e-ISBN 978-623-93343-4-5
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 15 September 2021

Analisis dan Mitigasi Resiko Teknologi Informasi dan Keamanan Informasi Menggunakan Framework Octave Allegro (Studi Kasus : Perusahaan Percetakan Documedia)

Yudin[1], Kraugusteeliana [2], Rafli Ramadhan[3] Muhammad Restu Alfiansyah[4]
Sistem Informasi, Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia
yudin@upnvj.ac.id[1], gusteeliana@gmail.com[2], raflir@upnvj.ac.id[3], m.restualfi@upnvj.ac.id[4]

Abstrak. Saat ini teknologi sangatlah berkembang dengan pesat. Begitu juga dengan perkembangan teknologi dan sistem informasi pada perusahaan semakin pesat, cara pelayanan dalam sebuah perusahaan juga selalu terkomputerisasi. Lambatnya pelayanan dalam sistem didalam suatu perusahaan dapat mengurangi ketertarikan konsumen serta data yang tidak terorganisir menyebabkan proses bisnis yang ada dalam sebuah peusahaan menjadi tidak terkontrol dan tidak ter integrasi antara jobdes satu dengan yang lainnya. Documedia merupakan sebuah perusahaan yang bergerak di bidang percetakan. Untuk mengantisipasi hal-hal yang tidak diinginkan berkaitan dengan cara pelayanan dan pengerjaan yang tidak terorganisir maka dilakukan managemen resiko. Penilaian risiko dan juga mitigasi risiko menggunakan framework *OCTAVE Allegro* yang terdiri dari tiga fase dengan pengumpulan data menggunakan wawancara terhadap 4 orang informan. Hasil dari penilaian mengungkapkan bahwa instansi tidak menerapkan praktek keamanan yang baik sehingga memiliki kelemahan di beberapa area. Strategi perlindungan instansi kurang berjalan baik dikarenakan pegawai belum mendapatkan pelatihan mengenai keamanan informasi.

Kata Kunci : Teknologi, *Documedia*, *OCTAVE Allegro*

1 Pendahuluan

Aset didefinisikan menjadi asal daya ekonomi yang dikuasai atau dimiliki pemerintah menjadi dampak berdasarkan insiden masa kemudian dan berdasarkan mana manfaat ekonomi atau sosial pada masa depan dibutuhkan bisa diperoleh, baik pemerintah juga warga, dan bisa diukur pada satuan uang, termasuk asal daya non keuangan yang diharapkan untuk penyediaan jasa bagi warga generik dan asal-asal daya yang dipelihara lantaran alasan sejarah dan budaya termasuk aset bersejarah.

Berdasarkan uraian diatas, asset yang digunakan melebihi satu tahun akan mengakibatkan risiko pemakaian ataupun risiko kecerobohan yang akhirnya mengakibatkan kerugian pada perusahaan. Jadi, secara umum risiko dapat diatasi dengan manajemen risiko yang baik, pengawasan suatu risiko dan juga perlindungan aset perusahaan merupakan hal yang utama dikarenakan dapat menimbulkan masalah yang cukup berisiko. Seperti kehilangan aset data perusahaan dan yang lebih membahayakan perusahaan adalah dapat bangkrutnya perusahaan atau jatuhnya perusahaan tersebut.

percetakan, perusahaan ini memiliki bisnius percetakan yang menitik beratkan pada pembuatan stiker. Tidak hanya itu, documedia juga melayani percetakan bender dan x bender yang memiliki ukuran maximal 5 X 5 meter, memiliki pemimpin perusahaan dengan 7 orang staf tetap yang masi ada orang yang melakukan double job dari costumer service dan bagian produksi, sterta control terhadap asset dalam perusahaan yang belum termanagemen dengan baik.

Pada setiap perusahaan yang memiliki proses bisnis perlu dilakukan menejemen resiko untuk mengetahui dan memenejem resiko yang ada. Dengan adanya menejen resiko ini pada sistem perusahaan Documedia dapat meningkatkan sistem informasi dalam proses bisnis dan meningkatkan hasil produksi.

2 Landasan Teori

2.1 Operationally Critical Threat, Aset, and Vulnerability Evaluation (OCTAVE)

Pendekatan terhadap system untung meningkatkan keamanan informasi serta evaluasi terhadap resiko yang bisa saja terjadi sewaktu waktu adalah hal yang harus dilakukan oleh suatu perusahaan atau organisasi, Operationally Critical Threat, Aset, and Vulnerability Evaluation atau (*OCTAVE)* merupakan suatu framework yang memiliki banyak manfaat untuk menanggulangi risiko yang terjadi atau pun penanggulangan resiko yang dapat terjadi di sebuah perushaan, manfaat dari *OCTAVE* itu sendiri antara lain seperti pengembangan terhadap evaluasi resiko, identifikasi asset, kerentanan dan ancaman terhadap asset, dan menentukan keputusan atau arahan bagi pemimpin perusahaan untuk mengambil Tindakan terbaik atau langkah terbaik bagi perushaan kedepannya.

2.2 Operationally Critical Threat, Aset, and Vulnerability Evaluation Allegro

Salah satu metode yang dapat digunakan untuk menanggulangi resiko salah satunya adalah Operationally Critical Threat, Aset, and Vulnerability Evaluation Allegro dibentuk *Carniege Mellon University Software Engineering Institute* (SEI). Salah satu kelebihan dari metode OCTAVE adalah evaluasi resiko yang difokuskan serta di perkuat, dengan menejemen investasi yang minim gpada pusat atau asal daya dan bahkan bagi organisasi yang tidak memiliki kualitas menejemen resiko yang tinggi. Pendekatan ini berbeda dari pendekatan *OCTAVE* sebelumnya menggunakan serius terutama dalam aset fakta pada konteksnya tentang bagaimana aset fakta tadi dipakai, penyimpanan, distribusi, diproses, dan bagaimana hal tadi terkena ancaman, kerentanan, serta gangguan tersebut dapat terjadi.

Seperti metode sebelumnya, *OCTAVE Allegro* bisa dilakukan pada gaya tempat karya, pengaturan kolaboratif dan di dukung menggunakan panduan, lembar kerja, dan informasi lapangan, yang termasuk pada lampiran dokumen ini. Namun, *OCTAVE Allegro* juga cocok untuk dipakai individu yang ingin melakukan risiko penilaian tanpa keterlibatan, keahlian, atau masukan organisasi yang luas. Tahapan yang terdapat dalam *OCTAVE Allegro* :

1. Langkah pertama
   Yang pertama adalah *Establish Risk Measurement Criteria* ini berfokus pada pengelompokan terhadap pengukuran dan memilih prioritas resiko dan dinilai seberapa penting hasil pengelompokan dari masing masing resiko terhadap perusahaan.

2. Langkah ke-Dua
   Selanjutnya ada *Develop an Information Aset Profile* pada tahapan ini yaitu membuat profil asset setelah dilakukannya identifikasi dari perusahaan terkait dan dibuatlah kriteria dari masing – masing aspek yang ada

3. Langkah ke-Tiga
   Kemudian ada *Identify Information Asset Containers* pada tahapan ini dilakukan identifikasi keamanan terhadap asset data dan menentukan cara untuk melindungi asset yang ada agar resiko terhadap data yang memiliki kemungkinan peretasandan penyalahgiunaan akibat tidak menentukan system bagaimana data yang di simpan baik data internal maupun external perusahaan dapat disimpan dan di lindungi.

4. Langkah ke-Empat
   Selanjutnya *Identify Areas of Concern* pada tahapan ini dilakukan komponen apasaja yang memiliki resiko dan dikoordinasikan pada staf terkait agar dapat dikelompokan bagian apa saja yang memilikin resiko terhadap keamanan asset yang kemungkinan dapat terjadinya penyerangan terhadap data primer perusahaan.

5. Langkah ke-Lima
   Selanjutnya ada Identify Threat Concern, dalam tahapan ini dialakukan identifikasi asset yang dapat diserang sewaktu – waktu dan menjabarkan sekenario dari pengisian informasi dari pihak internal terkait

fakta yang terjadi di lapangan dan melengkapi Information Asset Risk Worksheets dari sekenario yang sudah diketahui oleh pihak internal perusahaan

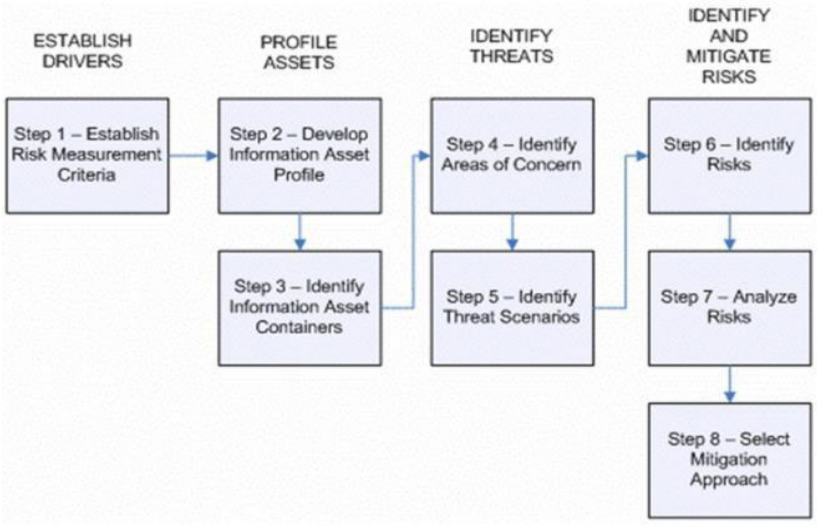
6. Langkah ke-Enam
   Selanjutnya ada *Identify Risks* ditahapan ini mulai dilakukan pemfokusan apasaja resiko yang mempunyai konsekuensi tinggi terhadap asset yang ada. Secara nilai di dalam taber ini kemungkinan resiko terjadi cukup besar dan di perlukannya penanggulangan yang lebih serius.

7. Langkah ke-Tujuh
   Selanjutnya ada *Analyze Risks* pada tahapan ini pengelompokan dari didentifikasi atau output dari identifasi sebelumnya mulai di evaluasi yang dapat mempengaruhi pada dokumentasi pada *Information Asset Risk Worksheet*. Lalu dilakukannya peninjauan terhadap *Risk Measurement Criteria*, lalu dilakukan penilaian seberapa besar nilai resiko relativ dan pertimbangan apakah konsekuensi dari resiko tersebut dapat berdampak pada perusahaan dari pertimbangan yang telah dilakukan di tahapan sebelumnya.

8. Langkah ke-Delapan
   Langkah yang terakhir adalah Select Mitigation Approach Pada tahapan terakhir ini, adalah evaluasi yang merupakan tahapan terakhir dari penilaian resiko yang ada pada tahapan ke-tujuh dan menentukan nilai Pool dari penilaian sebelumnya dari resikoi pada perusahaqan terkait.

3 Metode Penelitian

Untuk memecahkan permasalahan serta yang ada pada perusahaan ini, agar dicapainya tujuan penelitian terhadap resiko yang ada pada perusahaan docomedia ini kami memilih metodeogi menggunakan metode *OCTAVE Allegro*:



Gambar. 1.

Hasil akhir ini bertujuan untuk rancangan menejemen resiko, penilaian resiko, pengelompokan prioritas resiko, serta mitigasinya terhadap perusahaan documedia.

4 Analisis Dan Perancangan

Berikut delapan langkah Octave Allegro untuk menanggulangi resiko pada perushaan documedia

4.1 Kriteria Pengukuran Risiko

Di tahapan awal ini adalah *organizational driver* pada tabel ini digunakan untuk mengevaluasi dampak yang akan terjadi pada perusahaan dilihat dari usaha perusahaan untuk menanggulangi resiko yang ada dari masing masing area yang di identifikasi. Di dalamnya masih ada berukuran – berukuran kualitatif yg risikonya bisa dinilai dan menciptakan dasar berdasarkan evaluasi risiko sistem informasi. Dari area yg berdampak rendan, sedang dan tinggi antara lain adalah:

Tabel 1. Membangun Kriteria Pengukuran Risiko

Table 1	Dampak Area Utama
Prioritas	Area Terdampak
Prioritas Rendah = 2	Terkait Kepercayaan Karyawan Perusahaan
Prioritas Rendah = 1	Terkait Keuangan
Prioritas Sedang = 3	Terkait Produktivitas
Prioritas Tinggi = 5	Terkait Keselamatan dan Kesehatan
Prioritas Tendah = 4	Terkait Denda dan Pinalti

4.2 Membangun Profil Aset Informasi

Langkah ke 2 merupakan menciptakan profil aset keterangan pada asset yang ada pada perusahaan.. Metode ini difokuskan untuk menilai kerentanan serta *konsistenitas* terhadaf pendefinisian yang tidak jelas menurut batasa terhadap asset yang ada pada perusahaan serta Menyusun apasaja kebutuhan untuk keamanan pada asset yang ada.

Tabel 2. Membangun Profil Aset Informasi

Table 4.2	Profile Aset Kritis	
Kritikal aset	Rasional seleksi	Deskripsi
Server	Lantaran server berfungsi menjadi penggerak atau induk berdasarkan seluruh data *documedia* yang didapatkan diantaranya penyimpan pelaksanaan dan database yang terdapat dalam *komputerisasi* personal personal yang terkait pada system yang ada serta memfasilitasi keamanan pada computer yang yang terhubung pada *documedia*	Melakukan pengamanan data perusahaan yang merupakan data bisnis dan treansaksi yang dilakukan.
Pemilik Documedia		
Persyaratan keamanan		
Kerahasiaan	Yang dapat mengakses data utama *documedia* ini adalah karyawan tertentu yang dapat mengakses data :	Tim depelopme system, bagian IT documedia, pemilik Vendor, bagoan keuangan dan Transaksi
Integritas	Yang dapat mengakses data utama *documedia* ini adalah karyawan tertentu yang dapat mengakses data :	Bagian IT documedia, pemilik Vendor, bagoan keuangan dan Transaksi

Ketersediaan	Jaminan bagi asset ini untuk seluruh bagian vendor ini harus tersedia setiap saat pada jam kerja Documedia.	Menejemen webserfer terkait resiko server yang eror saat di akses dan tidak bisa di akses

4.3 Mengidentifikasi Container Dari Aset Informasi

Container merupakan loka dimana aset fakta disimpan, dikirim, dan diproses. Dalam langkah ketiga, seluruh container yg menyimpan, mengirim, & memproses, baik internal juga eksternal diidentifikasikan. Diantaranya Identifikasi (pemetaan) risiko lingkungan aset kritis (Teknikal), Identifikasi (pemetaan) risiko lingkungan aset kritis (Fisik), dan Identifikasi (pemetaan) risiko lingkungan aset kritis (Karyawan). Yang berkaitan menggunakan vendor, pemilik, menejer IT & pihak pendukung lainnya.

4.4 Mengidentifikasikan Area Yang Diperhatikan

Pada tahapan ini, melakukan identifikasi resiko pada pada system yang berjalan di perusahaan terkait kondisi dan situasi yang ada saat ini, dan menentukan Langkah selanjutnya yang harus di ambil oleh perusahaan terkait resiko yang ada. Disini perusahaan mengambil keputusan untuk membuat tim analis untuk menjelaskan kondisi terkini pada perusahaan documedia.

4.5 Mengidentifikasi Skenario Ancaman

Selanjutnya dilakukan pembuatan sekenario ancaman yang telah didapat dari area – area yang di sebutkan oleh tim analis. Selanjutynya menterjemahkan dan mengelompokan menggunakan *Treat tree*. Langkah ini diambil untuk untuk pertimbangan perusahaan dilihat dari sekenario ancaman yang telah di identifikasi sebelumnya dan dibagi pada kelompok rendah, sedang, ataupun tinggi.

Tabel 3. Identifikasi Skenario Ancaman

Table 5	Pengelompokan Resiko Aset Kritis	
Ancaman	Aset kritis	Kerentanan
	Area Objek	Manipulasi data utama dan data transaksi Keamanan data utama dan data transaksi
	User	Administrator IT infrastuktur Eksternal/ vendor
	Cara	Melakuan pencurian data perusahaan dengan cara Mengambil data secara Berkala dan meanfaatkan akses yang dimiliki pihak internal berupa data transaksi dan data master perusahaan Documedia. Mengambil dan menyebarkan data perusahaan untuk kepentingan individu.
	Dorongan	Human error Kesengajaan untuk keuntungan pribadi
	Keluaran	Destruksi Manipulasi
	Persyaratan keamanan	Merencanakan Pembackupan data perusahaan secara berkala yang terjadwal menggunakan donasi setting menggunakan system dan menyetel ulang agar system melakukan penolakan secara otomatis untuk data yang ada sebelumnnya. Adanya mitra Perusahaan dengan pihak yang ahli terkait pengamanan system dengan Vendor External yang Tersertifikasi *Treckrecord*-nya Secara hukum

4.6 Mengidentifikasi Risiko

Pada tahapan ini, Memberikan kosekuensi terhadap Documedia untuk mencatat apa saja amcaman yang serting terjadi pada perusahaan. Agar penenerima citra risiko dapat mendapatkan informasi secara lengkap. Sebuah ancaman bisa memiliki dampak – dampak yang potensial bagi organisasi. Area dampak ini diperoleh dari hasil wawancara terhadap karyawan dan pelanggan *documedia* yang akhirnya didapatkan nilai-nilai dampak dengan menggunakan *OCTAVE allergo* dan didapatkan area dampak sebagai berikut.

Tabel 4. Area Dampak

Tabel 6	Prioritas	Nilai dampak		
		Rendah	Sedang	Tinggi
Terkait Keuangan	Pertama	10	15	25
Terkait Kepercayaan Karyawan Perusahaan	Ke-Dua	7	14	21
Terkait Produktivitas	Ke-Tiga	6	12	18
Keselamatan dan kesehatan	Ke-Empat	4	8	12
Terkait Denda dan pinalti	Ke-Lima	2	4	6

4.7 Menganalisis Risiko

Selanjutnya dilakukan pengukuran secara kuantitatif untuk menghitung kemungkinan dampak yang didapat perusahaan Documedia derdasarkan threat yang telah di hitung sebelumnya, nilai relative ini didapat dari pengukuran dari kensekuensi resiko yang ada terhadap system dari dampak yang di hasilkan jika terjadi pada perusahaan *documedia*.

Tabel 5. Nilai Risiko Relatif

Tabel 7	Risiko			
Perubahaan yang terjadi diantaranya: perubahan data master dan data Transaksi yang ada pada Documedia.	Konsekuensi	Diperlukan kecakapan spesifik dan perhatian lebih jelasnya dalam mengerjakan back-up data		
	Kerentanan	Area terdampak	Nilai	skor
		Sektor Keuangan	Tinggi	25
		Kepercayaan Karyawan Perusahaan	Sedang	21
		Sektor Produktivitas	Sedang	18
		Sector Keselamatan dan kesehatan	Sedang	12
		Sektor Denda dan pinalti	Rendah	6
		Total		82

4.8 Memilih Pendekatan Pengurangan Risiko

Dalam langkah terakhir menurut proses Octave Allegro ini, Documedia memilih risiko yang memerlukan mitigasi dan membuatkan taktik untuk mengurangi risiko tersebut. Hal ini dilakukan menggunakan cara memprioritaskan risiko – risiko menurut nilai risiko relatif, lalu membuatkan taktik mitigasi menggunakan mempertimbangkan nilai menurut aset dan kebutuhan keamanan, kontainer atas aset, dan lingkungan operasional yang unik menurut Documedia.

Tabel 6. Skor Risiko

Pool	Pendekatan Mitigasi

20 - 35	Harus dilakukan Mitigasi
10 - 19	Memberikan Pilihan Pada Pihak vendor untuk memilih Mitigasi atau ditangguhkan
0 - 10	Mitigasi Diterima

Tabel 7. Mitigasi

Mitigasi Aset Risiko Yang ada di Documedia	
Area perhatian	Perubahaan yang terjadi diantaranya: perubahan data master dan data Transaksi yang ada pada Documedia.
Tindakan	Harus dilakukan Mitigasi
Kontainer	Melakukan control terkait asset yang ada serta pemilihan metode keamanan data yang sesuai dan Tersertyifikasi secara hukun
Kerentanan	Memilih vendor dari pihak external yang tepat untuk penyimpanan dan difasilitasi oleh jaminan back-up data secara berkala dan memiliki jaminan keamanan data dan meningkatkan kualitas pemegang data server yang tepat dari pihak internal.
TI depelopmen Perusahaan	Mengontrol semua aspek IT terkait TRansaksi Dan control Web-Server yang digunakan perusahaan serta mencatatan masalah dari Sistem agar Perusahaan bisa mengambil Tindakan yang lebih serius.

5 Kesimpulan

Berdasarkan uraian pembahasan terkait sistem informasi pelayanan di perusahaan documedia dapat di tarik kesimpulan bahwa :

a) Melakukan manajemen risiko dari identifikasi masalah, pengukuran masalah, dan kontrol keuangan, data perusahaan, serta produktivitas berdasarkan risiko-risiko yang telah dilakukan penilaian risiko serta mitigasi risiko yang ada pada perusahaan documedia
b) Dengan menerapkan manajemen risiko pihak manajemen dapat mengetahui dampak ancaman, kerawanan dan akibat dari masing-masing aset yang ada pada perusahaan documesia.
c) Dengan menggunakan metode octave allegro, penelitian evaluasi risiko lebih terarah atau difokuskan pada bagian ancaman (threat) dan kelemahan (vulnerability) berdasarkan aset yang dimiliki perusahaan documedia.

Referensi

[1] Lenawati, M. and Winarno, W.W., 2017. Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. Speed-Sentra Penelitian Engineering dan Edukasi, 9(1).
[2] Pratama, R., Syamsuar, D. and Kunang, Y.N., 2018, October. Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S. In Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK) (Vol. 1, No. 1, pp. 147-152).
[3] Hasibuan, S.I., Kusumasari, T.F. and Fauzi, R., 2019. Analisis Risiko Keamanan Informasi Dengan Metode Octave Allegro Pada Pt. Tirta Investama. eProceedings of Engineering, 6(2).
[4] Lenawati, M. and Winarno, W.W., 2017. Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. Speed-Sentra Penelitian Engineering dan Edukasi, 9(1).
[5] Pratama, R., Syamsuar, D. and Kunang, Y.N., 2018, October. Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S. In Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK) (Vol. 1, No. 1, pp. 147-152).
[6] Bekasi, D., 2021. DocuMedia Bekasi. [online] Documedia-bekasi.business.site. Available at: https://documedia-bekasi.business.site.
[7] Soleiman, I.D., and Maria 2019. PERLAKUAN AKUNTANSI UNTUK ASET BERSEJARAH PADA SITUS BUNG KARNO KABUPATEN ENDE. (Vol. 09, No 02).