# BAB V
# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berdasarkan hasil pembahasan dari penelitian ini, dapat dijelaskan kesimpulan sebagai berikut:

1. Untuk mengetahui risiko yang terdapat pada sistem aplikasi Oldist PT. Intan Pariawara, metode OCTAVE dapat diterapkan untuk mengidentifikasikan risiko terhadap seluruh aset yang ada dalam perusahaan. Dari hasil identifikasi risiko, didapatkan total 26 risiko yang terdaftar, dengan 11 risiko yang disebabkan *Human Error*, 6 risiko *Hardware Failure*, 4 *Network Failure*, 4 *Software Failure*, 1 risiko disebabkan dari Penyalahgunaan Hak.
2. Untuk mengetahui penggolongan risiko, FMEA dapat dipergunakan sebagai metode penilaian risiko pada PT. Intan Pariwara. Dari 26 risiko yang sudah teridentifikasi, terdapat 15 risiko yang memiliki ranking *Very Low*, 7 risiko dengan ranking *Low*, dan 3 risiko dengan ranking *Medium*. PT. Intan Pariwara dapat memprioritaskan untuk mengatasi risiko dari *medium*. Hal tersebut dikarenakan *level medium* adalah *level* risiko tertinggi dari hasil identifikasi risiko yang bisa berdampak terhadap kelancaran proses bisnis perusahaan.
3. Untuk langkah pengurangan dampak risiko, ISO dapat digunakan sebagai rekomendasi mitigasi risiko. Dari hasil identifikasi risiko, didapatkan 11 rekomendasi berdasarkan ISO 27001 yang dapat dijadikan acuan untuk dilakukan mitigasi risiko:
    a. Melakukan pemilihan terhadap calon karyawan yang memiliki kemampuan yang cocok dengan pekerjaan, dan penjelasan mengenai tugas yang dilakukan terhadap karyawan untuk meminimalisir kesalahan dalam pengerjaan tugas. Hal ini dilakukan untuk menghindari kesalahan-kesalahan yang

dilakukan oleh karyawan sehingga harus mengulangi pekerjaan yang sama.

b. Membuat kebijakan dan peringatan sebagai hasil tindak lanjut bagi karyawan yang melakukan tindakan yang merugikan perusahaan. Hal ini diterapkan untuk meminimalisir kemungkinan karyawan melakukan tindakan yang merugikan dengan memanfaatkan kelemahan baik dari sistem perusahaan maupun peraturan.
c. Menggunakan antivirus untuk mencegah perangkat terserang virus baik dari software yang akan di install maupun penyalinan berkas. Hal ini diterapkan untuk mencegah komputer terinfeksi virus yang berpotensi untuk menghambat kinerja karyawan.
d. Memberikan reward terhadap karyawan supaya karyawan bekerja keras sesuai dengan prosedur yang ada dalam perusahaan. Hal ini diterapkan untuk membuat karyawan berusaha bekerja dengan benar untuk memenuhi target perusahaan dan mengurangi tingkat kesalahan yang disebabkan oleh karyawan.
e. Melakukan perbaikan terhadap aplikasi yang sesuai dengan prosedur yang sudah diterapkan dalam perusahaan. Hal ini diterapkan supaya aplikasi dapat berjalan dengan sesuai dan mencegah adanya bug.
f. Memperbarui komponen yang lama dengan komponen yang baru dan support. Hal ini diterapkan untuk mencegah peralatan rusak dalam waktu pemakaian karena usia komponen yang sudah tua.
g. Memberi perlindungan tambahan untuk melindungi dari kerusakan fisik untuk memperpanjang umur peralatan. Hal ini diterapkan supaya kabel tidak mudah rusak karena digigit oleh hewan dan memperpanjang umur kabel.
h. Melakukan prosedur perawatan terhadap peralatan dan memperbarui komponen yang lama dengan komponen yang baru

dan support. Hal ini diterapkan untuk mencegah hal yang dapat menghambat kinerja karyawan seperti adanya malfungsi dari peralatan, hardware yang sudah tidak support lagi.

i. Menggunakan antivirus sebagai bentuk pencegahan terhadap serangan virus. Hal ini diterapkan untuk mengurangi potensi komputer terinfeksi virus dan menghambat kinerja karyawan.

j. Melakukan penjadwalan untuk proses backup dan verifikasi sebagai bukti bahwa backup sudah dilakukan. Hal ini diterapkan apabila data-data yang berada dalam aplikasi Oldist hilang, perusahaan memiliki backup yang dapat menggantikan data yang hilang.

k. Perusahaan memonitor kualitas pelayanan yang diberikan penyedia jasa internet dan memberi peringatan kepada penyedia jasa internet apabila kualitas jaringan yang diberikan kepada perusahaan menurun. Hal ini diterapkan apabila internet dalam perusahaan terdeteksi mulai mengalami gangguan, pihak perusahaan dapat memberitahu pihak penyedia layanan internet untuk memperbaiki layanannya.

## 5.2 Saran

Hasil mitigasi risiko sudah sesuai dengan acuan ISO 27001:2013 yang sudah dinilai menggunakan metode FMEA dapat dijadikan sebagai panduan bagi PT. Intan Pariwara untuk meminimalisir tingkat terjadinya risiko. Dari sisi sumber daya manusia, perusahaan memberikan pelatihan yang lebih mendalam terkait risiko yang teridentifikasi tidak sedikit disebabkan karena *Human Error*.

# DAFTAR PUSTAKA


[1] F. R. Destrianto, N. dan M. A. R. Sitorus, "Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE," *Jurnal Integrasi* , vol. 9, p. 13, Maret 2017.

[2] F. A. Anshori, S. dan A. R. Perdanakusuma, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, p. 7, 2019.

[3] M. K. KHANSA , "KEAMANAN INFORMASI," 26 November 2018. [Online]. Available: http://43217110334.blog.mercubuana.ac.id/2018/11/26/keamanan-informasi/#:~:text=Manajemen%20Risiko%20merupakan%20satu%20dari,yang%20harus%20dilindungi%20dari%20risiko. [Diakses 1 11 2020].

[4] "AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN KERANGKA KERJA ISO 27001 DI PROGRAM STUDI SISTEM INFORMASI UNIKOM," *Majalah Ilmiah UNIKOM*, vol. 16, p. 12, 2018.

[5] L. Munaroh, Y. Amrozi dan R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia Journal*, vol. 5, 2021.

[6] E. Purwanto, "Keamanan Informasi," bpptik kominfo, 24 3 2014. [Online]. Available: https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/. [Diakses 30 6 2021].

[7] B. Supradono, "MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)," *Media Elektrika,* vol. 2, p. 5, 2009.

[8] I. Santosa dan D. Kuswanto, "Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ," *Jurnal Ilmiah,* vol. 9, p. 8, 2016.

[9] S. Supatmi, "UNIKOM," 23 Maret 2020. [Online]. Available: https://repository.unikom.ac.id/62423/. [Diakses 1 11 2020].

[10] C. Alberts dan A. Dorofee, Managing Information Security Risks: The OCTAVE Approach, Addison Wesley, 2002.

[11] A. Kapczyński, E. Tkacz dan M. Rostanski, "Implementation of the OCTAVE Methodology in Security Risk Management Process for Business Resources," dalam *Internet - Technical Developments and Applications 2*, Springer-Verlag Berlin Heidelberg, 2012, p. 286.

[12] "PROTEKSI ASET INFORMASI," 21 11 2014. [Online]. Available: http://eprints.dinus.ac.id/6383/. [Diakses 30 6 2021].

[13] "Definisi Manajemen Risiko," Binus University, [Online]. Available: https://bbs.binus.ac.id/business-creation/2020/04/definisi-manajemen-risiko/. [Diakses 30 6 2021].

[14] S. Andiyanto, A. Sutrisno dan C. Punuhsingon, "PENERAPAN METODE FMEA (FAILURE MODE AND EFFECT ANALYSIS) UNTUK KUANTIFIKASI DAN PENCEGAHAN RESIKO AKIBAT TERJADINYA LEAN WASTE," *Jurnal Online Poros Teknik Mesin*, vol. 6.

[15] "Lean Six Sigma Tools: Mengenal Metode FMEA (Failure Mode and Effects Analysis)," Shift Indonesia, [Online]. Available: http://shiftindonesia.com/lean-six-sigma-mengenal-metode-fmea-failure-mode-and-effects-analysis/. [Diakses 24 11 2020].

[16] R. Budiarto, "MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ," *CESS (Journal of Computer Engineering System and Science)*, vol. 2, pp. 48-58, 2017.

[17] "Failure Modes & Effects Analysis (FMEA)," goleansixsigma, [Online]. Available: https://goleansixsigma.com/failure-modes-effects-analysis-fmea/. [Diakses 23 11 2020].

[18] "ISO 27001:2013," ISO, [Online]. Available: https://www.iso.org/standard/54534.html. [Diakses 3 12 2020].

[19] "The Requirements & Annex A Controls of ISO 27001," ISMS.online, [Online]. Available: https://www.isms.online/iso-27001/requirements-controls/. [Diakses 29 11 2020].

[20] M. L. Balqis, "ANALISIS RISIKO DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DINAS

PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA KABUPATEN TULUNGAGUNG," 2016.

[21] M. D. Purwitasari dan W. S. Sari, "Analisis dan Mitigasi Risiko Aset TI Menggunakan Framework OCTAVE dan FMEA".

# LAMPIRAN

| | |
|---|---|
| | Transkrip Wawancara |
| | **Narasumber 1**: Tri Wahyudi |
| | **Jabatan**: Manajer Software and Desktop |
| | **Narasumber 2**: Muhammad Yanwar Arifin |
| | **Jabatan**: leader IT maintenance BO Klaten |
| | **Narasumber 3**: Rahmat Purnama |
| | **Jabatan**: leader maintenance office |
| No | ***Organization View*** |
| | ***Critical Assets*** |
| 1 | Aset apa saja yang ada untuk mendukung aplikasi Oldist? |
| | Komputer, printer, jaringan yang sudah terhubung VPN |
| 2 | Aset apa yang paling mendukung/penting dalam aplikasi Oldist? |
| | Jaringan, komputer, printer |
| 3 | Seberapa besar pengaruh aset tersebut terhadap keberlangsungan proses bisnis yang ada dalam layanan Oldist PT. Intan Pariwara? |
| | Sangat besar pengaruhnya, tanpa adanya jaringan, komputer, dan printer, proses bisnis dalam perusahaan bisa tertunda. |
| 4 | Sistem informasi apa yang terdapat pada aplikasi Oldist PT. Intan Pariwara? |
| | Terdapat informasi perusahaan yang berisikan transaksi *online*: data penerimaan barang, penjualan, surat pertanggung jawaban (surat penyerahaan, kwitansi, dll) |
| 5 | Siapa saja yang mempunyai kepentingan menggunakan aplikasi Oldist PT. Intan Pariwara? |
| | Hampir semua karyawan menggunakan aplikasi Oldist, contoh: dari bagian tim pembukuan, admin, gudang & Tim 16 |
| | ***Security Requirement for Critical Assets*** |
| 1 | Apakah aplikasi Oldist di PT. Intan Pariwara sudah memberikan checklist terkait kebutuhan keamanan aset informasi yang dimiliki? |

| | |
|---|---|
| | a. Jika sudah, apa saja kebutuhan keamanan yang dilihat dari checklist tersebut yang sudah terpenuhi?<br>b. Jika belum, perlukan adanya checklist terkait kebutuhan keamanan aset informasi yang dimiliki? |
| | Pembagian server (API, interface penjualan, 2 database) dan menggunakan jaringan yg tertutup, sehingga jika ingin terhubung dengan jaringan perusahaan dari luar harus menggunakan VPN |
| 2 | Adakah aturan dalam melakukan pengamanan terkait akses aplikasi Oldist? |
| | Dalam pengaman data dalam server, dari segi arus listrik, apabila listrik mati, genset langsung menyala untuk menggantikan suplai listrik. Lalu ada mirroring server sebagai backup server apabila server pertama mati. |
| 3 | Apakah ada pemeriksaan secara rutin terhadap keamanan Oldist? |
| | Setiap hari dilakukan berdasarkan laporan yang didapat dari pengguna. Setiap hari juga dilakukan pemeriksaan kondisi server |
| 4 | Apakah ada kegiatan maintenance terhadap Oldist? |
| | Berdasarkan request selama maintenance tersebut tidak merubah alur sistem. Jika request seperti interface improvement akan dilayani. pemeriksaan terhadap komputer-komputer dalam perusahaan juga dilakukan setahun sekali. |
| 5 | Apa ada yang bertanggung jawab dalam memastikan hardware/software dpt diakses oleh orang yang berhak |
| | pengaksesan aplikasi Oldist hanya dibatasi dalam perusahaan |
| 6 | Apakah ada prosedur keamanan dalam pengaksesan layanan aplikasi Oldist? |
| | Setiap user memiliki hak akses yang sudah disesuaikan dengan role/jabatan |
| 7 | Apakah ada mekanisme untuk mencegah pembobolan aset maupun aplikasi? |

| | |
|---|---|
| | Dengan mengaktifkan antivirus dan firewall yang sudah menjadi satu paket bersama dengan instalasi software windows |
| 8 | Apakah sensitifitas informasi dilindungi oleh tempat penyimpanan yang aman? |
| | Seluruh data disimpan dalam database perusahaan. |
| | ***Threat to Critical Assets*** |
| 1 | Apakah aplikasi Oldist dan aset pendukungnya pernah mengalami ancaman?<br>a. Jika pernah, apa saja ancaman yang pernah dialami? Apa dampak yang dialami dari ancaman tersebut terhadap keberlangsungan aplikasi?<br>b. Jika belum, ancaman apakah yang memungkinkan terjadi? |
| | Pernah: website penjualan yang mati secara tiba-tiba sehingga menghentikan proses bisnis perusahaan, penggunaan hak akses untuk melakukan plagiasi, internet untuk cabang perlu internet |
| 2 | Di mana aset yang sudah disebutkan itu beroperasi/berada? |
| | Untuk seluruh aset bekerja di dalam perusahaan, namun jika untuk pengaksesan baik aplikasi web dan Modist dapat diakses di mana saja. |
| 3 | Bagaimana perusahaan melakukan pencegahan terhadap ancaman aset dan aplikasi Oldist? |
| | Dilakukan maintenance terhadap setiap aset yang ada. |
| 4 | Seberapa sering terjadinya server down pada server? Apa penyebab terjadinya server down? |
| | Server pernah down yang disebabkan karena adanya gangguan dari jaringan |
| 5 | Seberapa sering terjadinya pembobolan? |
| | Selama ini tidak pernah terjadi pembobolan |
| | ***Current Security Practice*** |
| 1 | Apakah ada informasi mengenai aplikasi Oldist di PT. Intan Pariwara? |
| | Ada di setiap perubahan yang terjadi dalam Oldist dibuatkan tutorial dalam bentuk video. |

| | |
|---|---|
| 2 | Apakah perusahaan menerapkan framework atau standar keamanan khusus aset informasi?<br>a. Jika iya, standart atau framework apa yang digunakan?<br>b. Jika tidak, perlukan adanya standart atau framework khusus pengamanan aset informasi? |
| | Belum pernah. Perusahaan memerlukan standar ataupun framework untuk pengamanan aset informasi untuk meningkatkan keamanan yang ada |
| 3 | Apakah di aplikasi Oldist milik PT. Intan Pariwara sudah melakukan penilaian risiko untuk keamanan informasi? |
| | Sudah untuk pemeriksaan data melalui tim DBA. |
| 4 | Apakah aplikasi Oldist menerima dan bertindak atas laporan rutin dari informasi yang berhubungan dengan keamanan? |
| | Setiap ada masalah yang ditemukan langsung dilaporkan untuk segera ditindak lanjuti |
| 5 | Apakah kendala dalam melakukan implementasi standart atau framework pengamanan aset informasi pada aplikasi Oldist milik PT. Intan Pariwara? |
| | Belum diketahui karena belum pernah mengimplementasikannya |
| 6 | Apakah di Department IT sudah memiliki kebijakan dan prosedur dalam melindungi informasi ketika bekerja sama dengan perusahaan lain? |
| | Kebijakan dan prosedur untuk perlindungan informasi sudah diatur melalui tim Bustra dengan memberikan hak pengaksesan terhadap data-data yang berkaitan kepada perusahaan yang bekerja sama |
| | **Current *Organizational*** |
| 1 | Apa masalah yang sering terjadi dalam aplikasi Oldist terkait aset informasi? |
| | Jaringan yang terputus, komputer mengalami masalah, adanya pembuatan laporan palsu (nota fiktif) |
| 2 | Pernahkah terjadi pencurian informasi dalam aplikasi Oldist?<br>a. Jika pernah, informasi apa yang telah dicuri? Apa penyebab asset informasi tersebut bermasalah? |

| | |
|---|---|
| | b. Jika belum, informasi apa saja yang memungkinkan terjadinya pencurian? |
| | Belum, dan apabila terjadi data yang tercuri hanya data transaksi dan data sekolah yang tidak menguntungkan pihak pencuri. |
| 3 | Apakah kapasitas server yang dimiliki aplikasi Oldist sudah mencukupi? |
| | Masih mencukupi |
| 4 | Berapa kali dalam setahun aplikasi Oldist PT. Intan Pariwara melakukan evaluasi terhadap keamanan teknologi informasi? |
| | Bergantung dari situasi, bisa dilakukan saat ada kasus, bisa dilakukan disaat waktu briefing dan melakukan sharing. |
| 5 | Apakah dalam aplikasi Oldist sudah diberlakukan verifikasi untuk setiap divisi dalam mengurus hak akses dan otorisasi? |
| | Sudah diterapkan sesuai dengan peran setiap pengguna |
| 6 | Bagaimana kode etik yang diterapkan pada aplikasi Oldist terkait pengamanan aset informasi? |
| | Melalui tim SOP pelatihan memberikan sosialisasi sesuai dengan user yang bersangkutan. |
| **No** | ***TECHNOLOGICAL VIEW*** |
| | ***Key Component*** |
| 1 | Perangkat IT apa saja yang dipakai aplikasi Oldist? |
| | Komputer, printer, jaringan |
| | ***Current Technology Vulnerability*** |
| 1 | Apakah dalam Department IT terdapat prosedur untuk menjaga kerentanan teknologi seperti meninjau sumber informasi, mengelola keamanan tempat penyimpanan dan mengidentifikasi komponen infrastruktur? |
| | Melakukan pengetesan internal untuk menghindari munculnya bug dalam aplikasi |
| 2 | Apakah Department IT melakukan penjadwalan dan evaluasi kerentanan TI secara berkala? |

| | |
|---|---|
| | Tidak pernah. Evaluasi hanya dilakukan apabila terjadi error dalam penggunaan aplikasi |
| 3 | Bagaimana bentuk penanggulangan terkait adanya gangguan dalam aplikasi Oldist? |
| | Dengan mencari di mana letak kesalahan yang terkait, sebagai contoh apabila gangguan dari sisi user penginputan data maka dilakukan pengeditan data yang ada dalam database. Lalu apabila kesalahan dalam konfigurasi komputer, maka tinggal komputer yang diperbaiki. |
| 4 | Apakah dinas komunikasi dan informatika memiliki dokumen mengenai jenis-jenis kerentanan dan metode serangannya? |
| | Tidak ada |
| 5 | Siapa yang bertanggung jawab memanajemen kerentanan aplikasi Oldist? |
| | divisi software, database. Tergantung dari masalah yang ada. |
| 6 | Apakah PT. Intan Pariwara menyediakan kesempatan bagi staff TI untuk mengikuti pelatihan untuk mengelola kerentanan teknologi dan menggunakan alat-alat evaluasi kerentanan? |
| | Iya dengan melalui mulut ke mulut supaya seluruh karyawan dapat mengetahui dan dapat mengatasinya apabila terjadi permasalahan yang sama |
| **No** | ***RISK ANALYSIS*** |
| | ***Protection Strategy*** |
| 1 | Adakah strategi dalam melakukan pengamanan data dan informasi dalam aplikasi Oldist?<br>a. Jika sudah ada, strategi pengamanan data dan informasi apa yang diterapkan?<br>b. Jika belum ada, perlukah adanya pengamanan data dan informasi? |
| | Dengan memberikan password kombinasi yang banyak. Dan apabila ada kelemahan yang ditemukan baik dalam aset maupun aplikasi langsung diperbaiki. |
| | ***Risk Mitigation Plans*** |

| | |
|---|---|
| 1 | Apakah aplikasi Oldist memiliki Disaster Recovery Plan (DRP) pada aset informasinya?<br>a. Jika sudah ada, aset informasi apakah yang sudah tercover oleh DRP tersebut?<br>b. Jika belum ada, perlukah adanya Disaster Recovery Plan (DRP) pada aset informasi? |
| | Ada, dengan melakukan backup data |

# TABEL REVISI

| No. | Tugas Revisi | Halaman Revisi |
|---|---|---|
| 1 | Gambar Metodologi Penelitian | Perubahan gambar metodologi penelitian dengan menghilangkan kolom “Metode” dan menaruh kolom “Tahap Penelitian” di posisi kiri dari kolom “Metodologi Penelitian OCTAVE” |
| 2 | Penataan Kalimat Bab 5 Kesimpulan | Penambahan pada awal kalimat pada nomor 1,2, dan 5 untuk membuat hasil kesimpulan dengan bagan keterkaitan menjadi sesuai. |
| 3 | Perbaikan Latar Belakang | Memperbaiki penataan kalimat supaya dapat dipahami dan paragraf dapat saling terhubung. |
| 4 | Perbaikan terhadap perumusan masalah, pertanyaan penelitian, tujuan, dan bagan keterkaitan | Perbaikan kalimat untuk sinkronisasi terhadap perumusan masalah, pertanyaan penelitian, tujuan, dan bagan keterkaitan |
| 5 | Perbaikan terhadap sub bab 2.1 | Penghapusan kalimat supaya isi kalimat langsung pada intinya. |
| 6 | Perbaikan kalimat dalam sub bab 2.1.1 | Menghapus kalimat supaya isi kalimat langsung pada intinya. |
| 7 | Pemanggillan terhadap nomor tabel dan gambar | Setiap tabel dan ngambar yang ada harus dipanggil. |
| 8 | Penghapusan isi tabel yang kosong | Menghapus isi tabel yang kosong yang tidak memiliki isi penjelasan. |
| 9 | Perbaikan format tabel | Perubahan format tabel sesuai dengan template yang sudah disediakan. |
| 10 | Perbaikan kalimat Bab 5 Kesimpulan | Perubahan kalimat dan poin yang terdapat dalam hasil kesimpulan supaya dapat menjawab dari pertanyaan penelitian yang terdapat dalam Bab 1 |