ANALISIS RISIKO ASET TI MENGGUNAKAN METODE OCTAVE PADA SWD RESTO

Fahri Husaini [1)], Awalludiyah Ambarwati [2)], Lukman Junaedi [3)]

[1)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Email: fahri04214119@gmail.com
[2)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Email: ambarwati1578@yahoo.com
[3)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Email: lukman.junaedi@narotama.ac.id

Abstrak

Rumah makan atau restoran merupakan salah satu jenis usaha yang sangat terbantu dengan adanya dukungan Teknologi Informasi/Sistem Informasi (TI/SI) dalam operasionalnya. Pengusaha rumah makan, baik yang belum ataupun yang telah memiliki cabang, sangat terbantu dengan penerapan TI/SI guna memantau kondisi dan kinerja perusahaan. SWD Resto adalah rumah makan yang berpusat di Surabaya dan telah memiliki cabang di luar pulau. SWD Resto menyajikan makanan di tempat dan menyediakan layanan *take-out dining* serta *delivery service*. Penerapan TI/SI pada SWD Resto bertujuan untuk meningkatkan pelayanan, ketepatan, kecepatan yang selaras dengan visi dan misi perusahaan. Aset TI yang dimiliki SWD Resto semakin bertambah sehingga perlu dilindungi dari risiko. Namun demikian, aset TI yang dimiliki belum dikelolah dengan baik. Penelitian ini bertujuan untuk melakukan analisis risiko TI pada SWD Resto menggunakan metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*). Pengumpulan data dilakukan melalui observasi, wawancara dan pengisian kuisioner. Hasil penelitian berupa dokumentasi identifikasi aset kritis yang terdapat pada SWD Resto pusat dan cabang beserta ancaman, kerentanan dan pendekatan mitigasi pada setiap aset kritis.
Kata kunci: analisis risiko, aset TI, OCTAVE

Abstract

A Restaurant is one of business type that is greatly helped by Information Technology/Information System (IT/IS) support in its business operations. IT/IS assist restaurant entrepreneurs, whether already have a branch or not, to monitor company condition and performance. SWD Resto is a restaurant based in Surabaya and has branches in other island. SWD Resto provide several services namely dine in, take-out dining and delivery services. IT/IS implementation at SWD Resto goals to improve service, accuracy, speed which is in line with the company's vision and mission. The IT assets owned by SWD Resto are increasing so it needs to be protected from risk. However, IT assets owned by SWD Resto are not managed properly yet. This study aims to conduct an IT risk analysis on SWD Resto using the OCTAVE (Operational Critical Threat, Assets, and Vulnerability Evaluation) method. Data is collected through observation, interviews and filling out questionnaires. As results, it generate documentation of critical asset identification in SWD Resto head and branch along with threats, vulnerabilities and mitigation approaches on each critical asset.
Keyword: *IT asset, OCTAVE, risk analysis*

I. PENDAHULUAN)

Penerapan Teknologi Informasi/Sistem Informasi (TI/SI) pada sebuah rumah makan atau restoran telah menjadi suatu kebutuhan yang dapat menunjang segala proses operasional. Pengusaha rumah makan, baik yang belum ataupun yang telah memiliki cabang, sangat terbantu dengan penerapan TI/SI guna memantau kondisi dan kinerja perusahaan. Informasi kinerja rumah makan yang akurat, sangat

ISSN : 2598-0076

mendukung pengambilan keputusan bisnis yang tepat pada usaha rumah makan.

SWD Resto adalah rumah makan yang berpusat di Surabaya dan telah memiliki cabang di luar pulau. SWD Resto menyajikan makanan di tempat dan menyediakan layanan *take-out dining* serta *delivery service*. TI/SI telah diterapkan dalam operasional SWD Resto, salah satunya adalah Restomate yang merupakan sistem informasi manajemen rumah makan yang memiliki fitur pemesanan, pengelolaan stok bahan makanan yang terdapat di gudang hingga pelaporan. SWD Resto membangun infrastruktur TI yang cukup handal, agar Restomate dapat berjalan dengan baik. Pengguna Restomate pada SWD Resto adalah Admin, Karyawan, Chef dan Pemilik SWD Resto.

Infrastruktur TI, perangkat lunak (Restomate dan lainnya), informasi yang dihasilkan dan pengguna Restomate merupakan aset TI yang berharga bagi SWD Resto. Aset TI yang dimiliki tersebut perlu dijaga dan dilindungi dari risiko (Salahuddin, Ambarwati, & Azam, 2018). Risiko merupakan kemungkinan terjadinya suatu peristiwa akibat adanya ancaman dan kerentanan yang dapat merugikan perusahaan. Penerapan TI/SI pada SWD Resto pernah mengalami beberapa masalah, salah satunya yaitu tidak berjalannya sistem karena kesalahan dari pengguna yang belum mengetahui cara penggunaan Restomate dengan benar.
Namun tidak dapat dipungkiri bahwa ada ancaman lain yang dapat mengganggu bahkan melumpuhkan aset TI yang dimiliki SWD Resto dan mengakibatkan kerugian. Untuk menghindari terjadinya kerugian perusahaan, perlu dilakukan identifikasi risiko aset TI yang dimiliki. Penelitian ini bertujuan untuk melakukan analisis risiko TI pada SWD Resto menggunakan metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) serta memberikan rekomendasi mitigasi dari risiko. Metode OCTAVE dapat digunakan untuk melakukan identifikasi dan evaluasi risiko keamanan informasi. OCTAVE dapat membantu perusahaan dalam melakukan evaluasi risiko kualitatif, identifikasi aset TI yang penting sesuai misi organisasi, juga melakukan identifikasi kerentanan dan ancaman terhadap aset TI tersebut serta melakukan evaluasi potensi konsekuensi jika ancaman tersebut terjadi (Caralli, Stevens, Young, & Wilson, 2007).

II. KAJIAN LITERATUR

Pemanfaatan TI memiliki beberapa risiko dalam institusi perguruan tinggi seperti Politeknik Kesehatan Kemenkes Semarang. Risiko tersebut diantaranya adalah hilangnya data, *redundancy*, data rusak, infeksi data oleh *malware* dan virus, personil yang menyalah gunakan hak akses yang dimiliki. Hal tersebut menghambat proses bisnis dan merugikan baik itu dari segi waktu maupun biaya bagi pihak institusi dan mahasiswa. Metode OCTAVE digunakan untuk mengetahui tingkat risiko, daftar komponen risiko dan cara menanggulangi risiko tersebut. Hasil identifikasi risiko aset TI menggunakan OCTAVE diperoleh 50 risiko. Mitigasi risiko dilakukan dengan cara *tolerate, treat, transfer* dan *terminate* (Purwitasari & Sari, 2017).

Dinas Komunikasi dan Informasi Pemerintah Kota Salatiga (Dinas Kominfo Kota Salatiga) bertugas membantu Walikota Salatiga untuk menyelenggarakan Pemerintah Kota Salatiga. Monitoring aset TI jarang dilakukan. Kehilangan aset TI sering kali dialami Dinas Kominfo Kota Salatiga yang berakibat mempengaruhi produktifitas. Penilaian risiko TI dilakukan menggunakan metode OCTAVE-S. Hasil penilaian risiko untuk kategori *hadware* dan keamanan adalah tinggi, sedangkan *software* dan jaringan memiliki tingkat risiko sedang. Hasil tersebut dapat digunakan Dinas Kominfo Kota Salatiga sebagai acuan untuk mengambil kebijakan dalam penanganan risiko TI (Setyawan & Wijaya, Agustinus Fritz, 2018)

ISSN : 2598-0076

III. METODE PENELITIAN

Analisis risiko TI di SWD Resto dilakukan dengan mengadopsi Metode OCTAVE yang memiliki beberapa fase, seperti pada Gambar 1. Pengumpulan data dilakukan melalui observasi, review dokumen dan wawancara kepada narasumber yaitu pemilik SWD Resto dan manager TI. Fase pada Metode OCTAVE dapat dijabarkan sebagai berikut (Supradono, 2009):

A. Persiapan

Persiapan yang dilakukan adalah menyusun jadwal, membentuk tim analisis yang terdiri dari Peneliti, Pemilik SWD Resto, Manager TI SWD Resto dari setiap cabang. Melakukan Studi Literatur, membuat *interview Protocol* dan wawancara.

B. Fase 1 : Membangun Aset Berbasis Ancaman Profil

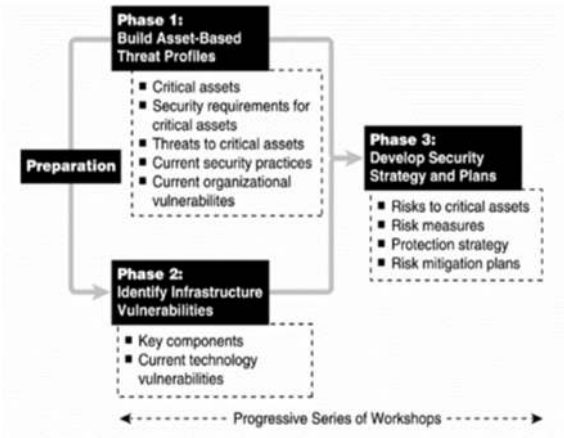
Melakukan pengolahan data yang diperoleh pada fase sebelumnya. Keluaran dalam fase 1 ini meliputi daftar aset penting SWD Resto, daftar kebutuhan keamanan SWD Resto (kerahasiaan, integritas dan ketersediaan), daftar ancaman aset kritis SWD Resto, daftar keamanan yang telah diterapkan SWD Resto dan daftar kelemahan SWD Resto.

C. Fase 2 : Identifikasi Infrastruktur Vulnerabilities

Melakukan identifikasi kelemahan dari segi infrastruktur SWD Resto sebagai bagian pendukung penggunaan aset TI. Keluaran yang didapatkan adalah daftar komponen kunci dan kerentanan/kelemahan dari komponen kunci.

D. Fase 3 : Mengembangkan Strategi Keamanan dan Perencanaan

Melakukan proses identifikasi risiko dari aset kritis, pemberian tindakan pada risiko, proteksi dan rencana mitigasi. Keluaran dari tahap ini adalah daftar risiko pada SWD Resto, daftar dampak risiko, proteksi dan mitigasi risiko dari SWD Resto.



Gambar 1. Fase dalam Metode OCTAVE (Caralli et al., 2007)

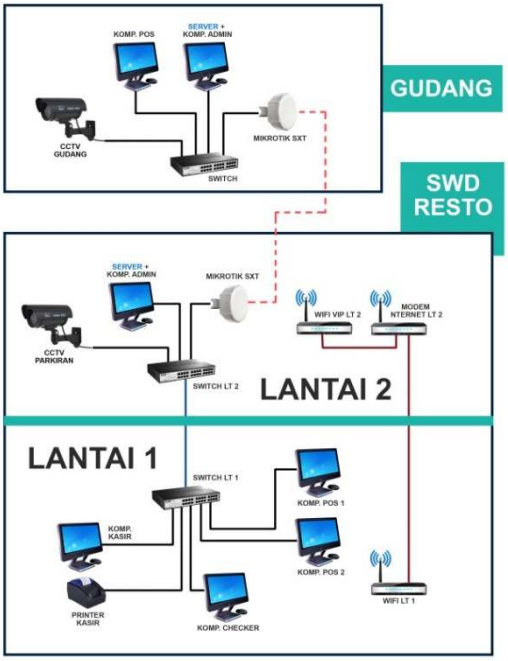
IV. HASIL DAN PEMBAHASAN

Hasil penelitian dari fase dalam Metode OCTAVE yang telah dilakukan dapat adalah sebagai berikut:

A. Persiapan

Hasil wawancara dan observasi yang telah dilakukan sebelumnya, dapat diketahui kondisi *existing* dan proses bisnis dari SWD Resto. Untuk mendukung proses bisnis perusahaan, SWD Resto telah menggunakan Restomate dan membangun infrastruktur TI (Gambar 2). Terdapat beberapa komputer untuk melayani pelanggan dan satu komputer yang berfungsi sebagai server yang digunakan admin untuk membuat laporan dan pengelolaan stok bahan makanan. Seluruh komputer terhubung antara satu dengan yang lainnya menggunakan jaringan LAN (*Local Area Network*).

ISSN : 2598-0076



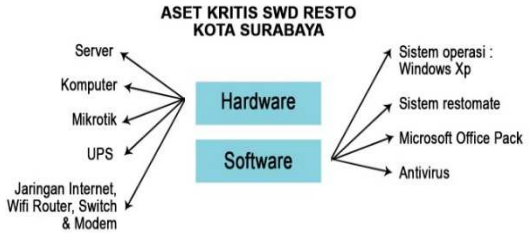
Gambar 2. Infrastruktur SWD Resto

Gambar 2 memperlihatkan bahwa SWD Resto juga memiliki dua komputer yang berada di gudang sebagai server dan pos. Komputer tersebut digunakan pegawai untuk mengatur *update* bahan makanan dan admin gudang untuk mengelola stok bahan makanan yang berada di gudang. SWD Resto juga menggunakan microtik sebagai penghubung antara server yang berada di Resto dengan server yang berada di gudang. Jaringan Wifi juga terpasang pada SWD Resto agar pelanggan juga dapat memiliki akses internet.

B. Fase 1 : Membangun Aset Berbasis Ancaman Profil

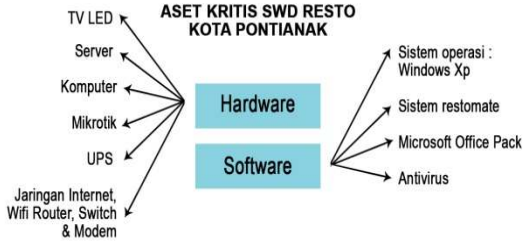
SWD Resto memiliki restoran yang berlokasi di Surabaya dan Pontianak. Aset kritis SWD Resto dikategorikan berupa *hardware* dan *software*. Gambar 3 adalah aset kritis SWD Resto kota Surabaya, sedangkan Gambar 4 adalah aset kritis SWD Resto kota Pontianak.

Aset kritis SWD Resto kota Surabaya pada kategori *hardware* terdapat Server, Komputer, Mocrotik, UPS dan jaringan internet, Wifi/Router, Switch & Modem. Sedangkan di kategori *software* terdapat Sistem Operasi Windows Xp, Sistem Restomate, Microsoft Office Pack & Antivirus.



Gambar 3. Aset kritis SWD Resto Surabaya

Gambar 4 merupakan aset kritis SWD Resto kota Pontianak. Pada kategori Hardware terdapat TV LED, Server, Komputer, Mocrotik, UPS dan jaringan internet, Wifi/Router, Switch & Modem. Sedangkan di kategori Software meiliki aset kritis Sistem Operasi Windows Xp, Sistem Restomate, Microsoft Office Pack & Antivirus.



Gambar 4. Aset kritis SWD Resto Pontianak

Sumber ancaman aset TI/SI pada SWD Resto dapat dibagi jadi empat sumber yakni:

a. Tindakan sengaja baik dari pihak dalam maupun dari pihak luar
b. Tindakan tidak sengaja baik dari pihak dalam maupun dari pihak luar
c. *Hardware/Software* bermasalah (termakan usia atau terkena virus)
d. Bencana Alam seperti banjir, kebakaran dan serangan petir

Identifikasi kelemahan SWD Resto dari pihak organisasi di antaranya pengetahuan tentang TI yang dimiliki oleh pengguna atau tim operational (Waiters, Kasir, Checker, Admin Rumah makan dan Admin Gudang) belum memadai. Pengguna yang bekerja di lapangan juga sangat sedikit. Informasi yang diberikan pada tim TI SWD Resto tidak lengkap, sehingga laporan yang masuk pada tim TI berbeda dengan kerusakan yang terjadi. Pengguna

ISSN : 2598-0076

di lapangan masih memiliki tingkat ketergantungan yang tinggi pada tim TI. Belum banyak tim TI yang menguasai Sistem Restomate, mengakibatkan tingkat ketergantungan yang tinggi pada pihak Vendor Restomate.

C. *Fase 2 : Identifikasi Infrastruktur Vulnerabilities*

Pada tahap ini dilakukan identifikasi kelemahan dari segi infrastruktur SWD Resto sebagai bagian pendukung penggunaan aset TI. Hasil identifikasi aset TI pada SWD Resto didapatkan empat aset yang merupakan komponen kunci yaitu Mikrotik, server, komputer dan jaringan. Setelah melakukan identifikasi komponen kunci tahap selanjutnya adalah menganalisis kerentanan/kelemahan pada komponen kunci yang disajikan pada Tabel 1.

Tabel 1. Kelemahan Komponen kunci

No.	Komponen kunci	Kelemahan
1	Mikrotik	Penempatan mikrotik berada ditempat yang terbuka. Tanpa perlindungan lebih sehingga berisiko terkena hujan dan serangan petir.
2	Server	Server tidak *redundant* karena terkendala dengan biaya.
3	Komputer	Perlindungan saat ini masih berupa antivirus. Belum menggunakan perlindungan yang lebih. Karena Tim TI yakin dengan pemisahan jaringan internet akan menjamin keamanan komputer.
4	Jaringan	Belum mengikuti kaidah yang sesuai untuk menjamin konsistensi peralatan tersebut untuk tetap sesuai dengan fungsinya.

D. *Fase 3 : Mengembangkan Strategi Keamanan dan Perencanaan*

Setelah mendapatkan komponen kunci beserta kelemahannya pada tahap ini dilakukan proses identifikasi risiko dari aset TI SWD Resto. Terdapat empat macam tindakan dalam menangani risiko yaitu:

a. *Take*, tindakan menerima risiko yang ada dikarenakan risiko tersebut tidak dapat dihindari seperti bencana alam yang tidak dapat dihindari
b. *Treat,* tindakan mengambil langkah langsung untuk mengurangi dampak dari risiko
c. *Terminate*, tindakan menghentikan risiko
d. *Transfer*, pengalihan risiko kepada pihak lain misalnya dialihkan kepada pihak asuransi.

Tabel 2. Daftar risiko pada kategori *hardware*

No	Risiko	Penyebab	Tindakan	Mitigasi
1	Kerusakan Server	Kesalahan melakukan konfigurasi	Treat	Adanya prosedur dalam proses konfigurasi
		Adanya serangan virus	Treat	Adanya antivirus yang dipasang pada *hardware*, dilakukan *update* setiap tiga bulan
		Usia *hardware* (RAM, Hardisk, dan lainnya) sudah terlalu lama	Treat	Melakukan *back up* data secara rutin

Tabel 2. Daftar risiko pada kategori *hardware* Lanjutan

No	Risiko	Penyebab	Tindakan	Mitigasi
2	Kerusakan Server	Bencana alam (kebakaran dan petir)	Take	Menyediakan alat pemadam kebakaran disetiap ruangan, memiliki *back up* data
		Masuknya pencuri kedalam rumah makan	Treat	Mengunci setiap ruangan yang memiliki aset penting, memiliki *back up* data
3	Gangguan pada komputer	Kesalahan dalam melakukan Instalasi Sistem Operasi	Treat	Adanya pelatihan dalam melakukan instalasi sistem Operasi pada tim IT pada awal masuk
		Adanya serangan virus	Treat	Adanya antivirus yang dipasang pada *hardware*, dilakukan *update* setiap tiga bulan
		Usia *hardware* (RAM, Hardisk, dan lainnya) sudah lama	Treat	Peremajaan *hardware* setiap beberapa tahun sekali
3	Gangguan pada komputer	Bencana alam seperti kebakaran dan petir	Take	Terdapat alat pemadam kebakaran disetiap ruangan
4	Kehilangan Komputer	Masuknya pencuri kedalam Rumah makan	Treat	Adanya CCTV yang terpasang dibeberapa ruangan
5	Gangguan Mikrotik	Usia Mikrotik sudah terlalu lama	Treat	Peremajaan Hardware setiap beberapa tahun sekali

ISSN : 2598-0076

		Terjadinya korsletting listrik	Treat	Terdapat alat pemadam kebakaran disetiap ruangan
		Bencana alam seperti serangan petir	Take	Terdapat alat penangkal petir disetiap ruangan
6	Kerusakan pada UPS	Terjadinya korsletting listrik	Treat	Memiliki Genset sebagai backup tenaga listrik jika terjadi pemadaman
		Bencana alam seperti kebakaran	Take	Terdapat alat pemadam kebakaran disetiap ruangan

Tabel 2. Daftar risiko pada kategori *hardware* Lanjutan

No	Risiko	Penyebab	Tindakan	Mitigasi
7	Kerusakan kabel dan konektor jaringan	Kabel terputus akibat hewan (tikus)	Treat	Memasang *Cable Duct* pada kabel setiap ruangan
		Konektor tidak terpasang dengan baik	Treat	Adanya pelatihan untuk tim IT dalam penataan kabel dan jaringan yang baik
8	Gangguan Pada switch	Kebakaran bangunan	Treat	Terdapat alat pemadam kebakaran disetiap ruangan
		Salah satu port Switch rusak akibat Arus listrik ground	Treat	Membuat grounding listrik yang baik
		Usia Switch yang sudah lama	Treat	Maintenance yang dilakukan rutin pada hardware setiap 1 tahun sekali / ganti baru
9	Gangguan pada LED TV	Bencana alam seperti petir dan hujan lebat	Take	Terdapat Penangkal petir dan alat pemadam kebakaran di setiap ruangan
9	Gangguan pada LED TV	Adanya kerusakan pada kabel dan jaringan	Treat	Memasang *Cable Duct* pada kabel setiap ruangan
		Terjadinya korsletting listrik	Treat	Terdapat alat pemadam kebakaran di setiap ruangan
		Penyalahgunaan oleh karyawan yang tidak sesuai dengan proses bisnis	Treat	Telah diberlakukan pembatasan penggunaan hak akses
		Usia LED Tv yang sudah lama	Treat	Maintenance yang dilakukan rutin pada hardware / ganti baru

Setelah mengetahui risiko dan memberikan tindakan pada risiko, tahap selanjutnya adalah membuat rencana mitigasi pada setiap risiko yang disajikan pada Tabel 2 dan Tabel 3. Tindakan yang diambil SWD Resto pada risiko adalah *take, treat* dan *transfer*. Untuk kategori *hardware*, hanya dilakukan *take* dan *treat*. Tindakan *take* diambil untuk risiko kerusakan server, gangguan pada komputer dan mikrotik, kerusakan pada UPS dan gangguan pada LED TV yang kesemuanya disebabkan bencana alam. Sedangkan tindakan *treat* diambil untuk risiko kerusakan server, gangguan pada komputer, kehilangan komputer, gangguan mikrotik, kerusakan pada UPS, kerusakan kabel dan konektor jaringan, gangguan pada switch dan gangguan pada LED TV yang disebabkan selain bencana alam.

Tabel 3. Daftar risiko pada kategori *Software*

No	Risiko	Penyebab	Tindakan	Mitigasi
1	Sistem Operasi *Crash*	Hardware tidak dapat bekerja dengan baik (kinerja RAM dan Hardisk tidak maksimal)	Treat	Maintenance yang dilakukan rutin pada hardware setiap 1 tahun sekali / ganti baru
		Adanya serangan virus yang membuat data registry hilang	Treat	Adanya backup data otomatis setiap software close
		Overheating hardware akibat penggunaan terlalu lama	Treat	Menambah Hardware pendingin PC *(Fan, Liquid cooler dll)*
2	Gangguan pada Sistem Restomate	Lisensi sistem tidak diperbarui	Treat	Maintenance yang dilakukan rutin pada Software
		Adanya serangan virus yang membuat data Sistem Restomate hilang	Transfer	Memiliki antivirus (database update minim 3 bulan sekali)
3	Kerusakan pada software pendukung	Adanya serangan virus yang membuat data software pendukung hilang	Treat	Memiliki antivirus (database update minim 3 bulan sekali)

ISSN : 2598-0076

Untuk kategori *software* dilakukan tindakan *treat* dan *transfer*. Tindakan *treat* diambil untuk risiko sistem operasi *crash*, kerusakan pada *software* pendukung dan gangguan pada sistem Restomate yang disebabkan lisensi sistem tidak diperbarui. Sedangkan tindakan *transfer* dilakukan pada risiko gangguan pada sistem Restomate yang disebabkan serangan virus sehingga mengakibatkan kehilangan data.

V. KESIMPULAN DAN SARAN

Melakukan identifikasi ancaman dan risiko merupakan salah satu faktor kesuksesan bagi Rumah makan. Dengan mengidentifikasi ancaman dan risiko Rumah makan dapat meminimalkan risiko yang mungkin terjadi di masa mendatang. SWD Resto memiliki sembilan risiko yang memiliki penyebab yang berbeda-beda. Dua risiko di antaranya risiko yang memiliki penyebab terbanyak yaitu Gangguan pada komputer dan Gangguan pada LED TV. Hasil identifikasi risiko dan mitigasi dapat digunakan sebagai acuan untuk melakukan pencegahan atau penanganan terhadap semua risiko dari setiap aset TI yang dimiliki SWD Resto.

Saran untuk penelitian selanjutnya adalah melakukan pengukuran nilai risiko aset IT SWD Resto, sehingga dapat memberikan perhatian lebih pada aset TI yang memiliki nilai lebih tinggi.
1)

REFERENSI

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process:* https://doi.org/10.21236/ADA470450

Purwitasari, M. D., & Sari, W. S. (2017). *Analisis Dan Mitigasi Risiko Aset Ti Menggunakan Framework OCTAVE dan FMEA (Studi Kasus: Poltekkes Semarang)* (Skripsi, Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro). Retrieved from eprints.dinus.ac.id/22059/3/jurnal_19387.pdf

Salahuddin, S., Ambarwati, A., & Azam, M. N. A. (2018). Identifikasi Risiko Keamanan Informasi Menggunakan ISO 27005 Pada Sebuah Perguruan Tinggi Swasta Di Surabaya. *Seminar Nasional Sistem Informasi (SENASIF)*, *2(1)*, 990–996. Retrieved from https://jurnalfti.unmer.ac.id/index.php/senasif/article/view/123

Setyawan, A. A., & Wijaya, Agustinus Fritz. (2018). Analisis Manajemen Risiko Teknologi Informasi Pada Diskominfo Kota Salatiga Menggunakan Metode OCTAVE-S. *Seminar Nasional Sistem Informasi Indonesia (SESINDO) 2018*, 6. Retrieved from http://is.its.ac.id/pubs/oajis/index.php/file/download_file/1824

Supradono, B. (2009). *Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation), Media Elektrika, 2*(1), 4-8.

ISSN : 2598-0076