# BAB IV

# HASIL DAN PEMBAHASAN

## 4.1 Skenario Risiko

Setiap perusahaan pasti memiliki berbagai macam risiko dan risikonya berbeda-beda. Sebelum dilakukannya skenario risiko terlebih dahulu melakukan penentuan kategori risiko, jenis ancaman serta peristiwa risiko bymatrans. Untuk kategori risiko berdasarkan COBIT 5 untuk risiko dapat dilihat pada Tabel 3.3. Pada tahap 3.3 Skenario risiko. Proses pengerjaan dalam menentukan kategori risiko telah disajikan pada Tabel 4.1. Selanjutnya dilakukan identifikasi terjadi risiko, dalam terjadi risiko berisi mengenai keterangan dan penyebab dari risiko terjadi pada Bymatrans. Berikut rincian dari terjadi risiko dapat disajikan pada Tabel 4.2.

Setelah melakukan penentuan terhadap tipe-tipe risiko pada Bymatrans. Berikut adalah penyajian dari tipe-tipe risiko Bymatrans dapat dilihat pada Tabel 4.3. Selanjutnya dilakukan skenario risiko. Berikut penyajian dari skenario risiko dapat dilihat pada Tabel 4.4.

Tabel 4.1 Kategori risiko

| No | Kategori risiko | Risiko | Jenis ancaman | Peristiwa |
|---|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* data kiriman | Kesalahan | Peraturan dan ketentuan |
| | | Kesalahan staf operasional dalam menggunakan PC | Kesalahan | Penggunaan tidak pas |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login staf | Kesalahan | Penggunaan tidak pas |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | Kejahatan | Pencurian |
| 4 | *Business ownership of IT* | Gangguan Tegangan listrik | Kebetulan | Gangguan |

Tabel 4.1 Kategori risiko (lanjutan)

| No | Kategori risiko | Risiko | Jenis ancaman | Peristiwa |
|---|---|---|---|---|
| 5 | *Malware* | PC ( Serangan virus, Mati sendiri) | Kebetulan | Gangguan |
| | | Laptop (Serangan virus, notresponding) | Kebetulan | Gangguan |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | Kebetulan | Gangguan |
| | | Mikrotik *switch* (tidak bisa terhubung*)* | Kebetulan | Gangguan |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | Kejahatan | Pencurian |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | Kebetulan | Gangguan |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | Kebetulan | Penghancuran |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | Kejahatan | Modifikasi |
| 11 | *Business ownership of IT* | Server mengalami gangguan | Kebetulan | Gangguan |

Tabel 4.2 Terjadi risiko

| No | Kategori risko | Risiko | Jenis ancaman | Peristiwa | Keterangan | Penyebab |
|---|---|---|---|---|---|---|
| 1 | Operasi staf | Kesalahan staf operasional dalam *input* data kiriman | Kesalahan | Gangguan | Data kiriman yang telah dimasukkan pada sistem tidak sesuai | Pengguna tidak teliti dalam *entry* pengiriman dikarenakan banyaknya kiriman atau tujuan kiriman tidak jelas |
| | | Kesalahan staf operasional dalam menggunakan PC | Kesalahan | Penggunaan tidak pas | Staf melakukan kesalahan dalam memahami prosedur pekerjaan | Staf bermain game pada PC pada saat bekerja |
| 2 | *IT expertise and skill* | Kesalahan staf teknologi informasi dalam memberikan password login staf | Kesalahan | Penggunaan tidak pas | IT *Support* melakukan kesalahan dalam memberikan akses login kepada staf perusahaan | Bagian TI memberikan *password* menggunakan tanggal lahir staf |

Tabel 4.2 Terjadi risiko (lanjutan)

| No | Kategori risko | Risiko | Jenis ancaman | Peristiwa | Keterangan | Penyebab |
|---|---|---|---|---|---|---|
| 3 | Informasi | Pengambilan data pelanggan perusahaan | Kejahatan | Pencurian | Pencurian data pelanggan dilakukan staf perusahaan yang mengakibatkan pengurangan biaya penghasilan perusahaan | Penyimpanan data pelanggan masih ada yang berupa kertas print |
| 4 | Business ownership of IT | Gangguan tegangan listrik | Kebetulan | Gangguan | Adanya lampu mati secara tiba-tiba | Adanya perbaikan secara berkala atau *problem* dari PLN |
| 5 | *Malware* | Serangan virus atau malware pada PC | Kebetulan | Gangguan | PC keadaan *notresponding* atau tidakbisa dipakai | 1. Banyaknya virus yang terdapat pada PC<br>2. Terdapat kendala didalam *hardware* ataupun *software*<br>3. Antivirus yang jarang terupdate |
| | | Serangan virus atau malware pada laptop | Kebetulan | Gangguan | Laptop tiba-tiba mati sendiri atau *notresponding* | 1. Terdapat banyak virus pada laptop<br>2. Laptop sudah menua<br>3. Belum ada antivirus yang kuat |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | Kebetulan | Gangguan | 1. Hasil print tidak jelas<br>2. Printer berhenti | 1. Catrige tidak berjalan<br>2. Tinta habis |
| | | Mikrotik *switch* (tidak bisa terhubung) | Kebetulan | Gangguan | Perangkat tidak dapat digunakan dikarenakana kabel terputus | Penataan kabel jaringan yang terhubung belum tertata dengan baik |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | Kejahatan | Pencurian | Aset monitor perusahaan hilang | Penampatan PC didalam ruang yang belum terkunci |

Tabel 4.2 Terjadi risiko (lanjutan)

| No | Kategori risko | Risiko | Jenis ancaman | Peristiwa | Keterangan | Penyebab |
|---|---|---|---|---|---|---|
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | Kebetulan | Gangguan | Sistem tidak berjalan sehingga layanan tidak berfungsi | 1. *Software* mengalami *crash* karena *software* terdapat virus ataupun malware<br>2. Aplikasi erorr tidak bisa diakses karena proses *troubleshooting* membutuhkan waktu lebih lama |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | Kebetulan | Penghancuran | Belum pernah terjadi | Belum pernah terjadi |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | Kejahatan | Modifikasi | Belum pernah terjadi | Belum pernah terjadi |
| 11 | *Business ownership of IT* | Server mengalami gangguan | Kebetulan | Gangguan | Belum pernah terjadi | Belum pernah terjadi |

Tabel 4.3 Tipe-tipe risiko

| No | Risiko | Tipe risiko | | |
|---|---|---|---|---|
| | | *IT benefit/value enblement risk* | *IT program me and project delivery risk* | *IT operations and service delivery risk* |
| 1 | Kesalahan staf operasional dalam *input* data kiriman | S | S | P |
| 2 | Kesalahan staf operasional dalam menggunakan PC | S | S | P |
| 3 | Kesalahan staf TI dalam memberikan password login staf | S | S | P |
| 4 | Pengambilan data pelanggan perusahaan | S | S | P |
| 5 | Gangguan Tegangan listrik | S | S | P |
| 6 | Serangan virus atau malware pada PC | S | S | P |

Tabel 4.3 Tipe-tipe risiko (lanjutan)

| No | Risiko | Tipe risiko | | |
|---|---|---|---|---|
| | | *IT benefit/value enblement risk* | *IT program me and project delivery risk* | *IT operations and service delivery risk* |
| 7 | Serangan virus atau malware pada laptop | S | S | P |
| 8 | Printer (Tinta habis, Catrige bermasalah) | S | S | P |
| 9 | Mikrotik *switch* (tidak bisa terhubung) | S | S | P |
| 10 | Pencurian aset monitor perusahaan | S | S | P |
| 11 | Sistem informasi Bymatrans tidak berjalan | S | S | P |
| 12 | Bencana alam (Tsunami, gempa bumi) dll | S | S | P |
| 13 | Pemanfaatan celah keamanan sistem informasi Bymatrans oleh pihak luar | S | S | P |
| 14 | Server mengalami gangguan | S | S | P |

Berdaskaran perincian Tabel 4.1, dapat diketahui empat belas risiko yang bertipe *IT Operations and Service Delivery risk*, dikarenakan proses bisnis terkait dengan Terkait dengan stabilitas operasional, ketersediaan, perlindungan, dan pemulihan layanan TI, yang dapat membawa penghancuran atau pengurangan nilai bagi perusahaan, sehingga kedua tipe diisi dengan 'S' (Sekunder).

Tabel 4.4 Skenario risiko

| No | Kategori risiko | Risiko | Tipe Risiko | | | Skenario risiko | |
|---|---|---|---|---|---|---|---|
| | | | T1 | T2 | T3 | Positif skenario | Negatif risiko |
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* data kiriman | S | S | P | Pengguna mengisi data kiriman dengan benar dan sesuai sehingga akibatnya tidak lambat *update* status pengiriman | Pengguna dalam mengisi data kiriman tidak sesuai sehingga terjadi lambat *update* status pengiriman |
| | | Kesalahan staf operasional dalam menggunakan PC | S | S | P | Perusahaan tidak mengalami kerugian dikarenakan cuma bermain game pada PC | Kerugian perusahaan disebabkan penyalahgunaan PC karena pengambilan perangkat keras atau informasi perusahaan |

Tabel 4.4 Skenario risiko (lanjutan)

| No | Kategori risiko | Risiko | Tipe Risiko | | | Skenario risiko | |
|---|---|---|---|---|---|---|---|
| | | | T1 | T2 | T3 | Positif skenario | Negatif risiko |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login staf | S | S | P | Perusahaan tidak mengalami kerugian baik finansial dikarenakan cuma pemberian password yang kuat | Kerugian perusahaan terhadap pemenuhan password login yang kuat |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | S | S | P | Penggunaan data pelanggan penting dikarenakan menghasilkan keutungan bagi perusahaan | Penggunaan data pelanggan yang salah mengakibatkan perugian terhadap perusahaan |
| 4 | *Business ownership of IT* | Gangguan Tegangan listrik | S | S | P | Listrik merupakan hal penting karena membantu perusahaan dalam memberikan layanan | Listrik tidak menyala atau mengalami gangguan mengakibatkan proses playanan perusahaan berhenti |
| 5 | *Malware* | Serangan virus atau malware pada PC | S | S | P | Pengujian yang sesuai dilakukan sebelum menetapkan PC kedalam perusahaan untuk memastikan kesiapan PC tersebut | PC yang tidak sesuai kesiapan menganggu layanan yang diberikan |
| | | Serangan virus atau malware pada laptop | S | S | P | Penggunaan pada laptop memberikan peran penting dalam proses bisnis perusahaan | Laptop berhenti dengan sendirinya yang dapat mengganggu proses pelayanan perusahaan |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | S | S | P | Pengguna dapat mengandalakan printer terkait kebutuhan laporan atau bukti kiriman | Printer yang bermasalah dapat mengganggu pengguna dalam proses pelayanan |
| | | Mikrotik *switch* (tidak bisa terhubung*)* | S | S | P | Mikrotik yang tidak bermasalah dapat membantu pengguna dalam memberikan layanan | Mikrotik tidak terhubung dikarenakan penataan kabel yang kurang handal mengakibtkan putus atau lepas |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | S | S | P | Monitor yang selalu terjaga keamanannya dan hanyak pihak yang berwenang dapat mengaksesnya | Monitor yang diketahui dapat disalahgunakan atau bahkan hilang oleh pihak yang tidak berwenang |

Tabel 4.4 Skenario risiko (lanjutan)

| No | Risiko | Kategori risiko | Tipe Risiko | | | Skenario risiko | |
|---|---|---|---|---|---|---|---|
| | | | T1 | T2 | T3 | Positif skenario | Negatif risiko |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | S | S | P | Pengguna dapat mengandalkan sistem ini dalam menjalankan proses bisnis dan permintaan layanan. | Tidak jalannya sebuah sistem menganggu pelayanan perusahaan |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | S | S | P | | Bencana alam yang dapat merugikan perusahaan |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | S | S | P | Perusahaan tidak mengalami kerugian baik finansial dikarenakan cuma layanan sesuai dengan prosedur serta data (aset kritis) | Perusahaan merugi terhadap pihak luar dikarenakan kehilangan data maupun kerugian finansial |
| 11 | *Business ownership of IT* | Server mengalami gangguan | S | S | P | Server yang lancar dan tidak mengalami masalah dapat memberikan layanan yang baik | Server mengalami masalah dapat mengganggu layanan perusahaan |

Sumber : Dioalah dari hasil penelitian

## 4.2 Analisis risiko

Selanjutnya pada tahap analisis risiko berisi mengenai hasil penilaian risiko, didalam analisis risiko berisi mengenai penentuan rentang kejadian suatu risiko Bymatrans serta hasil penentuan nilai dampak dan nilai rata-rata dampak dan gambaran dari peta risiko. Sebagai berikut pembahasannya :

1. Penentuan nilai frekuensi dapat dilihat pada Tabel 2.3. Kemudian menentukan risiko berapa kali kejadian dalam setahun dan menghasilkan Tabel 4.5 pada halaman selanjutnya.

Tabel 4.5 Hasil nilai frekuensi

| No | Kategori risiko | Risiko | Rentang kejadian | Frekuensi *value* |
|---|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* data kiriman | 15-20x | 4 |
| | | Kesalahan staf operasional dalam menggunakan PC | Pernah terjadi 1x | 1 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login staf | Pernah terjadi 1x | 1 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | Pernah terjadi 1x | 1 |
| 4 | *Business ownership of IT* | Gangguan Tegangan listrik | 1x | 1 |
| 5 | *Malware* | Serangan virus atau malware pada PC | 2x | 2 |
| | | Serangan virus atau malware pada laptop | 1x | 1 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 2x | 2 |
| | | Mikrotik *switch* (tidak bisa terhubung) | 1x | 1 |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 1x | 1 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 1x | 2 |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | - | 1 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | - | 1 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | - | 1 |

2. Menentukan nilai dampak produktivitas dapat dilihat pada Tabel 2.4. Kemudian menghasilkan nilai dampak produktivitas dilihat pada Tabel 4.6. Diperoleh dari kuisoner pada lampiran lima.

Tabel 4.6 Hasil nilai dampak produktivitas

| No | Kategori risiko | Risiko | Produktivitas |
|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 1 |
| | | Kesalahan staf operasional dalam menggunakan PC | 1 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 5 |

Tabel 4.6 Hasil nilai dampak produktivitas (lanjutan)

| No | Kategori risiko | Risiko | Produktivitas |
|---|---|---|---|
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 5 |
| 5 | *Malware* | Serangan virus atau malware pada PC | 2 |
| | | Serangan virus atau malware pada laptop | 1 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 1 |
| | | Mikrotik *switch*(tidak bisa terhubung*)* | 1 |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 2 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 5 |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | 5 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | 1 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 1 |

3. Dalam menentukan dampak biaya tanggapan pada Bymatrans dapat dilihat pada Tabel 2.5. Kemudian telah disajikan mengenai nilai dampak biaya tanggapan dapat dilihat pada Tabel 4.7. Diperoleh dari kuisoner pada lampiran enam.

Tabel 4.7 Hasil nilai dampak biaya tanggapan

| No | Kategori risiko | Risiko | Biaya tanggapan |
|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 1 |
| | | Kesalahan staf operasional dalam menggunakan PC | 1 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 5 |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 5 |
| 5 | *Malware* | Serangan virus atau malware pada PC | 1 |
| | | Serangan virus atau malware pada laptop | 1 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 2 |
| | | Mikrotik *switch*(tidak bisa terhubung*)* | 1 |
| 7 | *Pencurian infrastruktur atau pengrusakan* | Pencurian aset monitor perusahaan | 2 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 2 |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | 5 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | 1 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 1 |

4. Pada lampiran tujuh, menunjukkan contoh form kuisoner yang telah disebarkan kepada pengguna interal perusahaan, kemudian hasil kusioner keunggulan kompetitif menjadi seperti Tabel 4.8, maka selanjutnya mengolah dari setiap penilaian yang diberikan responden, dalam mengolah penilaian responden akan menggunakan nilai mean. Berikut penyajian nilai mean dapat dilihat pada Tabel 4.9. Kemudian acuan terhadap penentuan nilai keunggulan kompetitif dapat dilihat pada Tabel 2.6, selanjutnya menentukan nilai hasil pengolahan kuisoner yang menghasilkan mean dibulatkan menjadi genap telah disajikan, berikut penyajian pada Tabel 4.10.

Tabel 4.8 Hasil kuisoner responden

| R1 | R2 | R3 | R4 | R5 | R6 | R7 | R8 | R9 | R10 | R11 | R12 | R13 | R14 | R15 | R16 | R17 | R18 | R19 | R20 | R21 | R22 | R23 | R24 | R25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 4 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 3 | 4 | 4 | 5 | 4 | 3 | 5 | 4 | 4 | 5 | 4 | 4 | 4 |
| 3 | 2 | 3 | 3 | 4 | 5 | 4 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 4 | 4 | 5 | 3 | 5 | 4 | 5 | 4 | 3 | 4 | 3 |
| 4 | 3 | 3 | 3 | 4 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 2 | 4 | 2 | 4 | 2 | 5 | 2 | 2 | 4 | 3 | 4 | 3 | 3 |
| 4 | 2 | 2 | 3 | 2 | 4 | 3 | 3 | 3 | 2 | 4 | 2 | 2 | 4 | 5 | 2 | 3 | 4 | 2 | 1 | 2 | 3 | 1 | 2 | 5 |
| 2 | 5 | 2 | 4 | 2 | 3 | 1 | 3 | 2 | 2 | 4 | 2 | 3 | 2 | 3 | 1 | 5 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 5 |
| 4 | 4 | 4 | 2 | 2 | 2 | 5 | 5 | 4 | 2 | 3 | 3 | 4 | 3 | 2 | 4 | 4 | 5 | 2 | 2 | 2 | 2 | 2 | 3 | 3 |
| 4 | 3 | 2 | 5 | 2 | 4 | 5 | 4 | 4 | 3 | 5 | 4 | 3 | 1 | 2 | 4 | 3 | 3 | 4 | 3 | 5 | 3 | 5 | 4 | 5 |
| 3 | 3 | 3 | 3 | 2 | 3 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 3 | 4 | 3 | 2 | 4 | 3 | 2 | 2 | 3 | 4 | 3 | 2 |
| 1 | 2 | 2 | 1 | 3 | 3 | 2 | 2 | 1 | 3 | 3 | 2 | 1 | 3 | 2 | 2 | 1 | 1 | 1 | 3 | 3 | 2 | 3 | 2 | 2 |
| 5 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 3 | 4 | 3 | 4 | 3 | 4 | 5 | 3 | 4 | 3 | 4 | 4 | 4 | 3 | 3 |
| 1 | 2 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 3 | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 4 | 3 | 1 | 3 | 2 |
| 1 | 2 | 3 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 5 | 1 | 2 | 2 | 1 |
| 1 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 |
| 3 | 3 | 3 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 2 | 4 | 3 | 2 | 3 | 2 | 3 | 3 | 2 |

Tabel 4.9 Hasil pengolahan kuisoner responden

| No | Risiko | Total responden | Hasil Mean responden |
|---|---|---|---|
| 1 | Ketika Sistem informasi Bymatrans tidak berjalan tidak berjalan | 25 orang | 4.24 |
| 2 | Serangan virus/malware pada pc | 25 orang | 3.64 |
| 3 | Serangan virus/malware pada laptop | 25 orang | 3.04 |
| 4 | Gangguan listrik tegangan listrik | 25 orang | 2.8 |
| 5 | Ketika Sistem informasi Bymatrans tidak berjalan diretas oleh pihak luar atau dalam | 25 orang | 3.12 |
| 6 | Ketika server mengalami gangguan pada saat bekerja | 25 orang | 3.12 |
| 7 | Apabila bencana alam terjadi tiba-tiba | 25 orang | 3.6 |
| 8 | Ketika mikrotik *switch* tidak berjalan tiba-tiba | 25 orang | 2.72 |
| 9 | Ketika monitor hilang | 25 orang | 2.04 |
| 10 | Jika tujuan paket pengiriman tidak jelas (efek lambat udpate status pengiriman) | 25 orang | 3.96 |
| 11 | Jika password login staf lemah | 25 orang | 1.88 |
| 12 | Ketika data pelanggan hilang karena staf | 25 orang | 1.64 |
| 13 | Jika saya salah dalam pengoperasikan pc pada saat bekerja | 25 orang | 1.28 |
| 14 | Ketika Printer tidak berjalan karena tinta habis, catrige bermasalah | 25 orang | 2.72 |

Tabel 4.10 Hasil Nilai risiko dampak keunggulan kompetitif

| No | Kategori risiko | Risiko | Keunggulan kompetitif |
|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 3,96 |
| | | Kesalahan staf operasional dalam menggunakan PC | 1,28 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1,8 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 1,64 |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 3,56 |
| 5 | *Malware* | Serangan virus atau malware pada PC | 3,16 |
| | | Serangan virus atau malware pada laptop | 3,04 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 2,72 |
| | | Mikrotik *switch*(tidak bisa terhubung) | 2,72 |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 2,04 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 4,24 |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | 1,44 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | 3,08 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 2,64 |

5. Dalam penentuan nilai dampak hukum dapat dilihat perincian pada Tabel 2.7. Dalam penyajian dampak hukum pada Bymatrans dapat diketahui pada Tabel 4.11. Diperoleh dari kuisoner pada lampiran delapan.

Tabel 4.11 Hasil nilai dampak hukum

| No | Kategori risiko | Risiko | Hukum |
|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 1 |
| | | Kesalahan staf operasional dalam menggunakan PC | 1 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 1 |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 1 |
| 5 | *Malware* | Serangan virus atau malware pada PC | 1 |
| | | Serangan virus atau malware pada laptop | 1 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 1 |
| | | Mikrotik *switch*(tidak bisa terhubung) | 1 |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 1 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 1 |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | 1 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | 1 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 1 |

Setelah melakukan penentuan nilai frekuensi *value* dan nilai dampak *value*. Selanjutnya perhitungan untuk mengetahui nilai rata-rata dampak, karena dalam risk maps memerlukan suatu nilai rata-rata dampak risiko dan frekuensi *value*, cara menghitung nilai rata-rata dampak ialah menjumlahkan seluruh dampak dimulai dari kerugian penghasilan selama satu tahun, biaya terkait mengelola kerugian, peringkat keuapasan pelanggan, kepatuhan terhadap peraturan dana dan hasil perhitungan dari dampak tersebut dibagi empat sesuai jumlah aspek dampak risiko,

berikut adalah hasil nilai rata-rata dampak dapat dilihat pada Tabel 4.12. Setelah hasil rata-rata dampak telah ditemukan, maka proses setelahnya memasukkan data rata-rata dampak dan frekuensi kedalam *Microsoft excel* untuk memunculkan *risk maps*, data tersebut dapat diketahui pada Tabel 4.13. *Risk maps* menampilkan dua nilai, yaitu nilai dampak risiko sebagai sumbu (Y) sedangkan nilai frekuensi *value* sebagai sumbu (X). Untuk warna-warni pada *risk maps* menunjukkan tingkatan risiko penjelasannya, yaitu warna biru hingga hijau menunjukkan *very low* hingga *low*, dan untuk warna kuning menunjukkan medium sedangkan warna merah menunjukkan *high* sampai *very high*. Pada titik hitam mengetahui letak tingkatan risiko Bymatrans, berikut penggambaran risk maps dapat dilihat pada Gambar 4.1.

Tabel 4.12 Hasil perhitungan rata-rata nilai dampak

| No | Kategori risiko | Risiko | Hasil perhitungan dampak | | | | |
|---|---|---|---|---|---|---|---|
| | | | Produktivitas | Biaya tanggapan | Keunggulan kompetitif | Hukum | Hasil perhitungan |
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 1 | 1 | 4 | 1 | 1+1+4+1 =7:4= 1,75 |
| | | Kesalahan staf operasional dalam menggunakan PC | 1 | 1 | 1 | 1 | 1+1+1+1 =4:4= 1 |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1 | 1 | 2 | 1 | 1+1+2+1 =5:4= 1,25 |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 5 | 5 | 2 | 1 | 5+5+2+1 = 13:4= 2,75 |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 5 | 5 | 4 | 1 | 5+5+4+1=15 :4 =3,75 |

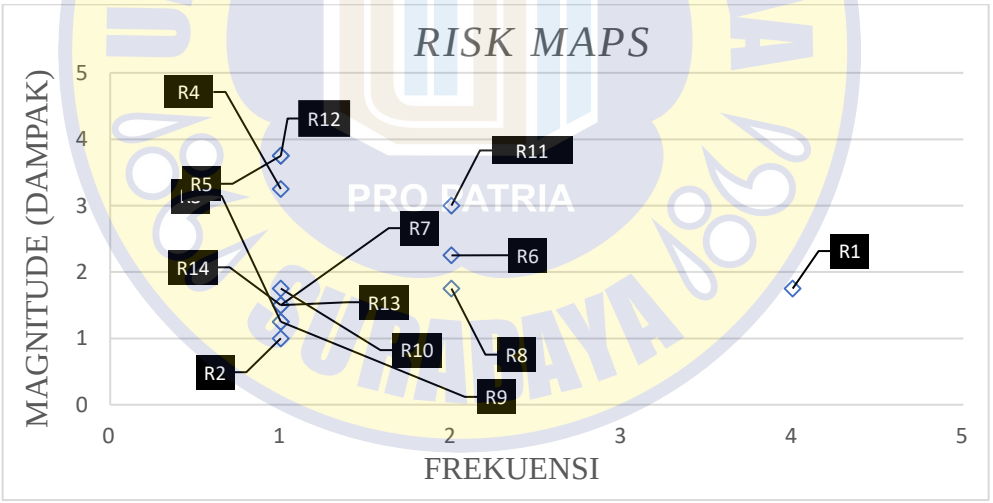
Tabel 4.12 Hasil perhitungan rata-rata nilai dampak (lanjutan)

| No | Kategori risiko | Risiko | Hasil perhitungan | | | | |
|---|---|---|---|---|---|---|---|
| | | | Produktivitas | Biaya tanggapan | Keunggulan kompetitif | Hukum | Hasil perhitungan |
| 5 | *Malware* | Serangan virus atau malware pada PC | 3 | 1 | 4 | 1 | 2+1+3+1 = 8:4= 2 |
| | | Serangan virus atau malware pada laptop | 1 | 1 | 3 | 1 | 1+1+3+1 =6:4= 1,5 |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 1 | 2 | 3 | 1 | 1+2+3+1=7:4= 1,75 |
| | | Mikrotik *switch*(tidak bisa terhubung*)* | 1 | 1 | 3 | 1 | 1+1+3+1=5:4= 1,25 |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 2 | 2 | 2 | 1 | 2+2+2+1 =7:4= 1,75 |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 5 | 2 | 4 | 1 | 4+3+4+1 =12:4=3 |
| 9 | *Acts of nature* | Bencana alam | 5 | 5 | 4 | 1 | 5+5+4+1=15:4 =3,75 |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans | 1 | 1 | 3 | 1 | 1+1+3+1= 6:4 = 1,5 |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 1 | 1 | 3 | 1 | 1+1+3+1= 6:4 = 1,5 |

Sumber : Dioalah dari hasil penelitian

Tabel 4.13 Data yang digunakan dalam risk maps

| Risiko | Kode risiko | Nilai Dampak | Nilai frekuensi |
|---|---|---|---|
| Kesalahan staf operasional dalam *input* kiriman | R1 | 1,75 | 4 |
| Kesalahan staf operasional dalam menggunakan PC | R2 | 1 | 1 |
| Kesalahan staf TI dalam memberikan password login | R3 | 1,25 | 1 |
| Pengambilan data pelanggan perusahaan | R4 | 2,75 | 1 |
| Gangguan tegangan listrik | R5 | 3,75 | 1 |
| Serangan virus atau malware pada PC | R6 | 2 | 2 |
| Serangan virus atau malware pada laptop | R7 | 1,5 | 1 |
| Printer (Tinta habis, Catrige bermasalah) | R8 | 1,75 | 2 |
| Mikrotik *switch*(tidak bisa terhubung) | R9 | 1,25 | 1 |
| Pencurian aset monitor perusahaan | R10 | 1,75 | 1 |
| Sistem informasi Bymatrans tidak berjalan | R11 | 3 | 2 |
| Bencana alam (Tsunami, gempa bumi) | R12 | 3,75 | 1 |
| Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | R13 | 1,5 | 1 |
| Server mengalami gangguan | R14 | 1,5 | 1 |




Gambar 4.1 *Risk maps*

## 4.3 Selera risiko

Dalam tahap ini penentuan risiko pada Bymatrans Surabaya, berdasarkan empat opsi respon risiko dan paramater respon risiko. Berikut perincian dari empat ospin respon risiko yang perlu diketetahui pada halaman selanjutnya.

1. Opsi respon risiko

Jadi Setiap perusahaan memiliki berbagai macam risiko. Risiko yang ada dalam perusahaan bersedia diterima, dihindari bahkan ada yang ditransfer serta risiko yang perlu dimitigasi, pada risiko Bymatrans Surabaya memiliki berbagai macam risiko yang bersedia diterima, dibagi dan dihindari oleh Bymatrans. Pada tahap ini dilakukan opsi respon risiko dan paramater respon risiko. Berikut adalah ringkasan data respon risiko yang diperoleh dari kuisoner yang diisi oleh direktur Bymatrans Surabaya, sebagai berikut empat respon risiko pada halaman selanjutnya.

a. *Accept*

Respon terhadap penerimaan risiko pada penelitian ini didapat dari hasil kuisoner yang diisi oleh pemilik Bymatrans Surabaya. Dengan menentukan selera risiko yang diinginkan Bymatrans Surabaya, berikut adalah kriteria penerimaan risiko dalam Bymatrans Surabaya dapat diketahui pada Tabel 4.14.

b. *Transfer*

Sedangkan untuk tahap transfer atau membagi suatu risiko perusahaan yang ada, Risiko yang ada dipilih oleh Bymatrans Surabaya untuk dibagikan kepada pihak lain dikarenakan dalam perusahaan tidak bisa menyelesaikan risiko tersebut dikarenakan tidak adanya programmer serta biaya yang dikeluarkan pada saat menangani risiko yang ada tidak terlalu banyak. Berikut risiko yang ada dalam perusahaan dibagi kepada pihak lain dapat dilihat pada tabel 4.14.

c. *Avoid*

Opsi respon mengenai penghindaran risiko yang ada dalam Bymatrans dikarenakan Bymatrans tidak ada cara untuk mengatasi risiko tersebut meskipun dengan cara membagi risiko ini. Berikut adalah risiko yang dihindari oleh Bymatrans surabaya dapat dilihat pada tabel 4.14.

d. *Mitigate*

Setelah dilakukan pemetaan risiko yang perlu dihindari, ditransfer, diterima lalu risiko yang perlu untuk dimitigasi. Dikarenakan setiap risiko memerlukan mitigasi, didalam mitigasi terdapat tindakan kejadian untuk risiko yang ada pada Bymatrans Surabaya. Berikut adalah mitigasi terhadap risiko-risiko Bymatrans Surabaya dapat dijelaskan pada tabel 4.14.

Tabel 4.14 Selera respon risiko

| No | Kategori risiko | Risiko | Repon risiko |
|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | *Mitigate* |
| | | Kesalahan staf operasional dalam menggunakan PC | *Mitigate* |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | *Mitigate* |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | *Mitigate* |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | *Mitigate* |
| 5 | *Malware* | Serangan virus atau malware pada PC | *Avoid* |
| | | Serangan virus atau malware pada laptop | *Mitigate* |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | *Mitigate* |
| | | Mikrotik *switch*(tidak bisa terhubung) | *Mitigate* |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | *Mitigate* |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | *Mitigate* |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | *Transfer* |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | *Avoid* |
| 11 | *Business ownership of IT* | Server mengalami gangguan | *Mitigate* |

## 4.4 Pemilihan prioritas risiko

Pada tahap ini penentuan tingkatan risiko yang ada pada Bymatrans, penentuannya tingkatan ditentukan berdasarkan *risk maps*. Hasil dari tahapan ini akan memuculkan frekuensi risiko, rata-rata dampak *value* yang diperoleh pada *risk maps*. Pada perusahaan serta tingkatan risiko. Berikut adalah perincian dari tahap ini dapat dilihat pada tabel 4.15.

Tabel 4.15 Penentuan prioritas risiko

| No | Kategori risiko | Risiko | Frekuensi | Rata-rata dampak | Tingkatan risiko |
|---|---|---|---|---|---|
| 1 | *Staff operation* | Kesalahan staf operasional dalam *input* kiriman | 4 | 1,75 | *High* |
| | | Kesalahan staf operasional dalam menggunakan PC | 1 | 1 | *Low* |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | 1 | 1,25 | *Low* |
| 3 | *Information* | Pengambilan data pelanggan perusahaan | 1 | 3,25 | *Medium* |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | 1 | 3,75 | *High* |
| 5 | *Malware* | Serangan virus atau malware pada PC | 2 | 2,25 | *Medium* |
| | | Serangan virus atau malware pada laptop | 1 | 1,5 | *Medium* |
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 2 | 1,75 | *Medium* |
| | | Mikrotik *switch*(tidak bisa terhubung) | 1 | 1,25 | *Low* |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor perusahaan | 1 | 1,75 | *Low* |
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 2 | 3 | *High* |
| 9 | *Acts of nature* | Bencana alam (Tsunami, gempa bumi) dll | 1 | 3,75 | *High* |
| 10 | *Logical attack* | Pemanfaatan celah keamanan sistem informasi bimatrans oleh pihak luar | 1 | 1,5 | *Low* |
| 11 | *Business ownership of IT* | Server mengalami gangguan | 1 | 1,5 | *Low* |

## 4.5 Rencana tindakan risiko

Pada tahap ini, yang pertama ialah penentuan proses COBIT 5, kemudian melakukan sebuah langkah mitigasi terhadap respon risiko berdasarkan pemetaaan COBIT 5 kemudian diambil berapa aktivitasnya, Berikut disajikan pada Tabel 4.16. kemudian penentuan pemetaan risiko kedalam langkah mitigasi dengan proses pemetaan COBIT 5 dapat dilihat pada Tabel 4.17.

Tabel 4.16 Proses pemetaan COBIT 5

| No | Kategori risiko | Proses COBIT 5 | Definisi dengan proses TI COBIT 5 |
|---|---|---|---|
| 1 | *Staff operation* | DSS01 | Proses bagaiman cara memilihara dan melakukan prosedur operasional dan tugas operasional dengan handal dan konsisten |
| 2 | *IT expertise and skill* | APO07 | Proses melakukan evaluasi kinjera individu tepat waktu secara teratur terhadap tujuan perusahaan, standar yang ditetapkan, tanggung jawab pekerjaan tertentu dan keterampilan dari staf |
| 3 | *Infrastructure* | DSS05 | Proses cara mempelihara dan melakukan langkah-langkah perbaikan terutama yang terbaru *patch* keamanan kontrol virus di perusahaan untuk melindungi sistem dan teknologi informasi dari malware (misal, virus, worm, spyware, spam). |
| 4 | *Malware* | DSS01 | Proses tentang mengkoordinasi dan melaksanakan kegiatan dan prosedur operasional yang diperlukan untuk memberikan layanan TI internal, termasuk pelaksanaan prosedur operasi standar yang telah ditentukan dan kegiatan pemantauan yang diperlukan serta memberikan hasil layanan operasional TI sesuai rencana. |
| 5 | *Infrastructure theft or destruction* | | |
| 6 | *Logical attack* | APO13 | Proses ini ialah menetapkan, operasikan dan pantau sistem untuk keamanan informasi, dan menjaga agar dampak dan kejadian insiden keaman informasi tetap berada dalam tingkat selera risiko perusahaan |
| 7 | *Business ownership of IT* | AP001 | Proses membahas tentang klarifikasi dan memeilihara misi dan visi TI perusahaan. Menerapkan dan memelihara otoritas untuk mengelola informasi dan pengguna TI di perusahaan |

Sumber : Diolah dari hasil penelitian

Tabel 4.17 Langkah mitigasi sesuai proses pemetaan COBIT 5

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi |
|---|---|---|---|---|---|---|---|
| 1 | Staff operation | Kesalahan staf operasional dalam *input* kiriman | Pengguna tidak teliti dalam *entry* pengiriman dikarenakan banyaknya kiriman atau tujuan kiriman tidak jelas | *Mitigate* | *High* | DSS01.01 *Perform operational procedures* | Memilihara dan melakukan prosedur operasional dan tugas operasional dengan handal dan konsisten.<br>Aktivitas :<br>1. Diharapkan semua data yang telah diproses sepenuhnya, akurat, dan tepat waktu. Memberikan *output* sesuai dengan layanan perusahaan.<br>2. Memantau kerjaan tiap staf secara berkala |
| | | Kesalahan staf operasional dalam menggunakan PC | Staf bermain game pada PC pada saat bekerja | | *Low* | | |
| 2 | *IT expertise and skill* | Kesalahan staf TI dalam memberikan password login | Bagian TI memberikan *password* menggunakan tanggal lahir staf | *Mitigate* | *Low* | APO07.04 *Evaluate employee job performance* | Melakukan evaluasi kinjera individu tepat waktu secara teratur terhadap tujuan perusahaan, standar yang ditetapkan, tanggung jawab pekerjaan tertentu dan keterampilan dari staf. Aktivitas :<br>1. Melakukan pengawasan dan pemantauan berkala terkait kinerja operasional<br>2. Memberikan intruksi spesifik untuk staf TI secara menyeluruh dan rutin |
| 3 | *Infrastructure theft or destruction* | Pengambilan data pelanggan perusahaan | Penyimpanan data pelanggan masih ada yang berupa kertas print | *Mitigate* | *Medium* | DSS01.04 *Manage the environment* | Mempertahankan langkah-langkah demi perlindungan aset terhadap lingkungan dengan cara memasang peralatan atau dengan perangkat khusus.<br>Aktivitas :<br>Melakukan pelatihan terhadap staf terkait keamanan berupa fisik atau non-fisik secara berkala |

Tabel 4.17 Langkah mitigasi sesuai proses pemetaan COBIT 5 (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi |
|---|---|---|---|---|---|---|---|
| 4 | *Malware* | Serangan virus atau malware pada laptop | 1. Terdapat banyak virus pada laptop<br>2. Laptop sudah menua | *Mitigate* | *Low* | DSS05.01 *Protect against malware* | Mempelihara dan melakukan langkah-langkah perbaikan terutama yang terbaru *patch* keamanan kontrol virus di perusahaan untuk melindungi sistem dan teknologi informasi dari malware (misal, virus, worm, spyware, spam).<br>Aktivitas :<br>1. Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru<br>2. instal dan aktifkan antivirus untuk PC dan laptop pada fasilitas pemrosesan. |
| | | Serangan virus atau malware pada PC | 1. Adanya debu karena jarang dipakai<br>2. Banyaknya virus yang terdapat pada PC<br>3. Terdapat kendala didalam *hardware* ataupun *software* | | *Medium* | | |
| 5 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 1. Catrige tidak berjalan<br>2. Tinta habis | *Mitigate* | *Medium* | DSS05.05 *Manage physical access to IT assets.* | Menetapkan dan terapkan prosedur untuk membatasi staf dalam mengakses serta mencatat atau memantau keadaan infrastruktur perusahaan. Aktivitas : Melakukan pelatihan terhadap staf terkait keamanan fisik secara berkala |
| | | Mikrotik *switch*(tidak bisa terhubung) | Penataan kabel jaringan yang terhubung belum tertata dengan baik | | *Low* | | |
| 6 | *Infrastructure theft or destruction* | Pencurian monitor | Penampatan PC didalam ruang yang belum terkunci | *Mitigate* | *Low* | DSS01.04 *Manage the environment* | Pertahankan langkah-langkah dalam melindungi perangkat terhadap lingkungan dengan cara pemantauan khusus terhadap lingkungan. Aktivitas : Mengharuskan pengunjung atau staf yang tidak memakai identifikasi untuk di waspadai oleh petugas keamanan |

Tabel 4.17 Langkah mitigasi sesuai proses pemetaan COBIT 5 (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi |
|---|---|---|---|---|---|---|---|
| 7 | *Logical attack* | Pemanfaatan celah keamanan oleh pihak luar | Belum pernah terjadi | *Mitigate* | *Low* | APO13.01 *Establish and maintain an information security management system (ISMS)* | Menetapkan dan memelihara ISMS yang menyediakan pendekatan standar untuk keamanan informasi bisnis. Aktivitas : Menetapkan dan komunikasikan peran dan tanggung jawab kepada keamanan informasi |
| 8 | *Business ownership of IT* | Server mengalami gangguan | Belum pernah terjadi | *Mitigate* | *Low* | *APO01.04 Communicate management objectives and direction.* | Komunikasikan kesadaran dan pemahaman tentang tujuan dan arah TI kepada pihak ketiga terkait kepentingan perusahaan. Aktivitas : Identifikasi pihak ketiga mengenai kepentingan utama dan persyaratan mereka |

Sumber : Diolah dari hasil penelitian

Tabel 4.18 Rekomendasi

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 1 | *Staff operation* | salah *input* data | Pengguna tidak teliti dalam *entry* pengiriman dikarenakan banyaknya kiriman atau tujuan kiriman tidak jelas | *Mitigate* | *High* | DSS01.01 *Perform operational procedures* | Memilihara dan melakukan prosedur operasional dan tugas operasional dengan handal dan konsisten. Aktivitas :<br>1. Diharapkan semua data yang telah diproses sepenuhnya, akurat, dan tepat waktu. Memberikan *output* sesuai dengan layanan perusahaan.<br>2. Memantau kerjaan tiap staf secara berkal | 1. Meningkatkan kompetensi setiap staf dengan mengadakan pelatihan atau training.<br>2. Menyediakan aplikasi tanda terima pada bag.pengiriman<br>3. Mengadakan monitoring dan evaluasi terhadap kinerja evaluasi staf<br>4. Menyediakan Scan barcode itu input data |
| | | Penyalahgunaan pada PC | Staf bermain game pada PC pada saat bekerja | *Mitigate* | *Low* | | | 1. Memperbaiki pola rekruitmen dan pelatihan SDM.<br>2. Mengadakan monitoring dan evaluasi terhadap kinerja evaluasi staf<br>3. Pemberitahuan notifikasi jika terjadi penyalahgunaan PC |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 2 | *IT expertise and skill* | Memberikan password login lemah | Bagian TI memberikan *password* menggunakan tanggal lahir staf | *Mitigate* | *Low* | APO07.04 *Evaluate employee job performance* | Melakukan evaluasi kinjera individu tepat waktu secara teratur terhadap tujuan perusahaan, standar yang ditetapkan, tanggung jawab pekerjaan tertentu dan keterampilan dari staf.<br>Aktivitas :<br>1. Melakukan pengawasan dan pemantauan berkala terkait kinerja operasional<br>2. Memberikan intruksi spesifik untuk staf TI secara menyeluruh dan rutin | 1. Meningkatka kompetensi staf TI dengan menambah itensitas dalam mengadakan pelatihan atau training terkait dengan kemanan informasi Meningkatkan<br>2. Memperbaiki pola rekruitmen dan pelatihan SDM.<br>3. Mengasah kemampuan setiap staf TI dengan membeirkan penugasan atua pekerjaan yang berbeda-beda agar staf TI mampu menguasai segala bidang kompetensi yang berhubungan dengan TI. |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 3 | *Infrastructure theft or destruction* | Pencurian data pelanggan | Penyimpanan data pelanggan masih ada yang berupa kertas print | *Mitigate* | *Medium* | DSS01.04 *Manage the environment* | Mempertahankan langkah-langkah demi perlindungan aset terhadap lingkungan dengan cara memasang peralatan atau dengan perangkat khusus. Aktivitas : Melakukan pelatihan terhadap staf terkait kesadaran keamanan berupa fisik atau non-fisik secara berkala | Penyimpanan data secara online, yaitu pada *cloud* (seperti google drive, dropbox, skydrive, dll) |
| 4 | *Business ownership of IT* | Gangguan tegangan listrik | Adanya perbaikan secara berkala atau *problem* dari PLN | *Avoid* | *High* | | | Menyediakan ganset apabila terjadi lampu mati tiba-tiba |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 5 | *Malware* | Serangan virus atau malware pada laptop | 1. Terdapat banyak virus pada laptop<br>2. Laptop sudah menua | *Mitigate* | *Low* | DSS05.01 *Protect against malware* | Mempelihara dan melakukan langkah-langkah perbaikan terutama yang terbaru *patch* keamanan kontrol virus di perusahaan untuk melindungi sistem dan teknologi informasi dari malware (misal, virus, worm, spyware, spam). Aktivitas :<br>1. Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru<br>2. instal dan aktifkan antivirus untuk PC dan laptop pada fasilitas pemrosesan. | 1. Melakukan *update* antivirus secara terjadwal<br>2. Membatasi akses internet hanya untuk aplikasi layanan.<br>3. Instal aplikasi yang dapat membatasi *malware* masuk |
| | | Serangan virus atau malware pada PC | 1. Banyaknya virus yang terdapat pada PC<br>2. Terdapat kendala didalam *hardware* ataupun *software* | *Mitigate* | *Medium* | | | 1. Melakukan *update* antivirus secara terjadwal<br>2. Membatasi akses internet hanya untuk aplikasi layanan<br>3. Instal aplikasi yang dapat membatasi *malware* masuk<br>4. Memperbarui terkait masalah *hardware* (seperti hardisk, ram dll) |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 6 | *Infrastructure* | Printer (Tinta habis, Catrige bermasalah) | 1. Catrige tidak berjalan<br>2. Tinta habis | *Mitigate* | *Medium* | DSS05.05 *Manage physical access to IT assets.* | Menetapkan dan terapkan prosedur untuk membatasi staf dalam mengakses serta mencatat atau memantau keadaan infrastruktur perusahaan. Aktivitas : Melakukan pelatihan terhadap staf terkait perbaikan infrastruktur secara berkala | Melakukan penjadwalan tentang pengecekan serta penjadwalan untuk dilakukan *maintance* |
| | | Mikrotik *switch*(tidak bisa terhubung) | Penataan kabel jaringan yang terhubung belum tertata dengan baik | *Mitigate* | *Low* | | | . Melakukan penataan ulang terhadap manajemen kabel dari setiap perangkat jaringan yang terhubung<br>2. Melakukan penjadwalan tentang pengecekan dan *maintance* |
| 7 | *Infrastructure theft or destruction* | Pencurian aset monitor | Penampatan PC didalam ruang yang belum terkunci | *Mitigate* | *Low* | DSS01.04 *Manage the environment* | Pertahankan langkah-langkah dalam melindungi perangkat terhadap lingkungan dengan cara pemantauan khusus terhadap lingkungan. Aktivitas : Mengharuskan pengunjung atau staf yang tidak memakai identifikasi untuk di waspadai oleh petugas keamanan | 1. Pemasangan CCTV<br>2. Melakukan kunci pada PC |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingakatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 8 | *Software* | Sistem informasi Bymatrans tidak berjalan | 1. *Software* mengalami *crash* karena *software* terdapat virus ataupun malware<br>2. Aplikasi erorr tidak bisa diakses karena proses *troubleshooting* membutuhkan waktu lebih lama | *Transfer* | *High* | | | 1. Menerapkan DRP (*Disaster Recovery Plan*)<br>2. Dilakukan pengujian dan memperbarui layanan secara berkala<br>3. Pelaporan kepada pihak ketiga terkait masalah yang terjadi. |
| 9 | *Acts of nature* | Bencana alam | Belum pernah terjadi | *Avoid* | *High* | | | Menyiadakan alat bantu pembaca benca alam atau alarm jika terjadi kebarakan tiba-tiba |
| 10 | *Logical attack* | Pemanfaatan celah keamanan oleh pihak luar | Belum pernah terjadi | *Mitigate* | *Low* | APO13.01 *Establish and maintain an information security management system (ISMS)* | Menetapkan dan memelihara ISMS yang menyediakan pendekatan standar untuk keamanan informasi bisnis.<br>Aktivitas :<br>Menetapkan dan komunikasikan peran dan tanggung jawab kepada keamanan informasi | 1. Menambahkan perangkat keamanan yang lebih<br>2. Menerapkan SMKI (Standart Manajemen Keamanan Informasi) |

Tabel 4.18 Rekomendasi (lanjutan)

| No | Kategori risiko | Risiko | Penyebab | Respon risiko | Tingkatan risiko | Proses pemetaan COBIT 5 | Langkah mitigasi | Rekomendasi |
|---|---|---|---|---|---|---|---|---|
| 11 | *Business ownership of IT* | Server mengalami gangguan | Belum pernah terjadi | *Mitigate* | *Low* | *APO01.04 Communicate management objectives and direction.* | Komunikasikan kesadaran dan pemahaman tentang tujuan dan arah TI kepada pihak ketiga terkait kepentingan perusahaan. Aktivitas : Identifikasi pihak ketiga mengenai kepentingan utama dan persyaratan mereka | Jika terjadi gangguan server *Backup* data dilakukan pada satu laptop dan data tersebut disimpan pada *cloud* |

Sumber : Diolah dari hasil penelitian