***Low*** |
| R07 | Data dan Informasi tidak sesuai | 4 | 4 | ***Low*** |
| R13 | Overheat | 3 | 1 | ***Low*** |
| R15 | Overcapacity | 2 | 1 | ***Low*** |
| R01 | Banjir | 1 | 3 | ***Low*** |
| R10 | Cybercrime | 1 | 3 | ***Low*** |
| R25 | Serangan virus | 1 | 3 | ***Low*** |
| R09 | Vandalisme | 1 | 2 | ***Low*** |
| R12 | Backup Failure | 1 | 3 | ***Low*** |
| R22 | Memori penuh | 1 | 2 | ***Low*** |

Pada tabel 9 datas, tahapan proses evaluasi risiko, terdapat 26 kemungkinan risiko yang sudah dianalisis dan dikategorikan sesuai dengan level risikonya. Terdapat 3 risiko dengan tingkatan *high* yaitu: R11, R17 dan R18. Lalu 13 risiko dengan tingkatan *medium* yaitu: R21, R06, R20, R05, R19, R23, R02, R16, R03, R24, R26, R04, R14. Dan terakhir 10 risiko dengan tingkatan *low* yaitu: R07, R08, R13, R15, R01, R10, R25, R09, R12, R22.

### 4.4. Perlakuan Risiko

Setelah analisis risiko diatas, maka selanjutnya akan masuk pada tahap *Risk Treatment* atau perlakuan risiko. Pada tahap ini dilakukan pemberian usulan tindakan risiko terhadap kemungkinan risiko yang sudah di kelompokkan berdasarkan *risk level* pada tabel 9.

Tabel 10. Usulan Perlakuan Risiko

| Id | Kemungkinan Risiko | Risk Level | Tindakan Risiko |
|---|---|---|---|
| R11 | Server down | **High** | Melakukan pengecekan berskala pada database |
| R17 | Web service mati secara tiba-tiba | **High** | Memberikan pemberitahuan kepada user saat web service mati. Melakukan troubleshooting saat web service mati. |
| R18 | Koneksi jaringan terputus | **High** | Mengganti ISP (Internet Service Proider) dengan yang baru |
| R21 | Gagal update | **Medium** | Setelah ditemukan beberapa kesalahan sistem segera melakukan perbaikan sistem. |
| R06 | Human Error | **Medium** | Melakukan training pada setiap SDM |
| R20 | Sistem crash | **Medium** | Melakukan perbaikan jika ditemukan kesalahan sistem pada saat melakukan maintenence |
| R05 | Listrik Padam | **Medium** | Menyediakan generator set listrik dengan daya yang sesuai dengan kebutuhan. Kemudian menyiapkan Uninterruptible Power Supply (UPS) |

| Id | Kemungkinan Risiko | Risk Level | Tindakan Risiko |
|---|---|---|---|
| R19 | Koneksi jaringan tidak stabil | **Medium** | Mengganti ISP (Internet Service Proider) dengan yang baru |
| R23 | Kegagalan software | **Medium** | Melakukan pengecekan terhadap driver, IRQ, atau resource lainya pada PC, jika diperlukan melakukan install ulang pada OS |
| R02 | Gempa Bumi | **Medium** | Menyediakan tempat yang aman untuk perangkat-perangkat yang ada |
| R16 | Overload | **Medium** | Melakukan refresh penggunaan db log, temp, dan RAM. Serta melakukan pengecekan terhadap database perusahaan |
| R03 | Petir | **Medium** | Memasang alat penangkal petir |
| R24 | Kegagalan hardware | **Medium** | Memberikan asuransi terhadap aset hardware yang ada |
| R26 | Proses maintenance tidak terjadwal | **Medium** | Melakukan penjadwalan maintenance rutin setiap minggu |
| R04 | Kebakaran | **Medium** | Menyiapkan alat pemadam kebakaran |
| R14 | Data corrupt | **Medium** | Melakukan backup data secara berskala |
| R08 | Penyalahgunaan hak akses | **Low** | Memberikan batasan akses pada setiap user |
| R07 | Data dan Informasi diakses oleh pihak yang tidak berwenang | **Low** | Memberikan batasan akses pada setiap user |
| R13 | Overheat | **Low** | Menyediakan ruang yang memiliki AC (Air Conditioner) dan menambah fan pada semua hardware |
| R15 | Overcapacity | **Low** | Menambah kapasitas memori yang lebih besar agar daya tampungnya lebih optimal. Melakukan cek memori secara berkala. |
| R01 | Banjir | **Low** | Meletakkan alat alat infrastruktur di tempat yang aman dari banjir |
| R10 | Cybercrime | **Low** | Mengganti password server secara berkala. |
| R25 | Serangan virus | **Low** | Melakukan scanning antivirus terhadap portable device, dan selalu mengaktifkan firewall dan internet security |
| R09 | Vandalisme | **Low** | Memasang dan memantau CCTV di gedung perusahaan. |
| R12 | Backup Failure | **Low** | Memperhatikan penggunaan memori yang digunakan database agar jangan sampai penuh. Membuat maintenance plan yang tepat. Serta membuat SOP dan melakukan backup data secara berkala. |
| R22 | Memori penuh | **Low** | Menambah kapasitas memori yang lebih besar agar daya tampungnya lebih optimal. Melakukan cek memori secara berkala. |

Dalam tabel 10 diatas ini diharapkan dapat meminimalisir kemungkinan risiko yang dapat terjadi pada aplikasi ERP.

## 5. KESIMPULAN DAN SARAN

Penelitian manajemen risiko dengan menggunakan kerangka kerja dari ISO31000:2018 yang telah dilakukan di sistem ERP pada PT. Trust Lerinvital Timur, mendapatkan hasil yang sudah dikaji dalam pembahasan, hasil tersebut mencakup penilaian risiko, identifikasi risiko, analisis risiko, evaluasi risiko hingga tahap perlakuan risiko. Dengan hasil akhir terdapat 26 risiko yang menghambat kinerja dari proses bisnis yang berjalan di Pt. Trust Lerinvital Timur. Berdasarkan penelitian ini, sudah ditemukan 3 risiko yang masuk dalam tingkatan high, seperti server down, webservice yang sering mati, dan juga koneksi jaringan yang sering terputus. Selain itu juga terdapat 13 risiko dengan klasifikasi medium, yang meliputi kegagalan software, sistem crash, human error, koneksi jaringan tidak stabil, gempa bumi, petir, kerusakan hardware, proses maintenence tidak terjadwal, overload, serta data corrupt. Dan juga terdapat 10 risiko dengan tingkatan low, seperti penyalahgunaan hak akses, overheat, overcapacity, banjir, cybercrime, serangan virus, vandalisme, kegagalan backup, serta memori penuh. Setelah penelitian ini dilakukan, diharapkan dari penelitian ini dapat digunakan sebagai acuan dan pedoman bagi PT. Trust Lerinvital Timur untuk melakukan penanganan risiko yang sudah direkomendasikan, sehingga risiko dapat diminimalisir. Diharapkan pula menerapkan perlakuan risiko seperti pada tabel 10 seperti mengganti ISP terbaru, melakukan troubleshooting ketika web service mati, serta melakukan pengecekan berskala pada database, sehingga proses bisnis perusahaan dapat terus berjalan dengan baik.

## DAFTAR PUSTAKA

[1] S. Wiyono and A. R. Tanaamah, “Analisis Kinerja SI/TI Pada PDAM Kota Salatiga

Menggunakan Kerangka IT Balanced Scorecard," *J. Buana Inform.*, vol. 8, no. 4, pp. 181–192, 2017, doi: 10.24002/jbi.v8i4.1442.

[2] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[3] F. Manoppo, "Perencanaan Strategis Sistem Informasi Menggunakan Metode Ward And Peppard (Studi Kasus: Pada STMIK Parna Raya Manado) Franky," *Semin. Nas. IPTEK Terap.*, vol. 2, pp. 56–62, 2017, [Online]. Available: http://conference.poltektegal.ac.id/index.php/senit2017.

[4] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *J. Ilm. Inform. Glob.*, vol. 11, no. 1, 2020, doi: 10.36982/jig.v11i1.1073.

[5] A. R. Tampubolon and Suhardi, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010," *J. Telemat.*, vol. 7, no. 2, pp. 1–10, 2011.

[6] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 ( Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square )," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[7] I. Lanin, "Standar Baru Manajemen Risiko ISO 31000:2018," *IBFG Institute*, 2018. https://ibfgi.com/risk-management-31000/ (accessed Apr. 12, 2018).

[8] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 3, pp. 250–258, 2017, doi: 10.29207/resti.v1i3.94.

[9] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201–6208, 2015.

[10] F. L. Nice and R. V. Imbar, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *J. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 1–11, 2017.

[11] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019.

[12] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 2020, doi: 10.33557/binakomputer.v2i1.799.

[13] Angraini and I. D. Pertiwi, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/431.

[14] D. E. Adi and N. Susanto, "Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar," *J. Metris*, vol. 18, pp. 113–118, 2017.

[15] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000," *Sebatik 2621-069X*, vol. 23 No. 1, pp. 36–43, 2019, doi: 1410-3737.

[16] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

[17] 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.