# ANALISIS RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DISHUBKOMINFO KABUPATEN TULUNGAGUNG

**Balqis Lembah Mahersmi[1)], Feby Artowini Muqtadiroh[2)] Bekti Cahyo Hidayanto[3)]**
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember
Jl. Raya ITS Sukolilo, Surabaya, 60111
Telp : (031) 599425, Fax : (031) 5923465
E-mail : balqis.lembah12@mhs.is.its.ac.id[1)]

***Abstrak***

*Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung adalah unit pelayanan masyarakat bidang tranportasi dan teknologi informasi. Untuk mencapai tujuan dan melaksanakan tugas fungsi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung, diperlukan adanya suatu manajemen risiko untuk mengarahkan dan mengendalian organisasi dalam mengelola risiko yang mungkin terjadi. Tujuan dari penelitian ini adalah untuk mengidentifikasi, menilai dan memitigasi risiko yang berkaitan dengan teknologi informasi yang dikelola oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung berdasarkan metode OCTAVE. Hasil dari penelitian ini adalah melakukan identifikasi risko yang dapat terjadi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung terkait implementasi teknologi informasi dan memberikan masukan atau rekomendasi mitigasi IS0 27001 kepada pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko yang akan muncul terkait implementasi teknologi informasi. Pada akhir penelitian ada 13 risiko yang muncul dengan 31 kejadian risiko. nilai RPN tertinggi sebesar 378 dan terendah sebesar 45. Mitigasi risiko menggunakan 12 kontrol pada ISO 27001.*

***Kata Kunci**: Analisis risiko, Keamanan Informasi, Octave, Teknologi Informasi*

***Abstract***

*Department of transportation Communication and Information district Tulungagung is a community service unit areas of transport and information technology. To succeed and perform tasks on the Department of Communication and Information Tulungagung, needed a risk management organization control to direct and manage the risks that may occur Purpose of this study is to identify, assess and mitigate risks based OCTAVE method. The results is to identify risking which can occur at the Department of Communication and Information Tulungagung related IT implementation and provide input or recommendations to the Department of Communication and Information Tulungagung how measures proper risk mitigation to the results of risk identification will appear related to the implementation of IT. At ending the study there is a risk that appeared 13 to 31 the risk event. The highest RPN value of 378 and a low of 45. Risk mitigation using 12 controls in ISO 27001.*

***Keywords**: Risk analysis, Octave, Information Technology*

## 1. PENDAHULUAN

Teknologi informasi merupakan bagian yang tidak terpisahkan dari suatu perusahaan karena dapat membantu meningkatkan efektifitas dan efisiensi proses bisnis perusahaan. Tetapi untuk mencapai hal tersebut, diperlukan adanya pengelolaan TI yang baik dan benar agar keberadaan TI mampu menunjang kesuksesan organisasi dalam pencapaian tujuannya.

Tugas utama dari dinas perhubungan komunkasi dan informatika kabupaten Tulungagung adalah memberikan pelayanan jasa transportasi dan pelayanan informasi publik yang efektif, efisien, aman, nyaman dan tepat waktu. Selain itu terdapat bidang baru di dinas perhubungan komunkasi dan informatika Kabupaten Tulungagung yakni komunikasi dan informatika yang bertugas dalam melaksanakan

pengendalian dan pengawasan kegiatan usaha jasa Komunikasi dan jasa Informatika selain itu juga melakukan penyiapan pengembangan Teknologi Elektronik Informatika di kabupaten Tulungagung [1].

Analisis risiko digunakan organisasi untuk melakukan identifikasi risiko yang timbul akibat penggunaan teknologi informasi. Dengan melakukan analisis risko, dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung dapat membuat langkah-langkah penanganan terhadap masing-masing risiko apa saja yang mungkin akan dihadapi di kemudian hari. OCTAVE merupakan sebuah kerangka kerja yang memungkinkan organisasi untuk memahami, menilai dan menangani risiko keamanan informasi mereka dari perspektif organisasi. Metode OCTAVE cocok digunakan untuk menganalisi risiko keamanan informasi karena menilai terjadinya risko dari berbagai perspektif organisasi [2].

Oleh karena itu, tujuan dari penelitian ini adalah untuk melakukan identifikasi risiko yang terdapat pada dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung terkait dengan aset teknologi informasi yang digunakan dalam layanan teknologi informasi dan memberikan rekomendasi mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko serta sesuai harapan organisasi. Harapan dari penulis adalah mampu menghasilkan sebuah dokumen mitigasi risiko pada layanan teknologi informasi yang dikendalikan oleh dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung.

## 2. Tinjauan Pustaka

Berikut ini adalah tinajauan pustaka yang digunakan dalam penelitian ini.

### 2.1 Profil Organisasi

Dalam konteks ini Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung memiliki kompetensi sebagai perumus kebijakan dan pelaksana kebijakan di Bidang Perhubungan Komunikasi dan Informatika. Bidang Komunikasi dan Informatika mempunyai tugas sebagai berikut:

- Melaksanakan perumusan kebijakan teknis telekomunikasi dan informatika di bidang perhubungan.
- Melaksanakan pengendalian dan pengawasan kegiatan usaha jasa Telekomunikasi dan jasa Informatika.

  Untuk melaksanakan tugas sebagaimana dimaksud Bidang Komunikasi dan Informatika mempunyai fungsi:
- Penyiapan perencanaan, pengaturan, pengawasan dan pengendalian usaha jasa informatika.
- Perencanaan, pengaturan, pengawasan dan pengendalian usaha jasa informatika.

### 2.2 Keamanan Informasi

Keamanan informasi adalah suatu upaya dalam mengamankan aset informasi dari berbagai sumber ancaman untuk memastikan keberlangsungan bisnis, meminimalisir dampak yan terjadi akibat adanya ancaman tersebut. Berikuti ini merupakan model CIA triad [3].


*Gambar 1. CIA Triad*

### 2.3 Manajemen Risiko

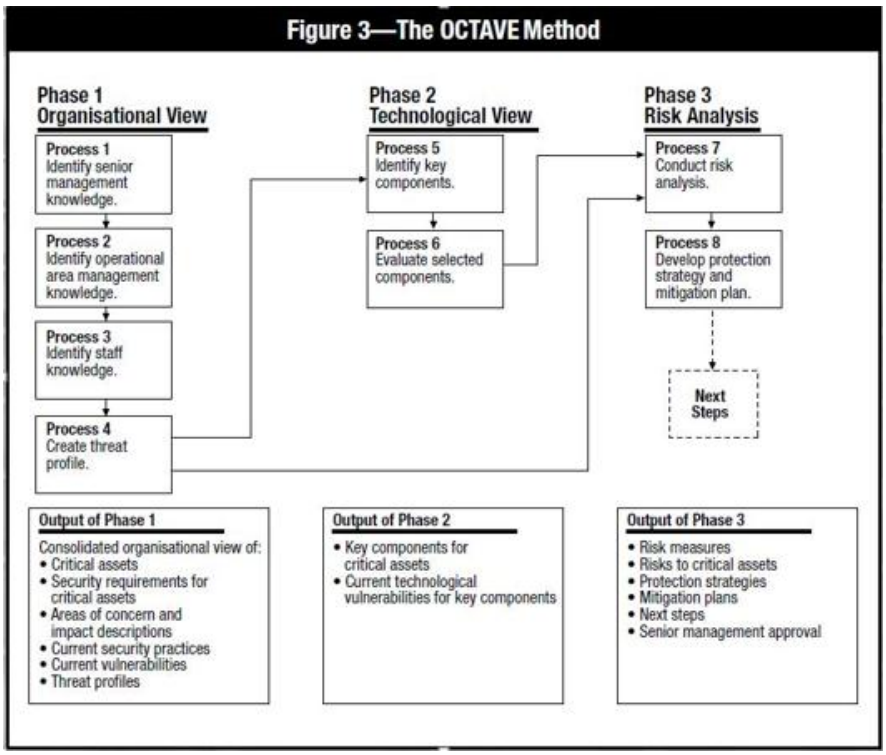
Manajemen risiko adalah proses pengelolaan risiko yang mencakup identifikasi, evaluasi, dan pengendalian risiko yang dapat mengancam kelangsungan usaha atau aktivitas perusahaan.

#### 2.3.1 Aset Informasi

Aset informasi merupakan sekumpulan pengetahuan yang diatur dan dikelola sebagai satu kesatuan oleh organisasi sehingga dapat dipahami, dibagikan, dilindungi dan dapat dimanfaatkan dengan baik. Aset informasi terdiri dari: *people, hardware, software, network, procedur, data*.

### 2.3.2 OCTAVE

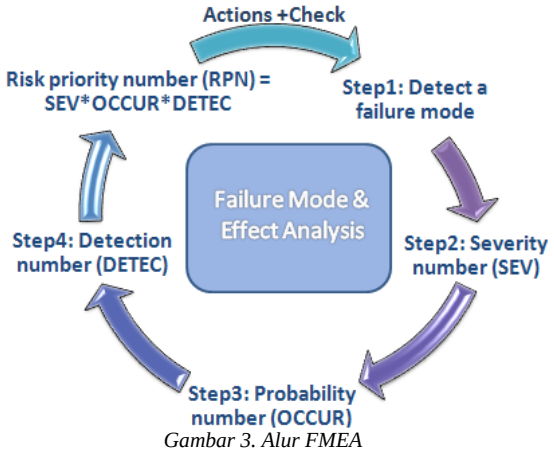
OCTAVE merupakan sebuah kerangka kerja yang memungkinkan organisasi untuk memahami, menilai dan menangani risiko keamanan informasi mereka dari perspektif organisasi Gambar berikut merepresentasikan gambaran metode OCTAVE yang berisi fase, proses, dan output dari setiap fase yang ada:




*Gambar 2. Octave method*

### 2.3.3 FMEA

*Failure Mode and Effect Analysis* (FMEA) merupakan metode yang digunakan menganalisa potensi kesalahan atau kegagalan dalam sistem atau proses, dan potensi yang teridentifikasi akan diklasifikasikan menurut besarnya potensi kegagalan dan efeknya terhadap proses. Berikut merupakan diagram alur dari tahapan proses FMEA.




*Gambar 3. Alur FMEA*

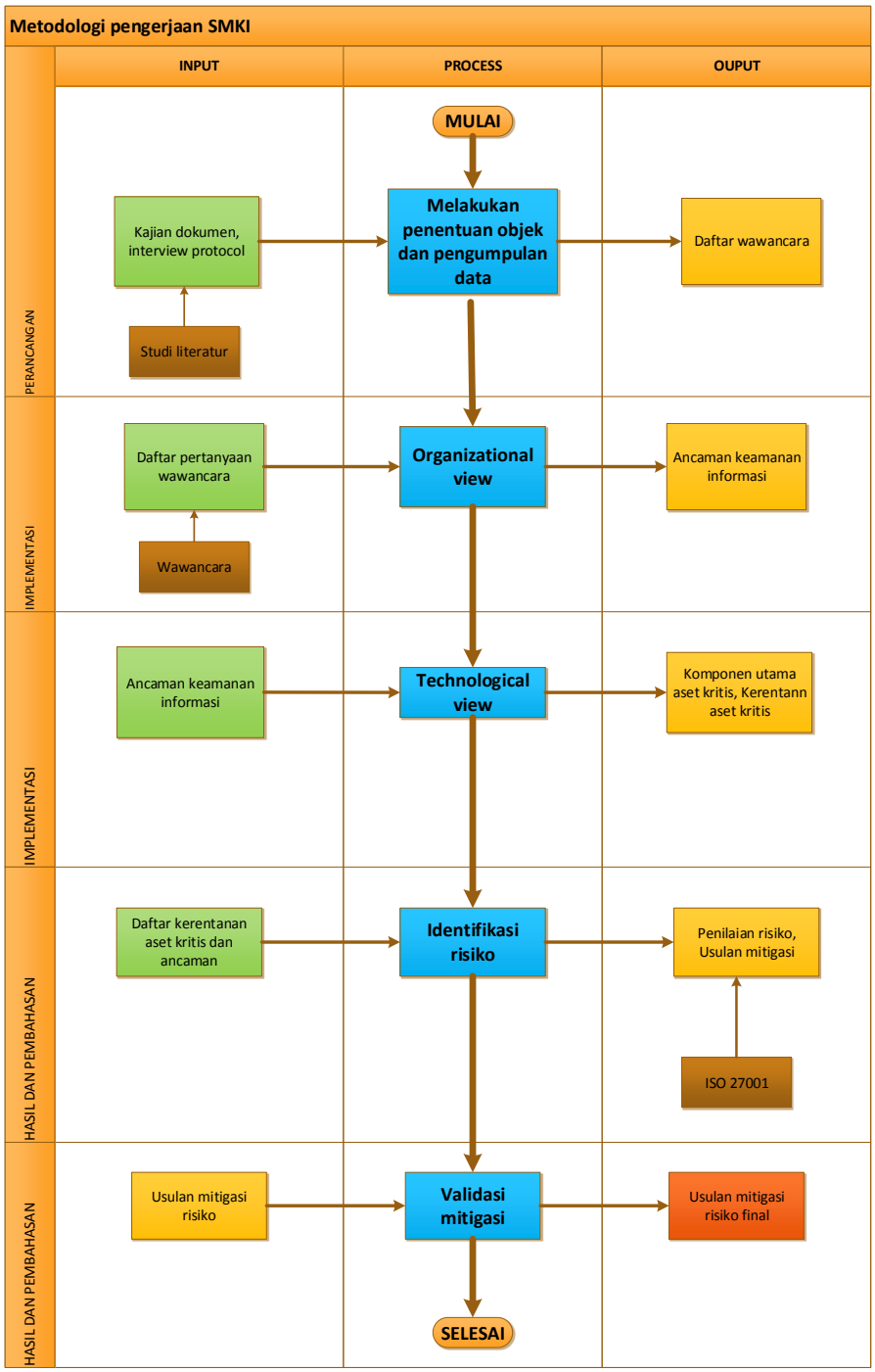
### 2.4 ISO 27001

Tujuan utama dari ISO 27001 adalah untuk membangun, mempertahankan, mengembangkan, dan terus meningkatkan sistem informasi manajemen yang efektif. ISO 27001 menjelaskan bagaimana mengelola keamanan informasi melalui sistem manajemen keamanan informasi. Fase-fase tersebut adalah sebagai berikut [4]:


*Gambar 4. ISO 27001*

## 2. METODOLOGI PENELITIAN

Permasalahan pada penelitian ini akan diselesaikan dengan metode penelitian yang tergambar pada diagram alir berikut.




*Gambar 5. Metodologi Penelitian*

- Pada tahap menggunakan fase pertama melakukan penentuan objek dan pengumpulan data yaitu melakukan analisis objek tujuan penelitian.
- Fase organizational view merupakan tahapan untuk membuat profil ancaman *(threat profile)* dengan cara menentukan aset yang penting bagi organisasi dan kebutuhan pengamanannya.
- Pada tahapan *Technological View* dilakukan identifikasi proses bisnis dan profil ancaman terhadap asset kritis yang didukung layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung dan identifikasi kelemahan infrastruktur.
- Pada tahap identifikasi risiko melakukan identifiksi risiko yaitu melakukan penilaian risiko dan melakukan mitigasi risiko berdasarkan ISO 27001 serta diskusi bersama dengan pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.
- Pada tahap ini validasi yang telah selesai dilakukan pengecekan kesesuaian dengan keadaan yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

## 3. HASIL DAN PEMBAHASAN

Berikut merupakan hasil dan pembahsan penelitian.

### 3.1 Identifikasi Potential Cause

Potensial causes merupakan penyebab dari timbulnya risiko yang terjadi dan didapatkan dari identifikasi kerentanan dan ancaman dari aset informasi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung. Berikut ini merupakan tabel potential cause:

Tabel 1. Potential cause

| Aset | Kerentanan | Ancaman | Potential Cause |
|---|---|---|---|
| Hardware<br>• Komputer<br>• Server<br>• CCTV | Kurangnya skema pergantian perangkat keras secara berkala<br>Kurangnya pemeliharaan/prosedur untuk pemeliharaan yang rumit | Perusakan peralatan atau media | *Maintenance* yang tidak teratur |
| | Kerentanan terhadap kelembapan, debu, kotoran. | Debu, korosi, pendingin, air | Kerusakan fisik pada server |
| | Kerentanan terhadap nilai informasi yang tersimpan pada PC | Pencurian | Kurangnya pengamanan organisasi |
| | Kerentanan terhadap voltase yang bervariasi<br>Hubungan arus pendek pada panel listrik | Hilangnya pasokan listrik | Korsleting listrik |
| | Supply listrik yang tidak stabil | Hilangnya pasokan listrik | Pemadaman listrik |
| | Beban kerja server yang tinggi | AC diruangan server mati/rusak | Server overheat |
| | Pertambahan memori yang cepat dalam pemrosesan data | Server lemot | Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full) |
| Data:<br>Data vendor LPSE | Data terlalu sering diupdate<br>Data tidak terupdate | Redudansi data<br>Data tidak lengkap | Kesalahan dalam penginputan dan penghapusan data |

| Aset | Kerentanan | Ancaman | Potential Cause |
|---|---|---|---|
| Data pengadaan barang setiap dinas<br>Data informasi seputar kegiatan di Kabapuaten Tulungagung | Kurangnya salinan back-up | Data hilang<br>Data tidak terbackup | Organisasi tidak melakukan prosedur *backup* |
| | Jaringan internet kurang optimal | Data korup | Speed koneksi internet yang lemah dan tidak stabil |
| | Kesalahan penempatan hak akses | Pembobolan data | Tidak ada penggunaan hak akses |
| | Terlalu banyak data yang diinputkan | Database penuh | Server down |
| Layanan teknologi informasi:<br>Website pemerintah<br>Pemantauan kondisi lalu lintas<br>Pengadaan barang LPSE. | Kurangnya dokumentasi user manual untuk aplikasi | Kesalahan pengguna | Kurangnya dokumentasi (user manual) untuk karyawan baru |
| | Kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi | Aplikasi terserang hacker | Password tidak pernah diganti |
| | Karyawan kurang memperhatikan pentingnya antivirus | Aplikasi terserang virus | PC terserang virus |
| | Kekurangan yang telah diketahui pada perangkat lunak<br>Tidak ada atau tidak cukup pengujian perangkat lunak | Penyalahgunaan wewenang pada hak akses yang dimiliki | Staf mengetahui kelemahan pada aplikasi |
| | Karyawan kurang teliti dan competen | Aplikasi eror | Kesalahan coding pada fungsional software |
| Perangkat jaringan (*network*) | Jalur komunikasi yang tidak dilindungi<br>Arsitektur jaringan yang tidak aman | Penyadapan informasi penting melalui jaringan<br>Celah masuknya hacker<br>Remote Spying | Lemahnya keamanan di sistem internal TI |
| | Manajemen jaringan yang tidak cukup (ketahanan routing)<br>Sambungan kabel yang buruk | Jaringan LAN lemot | Kurangnya mekanisme pemantauan terhadap jaringan |
| | Kualitas jaringan yang kurang baik | Konektifitas internet menurun | Gangguan jaringan pada provider |
| | Bencana alam dan kerjadian yang tidak terduga | Koneksi terputus | Kerusakan pada infrastruktur jaringan |
| | SDM yang tidak kompeten | Kesalahan pengalamatan IP | Kesalahan dalam melakukan konfigurasi access point |

| Aset | Kerentanan | Ancaman | Potential Cause |
|---|---|---|---|
| | Peletakan kabel yang sembarangan<br>Tidak ada pelindung kabel | Kabel LAN digigit tikus | Kabel digigit oleh hewan |
| | Karyawan yang tidak kompeten | Kesalahan pengalamatan IP | Kesalahan dalam melakukan konfigurasi access point |
| Karyawan (*People*) | Ketidakhadiran karyawan | Kekurangan tenaga kerja | Adanya share login |
| | Pelatihan terkait teknologi informasi tidak cukup | Kesalahan penggunaan | Kurangnya training prosedur penggunaan TI yang diberikan |
| | Kurangnya kesadaran akan keamanan | Kesalahan penggunaan | Kurangnya sosialisasi tentang regulasi dan sanksinya |
| | Kurangnya mekanisme pemantauan | Pengolahan data illegal | Pengolahan data illegal oleh karyawan |
| | Bekerja tanpa pengawasan senior management | Karyawan tidak memperhatikan prosedur yang ada<br>Pencurian PC | Kurangnya mekanisme pemantauan |
| | Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi | Penggunaan peralatan yang tidak sah<br>Penyangkalan atas tindakan | Tidak ada peraturan terkait keamanan informasi |
| | Karyawang kurang teliti | Kesalahan penginputan dan penghapusan data | Kesalahan penginputan dan penghapusan data |
| | Pelatihan keamanan yang tidak cukup | Penyalahgunaan wewenang pada hak akses yang dimiliki<br>Password PC diketahui orang lain<br>Pemalsuan hak | Staf tidak logout ketika meninggalkan komputer |
| | Karyawan bidang kominfo bisa mengakses | Tidak ada batasan hak akses | Tidak ada pengaturan untuk manajemen hak akses user atau user privilege |

**3.2 Identifikasi Risko**

Sebelum tahapan penilaian risiko, terlebih dahulu akan diidentifikasi risiko-risiko yang dapat mengancam asset informasi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung. Risiko yang dimaksudkan adalah berupa kejadian yang memiliki probabilitas untuk terjadi bahkan sering terjadi baik disebabkan oleh faktor yang berasal dari kondisi eksternal maupun kondisi internal perusahaan yaitu bencana alam, gangguan fasilitas umum, social, dan operasional. Berikut merupakan tabel identifikasi risiko:

Tabel 2. Identifikasi risiko

| Aset | Potential Cause | Risiko |
|---|---|---|
| Hardware<br>• Komputer<br>• Server<br>• CCTV | *Maintenance* yang tidak teratur<br>Server overheat<br>Kerusakan fisik pada server | Hardware failure |
| | Kurangnya pengamanan organisasi | Pencurian media atau informasi penting |
| | Korsleting listrik | Kebakaran |
| | Pemadaman listrik | Power failure |
| | Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full) | Memory penuh |
| Data:<br>Data vendor LPSE<br>Data pengadaan barang setiap dinas<br>Data informasi seputar kegiatan di Kabapuaten Tulungagung | Kesalahan dalam penginputan dan penghapusan data | Human atau technician error |
| | Organisasi tidak melakukan prosedur *backup*<br>Server down | Backup data failure |
| | Speed koneksi internet yang lemah dan tidak stabil | Network failure |
| | Password disimpan pada desktop komputer | Penyalahgunaan hak akses |
| Layanan teknologi informasi:<br>Website pemerintah<br>Pemantauan kondisi lalu lintas<br>Pengadaan barang LPSE. | Kurangnya dokumentasi (user manual) untuk karyawan baru<br>PC terserang virus | Human atau technician error |
| | Kesalahan coding pada fungsional software | Software failure |
| | Password tidak pernah diganti | Penyalahgunaan hak akses |
| | Staf mengetahui kelemahan pada aplikasi | Modifikasi dan pencurian database |
| Perangkat jaringan (*network*) | Lemahnya keamanan di sistem internal TI | Serangan hacker |
| | Kurangnya mekanisme pemantauan terhadap jaringan<br>Gangguan jaringan pada provider<br>Kerusakan pada infrastruktur jaringan<br>Kesalahan dalam melakukan konfigurasi access point<br>Kabel digigit oleh hewan<br>Kesalahan dalam melakukan konfigurasi access point | Network failure |
| Karyawan<br>(*People*) | Adanya share login<br>Tidak ada pengaturan untuk manajemen hak akses user atau user privilege | Penyalahgunaan hak akses |
| | Kurangnya training prosedur penggunaan TI yang diberikan<br>Kesalahan penginputan dan penghapusan data | Human atau technician error |

| Aset | Potential Cause | Risiko |
|---|---|---|
| | Staf tidak logout ketika meninggalkan komputer | |
| | Kurangnya sosialisasi tentang regulasi dan sanksinya | Pelanggaran terhadap aturan atau regulasi yang berlaku |
| | Pengolahan data illegal oleh karyawan | Modifikasi dan pencurian database |
| | Kurangnya mekanisme pemantauan<br>Tidak ada peraturan terkait keamanan informasi | Pencurian media atau informasi penting |

### 3.3 Penilaian Risiko

Pada tahap ini dilakukan penentuan tingkat severity, occutance, dan detection. Tahapan ini dilakukan dengan mendeskripsikan informasi secara lebih dalam terhadap risiko yang telah diidentifikasi. Hasil dari tahap ini adalah nilai severity, occurance dan detection pada setiap proses risiko yang nantinya akan digunakan untuk menghitung RPN (Risk Priority Number) parameter dari level severity, occurance, dan detection. Berikut meruapakan tabel penilaian risiko:

Tabel 3. Penilaian risiko

| Risiko | Potential Cause | SEV | OCC | DEC | RPN | LEVEL |
|---|---|---|---|---|---|---|
| Hardware failure | *Maintenance* yang tidak teratur | 9 | 3 | 3 | 45 | *Low* |
| | Server overheat | 9 | 1 | 6 | 54 | *Low* |
| | Kerusakan fisik pada hardware | 9 | 3 | 3 | 81 | *Low* |
| Software failure | Kesalahan coding pada fungsional software | 5 | 4 | 3 | 60 | *Low* |
| Network failure | Speed koneksi internet yang lemah dan tidak stabil | 9 | 7 | 6 | 378 | *Very high* |
| | Kurangnya mekanisme pemantauan terhadap jaringan | 7 | 1 | 6 | 42 | *Very low* |
| | Gangguan jaringan pada provider | 9 | 7 | 6 | 378 | *Very high* |
| | Kerusakan pada infrastruktur jaringan | 7 | 3 | 6 | 125 | *Medium* |
| | Kesalahan dalam melakukan konfigurasi access point | 7 | 4 | 6 | 168 | *High* |
| | Kabel digigit oleh hewan | 7 | 3 | 6 | 125 | *Medium* |
| Power failure | Pemadaman listrik | 9 | 7 | 6 | 378 | *Very high* |

| Risiko | Potential Cause | SEV | OCC | DEC | RPN | LEVEL |
|---|---|---|---|---|---|---|
| Backup data failure | Organisasi tidak melakukan prosedur *backup* | 6 | 4 | 4 | 96 | *Low* |
| | Server down | 9 | 7 | 6 | 378 | *Very high* |
| Human atau technician error | Kurangnya dokumentasi (user manual) untuk karyawan baru | 5 | 4 | 4 | 80 | *Low* |
| | PC terserang virus | 5 | 4 | 3 | 60 | *Low* |
| | Kesalahan dalam penginputan dan penghapusan data | 6 | 4 | 4 | 96 | *Low* |
| | Kurangnya training prosedur penggunaan TI yang diberikan | 5 | 3 | 4 | 60 | *Low* |
| | Staf tidak logout ketika meninggalkan komputer | 6 | 5 | 4 | 120 | *Medium* |
| Serangan hacker | Lemahnya keamanan di sistem internal TI | 6 | 4 | 5 | 120 | *Medium* |
| Penyalahgunaan hak akses | Tidak ada penggunaan hak akses | 6 | 4 | 5 | 120 | *Medium* |
| | Adanya share login | 6 | 4 | 5 | 120 | *Medium* |
| | Tidak ada pengaturan untuk manajemen hak akses user atau user privilege | 6 | 3 | 5 | 72 | *Low* |
| | Password tidak pernah diganti | 6 | 4 | 5 | 120 | *Medium* |
| Pencurian media atau informasi penting | Kurangnya pengamanan organisasi | 6 | 4 | 4 | 96 | *Very low* |
| | Kurangnya mekanisme pemantauan | 5 | 3 | 3 | 45 | *Very low* |
| | Tidak ada peraturan terkait keamanan informasi | 6 | 4 | 4 | 96 | *Low* |
| Kebakaran | Korsleting listrik | 9 | 1 | 6 | 54 | *Low* |
| Memory penuh | Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full) | 9 | 7 | 6 | 378 | *High* |

| Risiko | Potential Cause | SEV | OCC | DEC | RPN | LEVEL |
|---|---|---|---|---|---|---|
| Modifikasi dan pencurian database | Staf mengetahui kelemahan pada aplikasi | 9 | 1 | 5 | 45 | *Very low* |
| | Pengolahan data illegal oleh karyawan | 9 | 1 | 5 | 45 | *Very low* |
| Pelanggaran terhadap aturan atau regulasi yang berlaku | Kurangnya sosialisasi tentang regulasi dan sanksinya | 5 | 4 | 4 | 80 | *Low* |

### 3.4 Mitigasi Risiko

Setelah melaukan identifikasi aset kritis, identifikasi risko dan penilaian risiko selanjutnya adalah melakukan mitigasi terhadap risiko tersebut. Mitigasi dilakukan dengan menggunakan standar ISO 27001 dan diskusi langsung dengan pihak dinas perhubungan komunikasi dan informatika kabupaten tulungagung. Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO/IEC 27001 yang direkomendasikan untuk penanganan risiko-risiko yang telah diidentifikasi tersebut adalah :

*a. Performance evaluation*
*b. Information security incident management*
*c. System and aplication acess control*
*d. Supllier service delivery management*
*e. Equipment*
*f. Backup*
*g. Human resource security*
*h. Control of operational software*
*i. Assess control*
*j. Information transfer*
*k. Organization of information security*
*l. Leadership*

Berikut ini merupakan penjelasan singkat mengenai mitigasi risiko pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung:

Tabel 4. Mitigasi Risiko

| Aset | Risiko | Penyebab Risiko | Dampak Risiko | Tindakan Mitigasi Berdasarkan ISO 27001 | | |
|---|---|---|---|---|---|---|
| | | | | Kontrol | Sub-Kontrol | Keterangan |
| Hardware:<br>• Komputer<br>• CCTV<br>• Server | Hardware failure | *Maintenance* yang tidak teratur | • Kerusakan asset teknologi<br>• Kinerja hardware menurun | **Performance evaluation :** Untuk menjaga kualitas hardware diperlukan evluasi performa. | **Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring terhadar aset teknologi informasi yang dimiliki oleh organisasi. | • Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi.<br>• Monitoring dilakukan secara berkala untuk memastikan aset teknologi |

Penjelasan dari alasan dipilihnya 12 rekomendasi kontrol yang diberikan diatas sesuai dengan risiko-risiko tersebut adalah sebagai berikut :

1. Identifikasi risiko modifikasi dan pencurian database

Dengan penyebab data diakses oleh pihak yang tidak berwenang yang berdampak pada data diketahui dan dimanfaatkan oleh pihak yang tidak berwenang maka dilakukan tindakan pembatasan akses yaitu akses terhadap informasi dan aplikasi oleh user harus dibatasi sesuai dengan kebijakan keamanan yang

telah ditentukan. Selain itu dilakukan pemberhentian pegawai yaitu dengan penghapusan hak akses pegawai terhadap informasi dan fasilitas pemrosesan informasi sejak mereka dinyatakan berhenti.

2. Identifikasi risiko backup data failure

Data tidak terback-up biasanya terjadi karena kapasitas media penyimpanan yang tidak mencukupi yang berdampal informasi yang ditampilkan tidak updaye maka perlu dilakukan tindakan backup secara berkala dan manajemen kapasitas yaitu kebutuhan kapasitas harus dimonitor dan ditinjau secara berkala.

3. Identifikasi risiko human/technician error

Dengan penyebab kesalahan dalam pengoperasian system hardware maupun software yang berdampak kerusakan pada system hardware maupun software dalam kegiatan operasional terganggu maka perlau dilakukan tindakan pendidikan dan pelatihan keamanan informasi pada karyawan sehingga dapat memahami keamanan informasi yang ditetapkan perusahaan demi mengurangi terjadinya kesalahan kerja (human eror).

4. Identifikasi risiko memory full

Dengan penyebab kapasitas media penyimpanan tidak mencukupi dan banyak sekali data yang harus diinputkan setiap harinya yang berdampak tidak mampu meyimpan data-data baru maka perlu dilakukan tindakan back-up secara berkala dan manajemen kapasitas yaitu kebutuhan kapasitas harus dimonitor secara berkala.

5. Identifikasi risiko Serangan hacker

Dengan penyebab lemahnya keamanan di system internal TI yang berdampak data diketahui dan dimanfaatkan oleh pihak yang tidak berwenang yang menyebabkan terhambatnya proses bisnis dan merusak citra pelayanan publik maka perlu dilakukan tindakan control akses jaringan yaitu dengan prosedur monitoring dalam penggunaan system pengolahan informasi harus dilakukan secara berkala.

6. Identifikasi risiko Hardware failure

Hardware failure disebabkan oleh beberapa hal yaitu diantaranya adanya virus yang menyerang computer, server terserang malware, maintenance yang tidak teratur, dan kesalahan melakukan konfigurasi yang berdampak kehilangan data, database korup, bahkan kerusakan pada aset dan teknologi tersebut maka diperlukan adanya pemeliharaan dan control secara berkala terhadap hardware untuk memastikan ketersediaan dan integritas hardware.

7. Identifikasi risiko software failure

Dengan penyebab kesalahan coding pada fungsional software dan pc terserang virus yang dapat menyebabkan application crashed, kehilangan data, database korup maka diperlukan pembatasan akses ke source code program dan harus dikontrol dengan ketat untuk mencegah masuknya fungsionalitas yang tidak sah dan untuk menghindari perubahan yang tidak disengaja selain itu diperlukan adanya deteksi, pencegahan, dan pemulihan untuk melindungi software dari virus, trojan, dan malware sesuai dengan prosedur.

8. Identifikasi risiko power failure.

Dengan penyebab korsleting listrik berdampak kerusakan pada aset teknologi seperti server dan pc yang tiba-tiba mati dan dapat menyebabkan kehilangan data yang berdampak tidak dapat mengoperasionalkan server dan pc sehingga kegiatan operasional terhenti maka dari itu dibutuhkan perlindungan fisik terhadap kerusakan dan perlu dilakukan back-up agar data tetap tersimpan walaupun terjadi power failure.

9. Identifikasi risiko network failure

Dengan penyebab kerusakan pada komponen infrastruktur jaringan internal yang berdampak beberapa kegiatan operasioal organisasi yang terhubung dengan jaringan LAN dan internet terhenti, maka perlu dilakukan tindakan control jaringan dengan cara dimonitoring dan dipelihara keamanan sistemnya yang ditinjau secara berkala.

10. Identifikasi risiko kebakaran

Dengan penyebab terjadinya korsleting listrik dan terbakarnya generator berdampak tidak dapat mengoperasionalkan server dan pc sehingga kegiatan operasional terhenti dan memunculkan waktu dan biaya tambahan untuk perbaikannya maka perlu dilakukan tindakan perlindungan keamanan pengkabelan dari kerusakan dan juga dilakukan monitoring yang ditinjau secara berkala. Selain itu untuk melindungi data yang ada pada server juga perlu dilakukan back-up.

11. Identifikasi risiko Pencurian media atau dokumen penting

Dengan penyebab pencurian hardware yang berdampak benefit loss dan kekurangan hardware untuk menjalankan proses bisnis maka perlu dilakukan tindakan pengamanan pada setiap ruangan yaitu misalnya harus dilindungi dengan control akses masuk yang memadai untuk memastikan hanya orang yang berhak saja diizinkan masuk sehingga cara tersebut dapat mencegah terjadinya pencurian.

12. Identifikasi risiko penyalahgunaan hak akses

Dengan penyebab semua karyawan memiliki hak akses yang sama dan adanya share login yang sering dilakukan antar karyawan maka perlu dilakukan pembatasan akses terhadap informasi dan aplikasi oleh pengguna dan personel pendukung sesuai dengan kebijakan pengendalian akses yang ditetapkan serta diperlukan adanya perjanjian dengan user bahwa password pribadi yang bersifat rahasia harus dijaga dan tidak boleh diberitahukan kepada orang lain untuk menghindari terjadinya risiko penyalahgunaan hak akses.

13. Pelanggaran terhadap aturan atau regulasi yang berlaku

Dengan penyebab kurangnya sosialisasi tentang regulasi dan sanksinya yang berdampak terjadinya penurunan etika kerja karyawan terhadap keamanan system dan mengakibatkan pekerjaan yang tidak efektif maka diperlukan adanya pelatihan kesadaran yang tepat dalam kebijakan keamanan organisasi bagi semua karyawan di organisasi.

## 4. SIMPULAN DAN SARAN

Berikut ini merupakan kesimpulan dan saran terkait dengan penelitian yang dilakukan.

### 4.1 Simpulan

Berdasarkan hasil penelitian, berikut ini merupakan beberapa kesimpulan yang dapat diambil :

1. Dari proses identifikai risiko terhadap layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung diperoleh 13 risko dan 31 kejadian risiko dengan demikian terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab.
2. Hasil penilaian dikategorikan dalam empat level penilaian risiko yaitu *very high, high, medium, low,* dan *very low*.
   a. Level *very high mempunyai* 4 risiko dengan nilai RPN sebesar 378.
   b. Level *high* mempunyai 2 risiko dengan nilai RPN antara 151-200.
   c. Level *medium* mempunyai 7 risiko dengan nilai RPN antara 101-150.
   d. Level *low* mempunyai 13 risiko dengan nilai RPN antara 51-100.
   e. Level *very low* mempunyai 5 risiko dengan nilai RPN antara 0-50.
3. Dari hasil identifikasi risiko terdapat 12 kontrol dalam ISO 27001 yang dapat dijadikan acuan penentuan rekomendasi mitigasi risiko.

### 4.2 Saran

Berdasarkan pelaksanaan penelitian penelitian ini, saran yang dapat diberikan agar bisa dijadikan rekomendasi untuk penelitian selanjutnya adalah menerapkan metode identify senior management knowledge. Karena keterbatasan akses peneliti melakukan pendekatan dengan menanyakan bagaimana senior management dipandang dukungannya terhadap keamanan informasi oleh pihak operasional dan staf. Maka untuk penelitian selanjutnya perlu dipertimbangkan untuk melakukan penggalian informasi terhadap senior management di organisasi.

## 5. DAFTAR RUJUKAN

[1] P. K. Tulungagung, *PERDA & Pembentukan Struktur Organisasi TUPOKSI*, Tulungagung, 2013.

[2] P. M. J, *The OCTAVE methodology as a risk analysis tool for business resources. roceedings of the International Multiconference on Computer Science and Information Technology*.

[3] "*What is security analys*?," [Online]. Available: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm. [Accessed 16 January 2016].

[4] "*PDCA Security*," [Online]. Available: http://www.pdca-security.com/.

[5] Z. Z, *Case Study As A Research Method*," J. Kemanus, Bil9, 2007.

[6] Widodo, "*Perencanaan dan implementasi SMKI*," Universitas Diponegoro, Semarang, 2008.

[7] K. K. d. I. RI, *Panduan Penerapan Tatakelola KIPPP, Jakarta*, 2011.

[8] Y. K. R, "Case Study Research Design and Methods Second Edition," *International Educational and Professional Publisher*, vol. 5.

[9] Paryati, "*Keamanan Informasi*," UPN Veteran, Yogjakarta, 2008.