ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA DISKOMINFO KOTA SALATIGA MENGGUNAKAN METODE *OCTAVE-S*

Antonius Aris Setyawan[1)] dan Agustinus Fritz Wijaya[2)]
[1,2] Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo, Kel. Blotongan, Kec. Sidorejo, Salatiga, 50715
Telp : (0298) 321212, Fax : (0298) 321433
E-mail : 682014015@student.uksw.edu[1)]

Abstrak

Artikel ini menjelaskan pengukuran tingkat risiko Teknologi Informasi dan menganalisa keamanan yang cocok untuk menanggulangi risiko berada pada Dinas Kominfo Kota Salatiga. Dinas Kominfo Kota Salatiga memiliki permasalah yang tidak diselesaikan seperti aset yang mudah hilang hingga terganggunya produktifitas. Maka diperlukanlah penanggulan dan metode yang digunakan untuk menganalisa OCTAVE-S. Metode ini akan digunakan untuk menganalisa yang ada di Dinas Komunikasi dan Informatika Pemerintah Kota Salatiga melalui langkah langkah untuk mencari hasil pengukuran risiko dan mengatasi permasalahan risikonya. Hasil yang didapat melalui metode yang diterapkan melalui OCTAVE -S adalah perlunya tinjau ulang untuk beberapa hardware yang cukup berumur yang bias menyebabkan terganggu produktifitas hingga perlunya peningkatan keamanan terhadap aset yang ada di Dinas Kominfo Kota Salatiga. Bahwa melalui metode ini sudah diakui bisa mengatasi risiko risiko yang akan datang.

Kata Kunci: *analisa risiko, teknologi informasi, octave-s*

1. PENDAHULUAN

Teknologi saat ini menjadi sangat penting di dunia pekerjaan.mulai dari pemerintahan hingga perusahaan besar sekalipun.Teknologi Informasi atau disebut juga sebagai TI sangat berguna untuk efisiensi pekerjaan [1]. Di balik itu semua tentunya ada kelebihan dan kelemahan TI di setiap masing masing perusahaan/pemerintahan. Mulai data hilang, *corrupt*, virus hingga dukungan TI perusahaan yang kurang diperbarui [2]. Oleh karena itu diperlukan pengukuran pada risiko TI. Untuk mengetahui risiko TI di sebuah perusahaan. Tentu saja perusahaan mempunyai aset informasi mulai dari *hardware*, *software*, sistem informasi hingga manusia merupakan aset yang paling penting bagi suatu organisasi maupun perusahaan yang harus dilindungi dari risiko keamannya mulai dari luar hingga dalam organisasi. Dinas Kominfo Kota Salatiga adalah departemen yang membidangi urusan komunikasi dan informatika yang berada di Kota Salatiga. Tugas dari Dinas Kominfo Pemerintahan Kota Salatiga mempunyai tugas untuk membantu Walikota Salatiga untuk menyelenggarakan Pemerintah Kota Salatiga. Dinas Kominfo Kota Salatiga tentu saja pelayanan yang diberikan berdampak selalu baik untuk warga Kota Salatiga. Dinas Komunikasi dan Informatika sangat jarang sekali untuk memonitor ada barang yang bisa digunakan tetapi tidak pernah dipakai hingga kurangnya persiapan perencanaan ancaman ke depan pada suatu organisasi pada perusahaan itu sendiri. Faktor yang menyebabkan masalah tersebut adalah sangat jarang sekali melakukan manajemen risiko TI. Seperti komputer yang ada di kantor belakang dekat kantor utama, ada 3-4 komputer dengan spesifikasi terbilang cukup mumpuni dan mengeluarkan biaya yang cukup banyak yang jarang sekali dipakai karena beberapa ada yang terkadang membawa/menggunakan laptop pribadi, selain itu keamanan kantor sendiri dimana para penjual dengan mudahnya memasuki ruang kantor bisa berdampak risiko yang cukup tinggi. Manajemen risiko TI penting sekali untuk meminimalisir setiap kegagalan pada suatu perusahaan, sehingga bisa menemukan risiko yang ingin dicari bisa cepat diselesaikan. Melalui Penelitian ini dilakukan penilaian risiko TI menggunakan metode OCTAVE-S, diharapkan dengan metode ini hasil yang didapat bisa berguna untuk mengambil kebijakan dalam penanganan risiko yang bertempat di Dinas Komunikasi dan Informasi Pemerintah Kota Salatiga.

2. TINJAUAN PUSTAKA

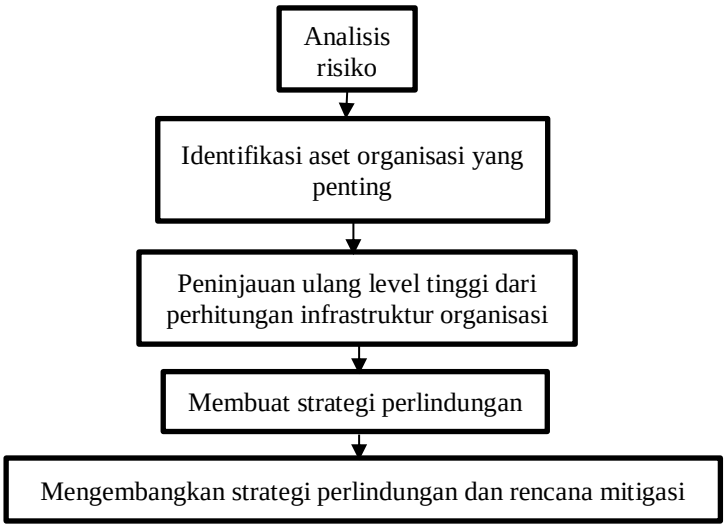
Penelitian diambil dari Universitas Binus dengan judul "*Pengukuran Risiko Teknologi (TI) dengan Metode Octave-S pada PTNL"* oleh Anderes Gui, Sanyoto Gondodiyoto, Irvan Timotius di tahun 2008. Dimana hasil yang difokuskan untuk akses jaringan hingga keperluan pelatihan karyawannya [3]. Kemudian penelitian kedua oleh Jurusan Sistem Informasi, STMIK AKBA, Makassar dengan judul "*Analisis Risiko Keamanan Sistem Informasi Menggunakan Metode Octave-S (Studi Kasus: Sistem Informasi Akademik STMIK AKBA Makassar)*" oleh Syaharullah Disa ditahun 2012. Hasil yang dicapai ialah sistem keamanan dianalisa bagaimana tingkat risikonya [4].

Octave-S menurut Alberts, C dan Dorofee (2003) merupakan pendekatan OCTAVE untuk menemukan kebutuhan kebutuhan kecil. Terhadap organisasi yang bersifat komprehensif, sistematis, kontekstual, dan dapat diarahkan.[5]. Terdapat 3 tahapan untuk melakukan OCTAVE-S berikut:

1. Membangun Aset Berbasis Profil Ancaman
   Membangun Aset Berbasis Profil Ancaman merupakan sebuah evaluasi dari aspek organisasi. Selama dalam tahap ini, tim analisis menggambarkan kriteria dampak evaluasi yang akan digunakan nantinya untuk mengevaluasi risiko. Tahap ini juga mengidentifikasi aset-aset organisasi yang penting, dan mengevaluasi praktek keamanan dalam organisasi saat ini. Tim menyelesaikan tugasnya sendiri dan mengumpulkan informasi tambahan hanya ketika diperlukan.

2. Mengidentifikasi Kerentanan Infrastruktur
   Tim analisis melakukan peninjauan ulang level tinggi dari perhitungan infrastruktur organisasi yang berfokus pada keamanan yang dipertimbangkan pemelihara dari infrastruktur. Tim analisis pertama menganalisis bagaimana orang-orang menggunakan infrastruktur komputer pada akses aset kritis, menghasilkan kunci dari kelas komponen-komponen. Tahap ini memiliki satu proses yaitu memeriksa perhitungan infrastruktur dalam kaitannya dengan aset yang kritis dimana terdapat dua aktivitas.

3. Mengembangkan Strategi Keamanan dan Perencanaan
   Selama tahap ketiga tim analisis mengidentifikasi risiko dari aset kritis organisasi dan memutuskan apa yang harus dilakukan mengenainya. Berdasarkan analisis dari kumpulan informasi, tim membuat strategi perlindungan untuk organisasi dan rencana mitigrasi risiko yang ditujukan pada aset kritis. Kertas kerja OCTAVE yang digunakan selama tahap ini mempunyai struktur tinggi dan berhubungan erat dengan praktek katalog OCTAVE, memungkinkan tim untuk mengubungkan rekomendasi-rekomendasinya untuk meningkatkan praktek keamanan dari penerimaan *benchmark*. Tahap ini terdiri atas dua proses, yaitu: identifikasi dan analisis risiko serta mengembangkan strategi perlindungan dan rencana mitigasi, di mana proses ini memiliki delapan aktivitas. Untuk lebih jelasnya, langkah-langkah tersebut dapat diikuti pada Gambar 1.



Gambar 1. Bagan Tahapan Penelitian

3. METODOLOGI PENELITIAN

Penelitian Manajemen Risiko TI yang bertempat di Dinas Kominfo Kota Salatiga menggunakan metode analisa, pengumpulan data, hingga wawancara [6]. Tahapan pertama pada metode analisa yang didapat di Dinas Kominfo Salatiga terdapat 40 orang dimana di antaranya 20 pranata komputer terampil, 10 pranata komputer ahli, 3 finansial, 2 aset, dan 5 administrator *database*. Tahapan kedua pengumpulan data dilakukan melalui berbagai daftar pustaka yang ada dan tentunya informasinya harus valid sehingga akan lebih mudah untuk penyusunan *paper* ini. Pihak Dinas Komunikasi dan Informatika Pemerintahan Kota Salatiga memberikan sebuah data-data informasi pemerintahan mulai dari *software* dan *hardware* yang digunakan hingga *brainware*. Setelah itu ada pula wawancara jika data Dinas Komunikasi dan Informatika Pemerintahan Kota Salatiga yang diberikan ke penulis kurang, seperti dampak dan risiko terhadap *software*, jaringan, dan *hardware* yang digunakan. Terdapat 18 PC dengan spesifikasi Windows 7 Professional, RAM 4 GB, Intel Core i5, 3610 ME 3.30 Ghz dimana sebagian besar adalah mutasi dari tahun 2008, 6 laptop yang juga hasil mutasi tetapi belum begitu lama karena dari tahun 2013. Dengan jaringan ISP dari PT. Telekomunikasi Indonesia, Tbk serta Bandwidth IP Transit Internasional 60 Mbps *Upload*, 60 Mbps *Download*, IP Transit Domestik 40 Mbps *Upload*, 40 Mbps *Download*, Speedy Gold Internasional-Domestik 20 Mbps *Upload*, 20 Mbps *Download*, Speedy *Backup* Internasional-Domestik 1 Mbps *Upload*, 5 Mbps *Download*, IP Publik AS Number Sekretariat Daerah Kota Salatiga 103.230.100.0/24. Kegunaan internet tersebut digunakan untuk aplikasi *online*, *streaming*, dan *browsing*. *Software* yang digunakan berbasis C+, Debian, Java, dan Visual Studio untuk pengembangan *website* untuk setiap dinas lain dan anti virus yang mereka gunakan SMADAV, AVAST, Windows Defender. Berikut adalah tabel data aset aset pada Dinas Kominfo Salatiga pada Tabel 1.

Tabel 1.Tabel Aset Dinas Kominfo

No.	Nama Barang	Tahun Pemberian	Jumlah Barang	Harga Total Barang	Asal Usul Pwmberian	Masa digunakan
1	*Router* mikrotik	2013	1	RP. 1.430.000	mutasi	4 tahun
2	Jaringan komputer	2009	1	RP. 222.777.750	mutasi	4 tahun
3	*Access point indoor*	2013	5	RP. 3.410.000	mutasi	4 tahun
4	*Access point outdoor*	2013	5	RP. 3.850.000	mutasi	4 tahun
5	PC unit	2008	10	RP. 100.040.000	mutasi	4 tahun
6	Komputer *maintenance*	2013	1	RP. 5.013.000	mutasi	4 tahun
7	Komputer LG	2005	1	RP. 5.637.000	mutasi	4 tahun
8	Komputer Dell	2012	1	RP. 6.030.000	mutasi	4 tahun
9	*Router* CC	2016	2	RP. 33.846.590	mutasi	4 tahun
10	*Server*	2016	1	RP. 42.950.000	mutasi	4 tahun
11	*Server*	2016	1	RP. 45.750.000	mutasi	4 tahun
12	Alat pemadam kebakaran	2014	1	RP. 938.375	mutasi	5 tahun
13	Peralatan jaringan komputer	2016	1	RP. 8.703.410	mutasi	4 tahun
14	*Harddisk* eksternal	2013	1	RP. 1.760.000	mutasi	4 tahun
15	Mesin fax	2011	2	RP. 4.520.000	mutasi	5 tahun
16	Laptop Fujitsu	2013	1	RP. 5.940.000	mutasi	4 tahun
17	Laptop Sony	2013	1	RP. 14.300.000	mutasi	4 tahun
18	Laptop Dell	2013	1	RP. 15.840.000	mutasi	4 tahun
19	Laptop Asus	2015	1	RP. 6.710.000	mutasi	4 tahun
20	Laptop Lenovo	2015	1	RP. 13.860.000	mutasi	4 tahun
21	Printer multifungsi	2014	1	RP. 2.450.000	mutasi	4 tahun
22	*Hardware* anjungan informasi	2012	1	RP. 194.392.000	mutasi	4 tahun
23	*Scanner cautions*	2014	1	RP. 8.374.167	mutasi	4 tahun
24	UPS (besar)	2016	1	RP. 96.250.000	mutasi	4 tahun
25	UPS (kecil)	2016	1	RP. 17.930.000	mutasi	4 tahun

Pemetaan Responden dilakukan melalui tahap wawancara dengan 4 pertanyaan dengan hasil yang berbeda beda dari setiap responden dan dibagi 5 tingkat kepuasaan: 1 = tidak puas, 2 = kurang puas, 3 = cukup, 4 = puas, 5 = sangat puas, dan R = Responden pada Tabel 2.

Tabel 2. Tabel Frekuensi Responden Menjawab

Pertanyaan	R1	R2	R3	R4	R5	R6	R7	R8	JML
Keamanan kantor	3	3	3	3	3	4	4	4	27
Kendala di perangkat PC maupun laptop yang dialami	4	4	3	4	4	3	3	4	29
Kepuasan pengunaan internet	3	3	4	3	4	4	3	3	27
Update secara berkala	4	3	4	4	4	3	4	4	30
	14	13	14	14	15	14	14	15	

Berdasarkan frekuensi tabel pada pemetaan responden yang diterapkan menggunakan SPSS, menunjukan bahwa setiap staf rata-rata memiliki tingkat kepuasan yang cukup dan dimana para 5 dari 8 responden memilih jawaban yang seimbang sebanyak perbandingan 50 persen tersebut memilih daripada 2 responden lebih banyak menjawab puas sekali dan 1 responden lebih banyak menjawab cukup puas sebanyak 75. Dengan total nilai mencapai 30, responden lebih banyak mendominasi jawaban puas sekali daripada jawaban lain. Bisa disimpulkan bahwa para responden memiliki respon yang sebagian besar mendominasi jawaban seimbang dibanding respon puas sekali maupun cukup puas.

4. PEMBAHASAN

Ancaman yang dihasilkan melalui hardware bisa terjadinya kerusakan yang fatal, dikarenakan ada beberapa barang lama di pakai lagi sehingga di masa yang akan datang bisa terhambat dalam tugas-tugas atau produktifitas yang ada di Dinas Komunikasi dan Informatika yang ada di Kota Salatiga. Selain itu ada beberapa barang seperti komputer unit hingga laptop tidak digunakan lagi walau sudah didaur ulang[7]

Ancaman yang dihasilkan melalui keamanan pada Dinas Komunikasi dan Informatika Kota Salatiga terbilang cukup. Walau sudah ada beberapa jaminan keamanannya seperti satpam sebelum pintu masuk utama gerbang pemerintahan kota Salatiga hingga adanya alat pemadam kebakaran. Seringkali ada beberapa orang asing masuk tanpa ada kepentingan sama sekali sehingga bisa terjadi adanya hal yang tidak dinginkan seperti pencurian maupun pengrusakan fasilitas.

Ancaman yang dihasilkan melalui keamanan jaringan dan software juga terbilang cukup. Hanya saja pernah terjadi terkena virus sebanyak satu kali saja karena yang digunakan Avast, Smadav dan Windows Defender saja walau memang sering rutin *update* dan pada saat itu juga pernah terjadi lupa *update*. Sedangkan untuk jaringan terbilang sangat mencukupi sekali untuk kebutuhan yang ada di Dinas Komunikasi dan Informatika Kota Salatiga untuk akses hiburan, informasi, dan produktifitas. Hasil analisa risiko yang sudah di temukan. Berikut kondisi yang diharapkan serta tingkat risikonya pada Tabel 3.

Tabel 3. GAP Kondisi Yang Diharapkan dan Tingkat Risiko

Kategori	Risiko saat ini	Penyebab	Kondisi yang diharapkan	Tingkat risiko
Hardware	Kerusakan beberapa komponen, sempat berhenti produktifitas kerja dan beberapa komputer tidak terpakai	*Hardware* yang digunakan rata-rata merupakan mutasi dan ada yang memakai komputer sendiri	Akan lebih baik *hardware* yang sudah berumur atau lebih dari 7 tahun sebaiknya perlu lebih dipertimbangkan kembali	Tinggi
Keamanan	Sudah mencukupi walau sering terjadi ada beberapa barang atau aset yang hilang	Sering ada pengunjung yang mudah masuk ke kantor seperti contoh penjual hingga jasa yang tidak ada kepentingan dengan kedinasan	Walau sudah ada keamanan seperti alat pemadam kebakan akan lebih meningkatkan keamanan tambahan seperti sebuah CCTV	Tinggi
Software	Produktifitas sepat terhentikan karena kendala virus	Pernah sekali mengalamai *human error* atau lupa dalam *update* secara berkala sehingga *update* diubah ke mode manual	Perlunya kepada mereka yang Non IT untuk melakukan *update* pada komputer maupun laptop milik aset kantor yang mereka gunakan agar mereka yang IT produktifitas utama tidak terganggu	Sedang
Jaringan	Seringnya menerima komplain dari dinas lain	Dikarenakan *server* yang sering bermasalah	Lakukan *maintenance* setidaknya seminggu sekali untuk menghindari hal-hal yang tidak diinginkan	Sedang

5. SIMPULAN DAN SARAN

Dinas Kominfo Kota Salatiga sudah terbilang cukup baik.hanya saja perlu diperhatikan banyak sekali. Seperti pada Tabel 3, kondisi yang diharapkan keamanan yang sangat rentan pada aset sehingga berisiko tinggi pada Dinas Kominfo Kota Salatiga sendiri. Untuk *hardware* perlu sekali ditinjau ulang sehingga tidak menganggu

produktifitas yang ada di Dinas Kominfo Kota Salatiga. Sedangkan *software* perlu juga dibuat serutin mungkin agar ketika dinas lain akan mengakses atau ingin memasukkan data ke Dinas Pemerintahan Kota Salatiga tidak terjadi kendala. Di samping itu perlu juga memanfaatkan barang secara penuh dikarenakan beberapa aset penting seperti beberapa komputer yang menjadi tidak terpakai lagi karena memakai laptop maupun *gadget* tersendiri. Dengan penelitian ini dengan harapan bisa menjadi acuan sebagai alat yang membantu memperbaiki kekurangan yang ada di Dinas Kominfo Kota Salatiga

6. DAFTAR RUJUKAN

[1] Turban, Efraim. et al, 2003. *Introduction to Information Technology*. 2nd ed. England: John Wiley and Sons, Inc.

[2] Rainer, R. K., Turban, E., & Potter, E, 2009. *Introduction to Information Systems: Supporting and Transforming Business (International Student Version)*. New York: John Wiley & Sons.

[3] Anderes, G., Sanyoto, G., Irvan,T., 2008. *Pengukuran risiko teknologi informasi (TI) dengan metode Octave-S*. Jakarta Barat: Universitas Bina Nusantara.

[4] Syaharullah, D., 2012. *Analisis risiko keamanan sistem informasi AKBA Makassar menggunakan metode Octave-S*. Makassar: STMIK AKBA Makassar.

[5] Alberts, C., dan Dorofee., 2003. *Managing Information Security Risks: The OCTAVE (SM) Approach*. Boston: Addison-Wesley Professional.

[6] Department Of the Prime Minister and Cabinet, 2002. *Security The Government Sector Information Technology Security Policy Handbook*, Chapter 3 Asset Classification and Control.

[7] Haag, Cummings, Cuberry, C., 2005. *Management Information Systems for the Information Age*, 5th ed. New York: McGraw-Hill.

Halaman ini sengaja dikosongkan.