AUDIT KEAMANAN SISTEM INFORMASI KANTOR BAPPEDA KABUPATEN SLEMAN

Andriyan Dwi Putra[1], Wing Wahyu Winarno[2], Roy Rudolf Huizen[3]
[1,3] Magister Teknik Informatika STMIK AMIKOM Yogyakarta
[2]STIE YKPN Yogyakarta
E-mail: [1]ndre.bekool@gmail.com,[2]maswing@gmail.com,[3]royrudolf.usm@gmail.com

ABSTRAK

Pencegahan dapat menghindarkan dari timbulnya kejahatan, kerugian yang besar, atau biaya yang besar dalam upaya melakukan deteksi terhadap sistem informasi yang rentan terhadap celah keamanan (security hole) sistem informasi. Untuk mengelola risiko yang mungkin terjadi terhadap sistem informasi BAPPEDA Kabupaten Sleman, perlu dilakukan audit sistem informasi dalam konteks risiko, guna mengurangi kerugian kerugian yang mungkin terjadi pada sistem informasi BAPPEDA Kabupaten Sleman. Metode OCTAVE-S digunakan dalam penelitian ini karena metode tersebut mampu mengelola risiko dan mengenali tingkat risiko yang mungkin terjadi pada sebuah sistem informasi. Dan berdasarkan analisa OCTAVE-S maka mendapatkan hasil bahwa masih ada beberapa praktek keamanan yang perlu mendapatkan perhatian khusus yaitu sistem crash dan kode berbahaya pada bagian sistem 22,67% faktor kesengajaan pada akses fisik rata- rata 21% , akses jaringan rata- rata 24,51%, dan masalah pihak ketiga pada faktor lainnya sebesar 15,17%. Dengan hasil tersebut, maka dibuatlah saran/ rekomendasi pengamanan rekomendasi/ saran pemantauan dan audit keamanan fisik, rekomendasi/ saran pengamanan sistem informasi, rekomendasi terkait akses jaringan dan kebijakan masalah pihak ketiga. Dengan harapan dapat membantu pihak BAPPEDA mengurangi tingkat resiko yang dihadapi.

Kata Kunci*— Audit, BAPPEDA Sleman, OCTAVE-S*

ABSTRACT

The prevention is able to avoid the crime, many losses or costs in the detection of vulnerable information system for security hole of information system. To manage the possible risk of information system in BAPPEDA Sleman, It is necessary the audit of information system in the context of risk for reduce the risks of the information system in BAPPEDA Sleman. This research is using OCTAVE-S method because it is able to manage the risks and identify the level of risk that possible found in an information system. And based on the analysis by OCTAVE-S method, the results are; there are still some security practices that need special attention, namely; a crash system and malicious code of system is 22.67%. Intentional factor's average of physical access is 21%, the average of network access is 24, 51%, and the problem of third parties in the other factors is 15.17%.By the results, the suggestion /safety recommendation, recommendation/ monitoring suggestion and physical security audit, recommendation/ suggestion securing information system, recommendation regarding network access and third party policy issues are made. Hopefully, those can help BAPPEDA to reduce the risks.

Keywords*— Audit, BAPPEDA Sleman, OCTAVE-S*

PENDAHULUAN

Sistem Informasi saat ini merupakan sumber daya yang sangat penting, mempunyai nilai yang tinggi. Kemudahan dan keuntungan dapat kita rasakan dengan diimplementasikannya sistem informasi. Tetapi perlu disadari bahwa semakin banyak sistem informasi yang diterapkan, semakin banyak sistem informasi yang rentan akan ancaman[1].

Mengingat pentingnya informasi, maka kebijakan, prosedur dan mekanisme pengamanan sistem informasi harus mampu menjamin informasi yang ada didalamnya dapat terlindungi dengan baik dari ancaman yang sewaktu waktu bisa terjadi[2]. Oleh karena itu untuk mengelola risiko yang mungkin terjadi terhadap sistem informasi BAPPEDA Kabupaten Sleman, perlu dilakukan audit

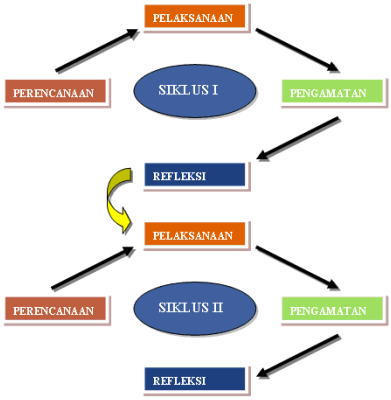
sistem informasi dalam konteks risiko, guna mengurangi kerugian kerugian yang mungkin terjadi pada sistem informasi BAPPEDA Kabupaten Sleman

Pramudya, pada tahun 2013 tentang Pengukuran Risiko Teknologi Informasi Pada Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Menggunakan Metode OCTAVE-S juga mendapatkan hasil atau simpulan. Diantaranya adalah dari lima belas praktek keamanan Instansi Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi memiliki tiga kelemahan yang berada pada area merah tersebut yaitu dalam hal : Kebijakan Keamanan, Pengesahan dan Otorisasi, serta Manajemen Insiden[3].

Disa juga meneliti tentang analisis risiko keamanan sistem informasi akademik STMIK AKBA Makasar dengan metode OCTAVE-S. Menghasilkan Persentase total risiko (dengan klasifikasi) sebesar 44,8. Sedangkan Persentase total risiko (tanpa klasifikasi) sebesar 67,3. Dengan hasil persentasi tersebut, maka dapat dikatakan bahwa tingkat keamanan sistem informasi pada STMIK AKBA makassar tergolong sedang[4].

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian kali ini adalah metode penelitian tindakan. Penelitian tindakan sering juga disebut *action research* dikarenakan penelitian ini menuntut untuk bisa mendeskripsikan, mengintepretasikan, dan menjelaskan pada suatu situasi, dimana pada waktu yang bersamaan juga melakukan perubahan dengan tujuan atau *goal* sebuah perbaikan. Pandangan tradisional action research bisa dijabarkan sebagai suatu kerangka penelitian pemecahan masalah, dimana akan terjadi kombinasi atau kolaborasi antara peneliti dengan objek/ *client* dalam rangka mencapai sebuah tujuan [5]. Ada empat langkah yang ada dalam metode penelitian tindakan, perencanaan, tindakan, pengamatan dan penilaianp[6]. Ke empat langkah tersebut dilakukan secara sistematis. Dalam penelitian lain kembali ke perencaan merupakan hal yang mutlak jika terjadi atau ditemukan hasil yang belum sesuai, namun hal yang spesial saat melakuan penelitian audit, karena ketidak sesuaian merupakan temuan bagi penelitian ini untuk membuat rencana mitigasi.



Gambar 1. Alur *action research* [7]

2.1 Metode Analisis Data

Untuk melakukan analisis lingkungan internal dan eksternal diperlukan metode analisis yang tepat dan sesuai, sehingga nantinya akan memudahkan dalam Ada banyak metode analisis yang bisa dipakai sesuai dengan kebutuhan dalam hal ini kaitannya dengan sistem informasi. Dalam penelitian ini, menggunakan metode OCTAVE-S. Metode ini dinilai tepat untuk penggunaannya dan sesuai dengan beberapa referensi yang ada serta sejalan dengan tahapan-tahapan yang ada pada framework OCTAVE.

2.2 Pengenalan metode OCTAVE-S

Hal yang terpenting dalam sistem informasi adalah informasi yang terkandung didalamnya, tidak terkecuali bagi pemerintah. Sistem informasi menyimpan banyak data yang sangat vital,oleh sebab itu maka diperlukannya pengamanan terhadap asset yang dimiliki. Namun pemerintah yang menjalankan strategi pengamanan infrastruktur seringkali masih kecolongan karena memang dampak tingginya tingkat ancaman. Banyak pendekatan manajemen risiko keamanan informasi yang tidak lengkap atau kurang searah dengan masalah yang dihadapi, sehingga gagal dalam mencakup seluruh komponen risiko (aset, ancaman, dan vulnerability)

Langkah pertama untuk mengelola risiko keamanan sistem informasi adalah mengenali terlebih dahulu pemerintah yang menerapkan sistem informasi tersebut. Setelah risiko diidentifikasi, pemerintah dapat membuat rencana penanggulangan terhadap risiko yang telah diketahui. Metode OCTAVE-S (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation*) memungkinkan sebuah organisasi/pemerintah melakukan hal diatas. OCTAVE-S adalah sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif, sistematik, terarah, dan dilakukan sendiri. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informas [8].

2.3 Tahapan Metode OCTAVE-S

Menurut Alberts, C dan Dorofee.A, OCTAVE-S mempunyai 3 tahapan terpenting yang telah terdeskripsi. Pada bagian ini memberikan penjelasan singkat atas tahapan, proses,dan kegiatan dari OCTAVE-S itu sendiri. Dalam tahap ini terdiri atas 2 proses, yaitu identifikasi informasi organisasi/ perusahaan dan membuat profil ancaman serta memiliki enam aktivitas [9].

Framework OCTAVE-S dapat dijabarkan menjadi 3, yang pertama adalah membangun aset berbasis profil ancaman.

Tahap pertama adalah sebuah mengevaluasi dari segi aspek organisasi. Selama dalam tahap ini, bagian ini menggambarkan kriteria dampak dari evaluasi yang akan digunakan nantinya untuk mengevaluasi risiko perusahaan. Tahapan ini juga mengidentifikasi aset-aset organisasi atau perusahaan yang penting, dan mengevaluasi praktek keamanan dalam organisasi ataupun perusahaan saat ini. Dalam hal ini menyelesaikan tugasnya sendiri dan mengumpulkan informasi tambahan jika hanya diperlukan. Selanjutnya memilih 3 dari 5 aset kritikal untuk menganalisa dasar kedalaman dari hubungan penting dalam organisasi tersebut. Pada akhirnya dalam tahapan ini, tim menggambarkan kebutuhan - kebutuhan keamanan dan menggambarkan profil ancaman pada setiap aset yang dimiliki.

Tahapan kedua identifikasi kerentanan infrastruktur, analisis melakukan peninjauan ulang langsung dari sebuah perhitungan infrastruktur organisasi maupun perusahaan yang bersangkutan, yang berfokus pada keamanan yang dipertimbangkan pemeliharaannya dari infrastruktur. Tugas pertama adalah menganalisis bagaimana orang-orang menggunakan sumber daya infrastruktur komputer pada akses aset kritis dan menghasilkan kunci (*key*) dari komponen-komponen. Tahapan ini memiliki sebuah proses yaitu memeriksa perhitungan infrastruktur dalam kaitannya dengan aset yang kritis dimana

terdapat 2 aktivitas [10]. Dari hasil analisis tersebut, penulis memasukkan hasil dari analisis kedalam kertas kerja *security practice.* Evaluasi praktek keamanan ini dilakukan penulis menggunakan framework atau kertas kerja yang telah disediakan OCTAVE-S yaitu kertas kerja *Security Practices*, tapi dengan *customized* / penyesuaian dengan batasan dan tujuan penelitian, sehingga dapat dihasilkan aspek keamanan yang mendukung proses bisnis di BAPPEDA Kabupaten Sleman.

Tahapan yang ketiga atau yang terakhir adalah Pengembangan Strategi Keamanan dan Perencanaan, penulis mengidentifikasi risiko dari aset kritis organisasi ataupun perusahaan dan memutuskan apa yang nantinya harus dilakukan terhadap hasil identifikasi. Berdasarkan analisis dari kumpulan informasi, tim penulis membuat strategi perlindungan kedepannya untuk organisasi ataupun perusahaan dan rencana mitigrasi risiko yang ditujukan pada aset kritis. Kertas kerja OCTAVE yang digunakan dalam seluruh tahapan ini mempunyai struktur yang tinggi dan berhubungan erat dengan praktek katalog OCTAVE, sehingga memungkinkan untuk menghubungkan saran untuk meningkatkan praktek keamanan dari hasil lain.

HASIL DAN PEMBAHASAN

3.1. Gambaran Umum Sistem Informasi BAPPEDA

Sekilas tentang gambaran tentang sistem informasi BAPPEDA, sistem informasi BAPPEDA yang dijadikan obyek penelitian adalah sistem informasi website dengan penanggung jawab adalah KOMINFO. BAPPEDA diberi kewenangan oleh KOMINFO untuk mengelola sub domain (bappeda.slemankab.go.id), pengelolaan website BAPPEDA yang ada saat ini adalah seputaran memberikan informasi hal yang berkaitan langsung dengan BAPPEDA seperti agenda kegiatan, berita, izin penelitian, hasil penelitian, pengumuman penting, dan lain- lain. Website BAPPEDA juga memberikan menu buku tamu untuk interaksi (tanya jawab) masyarakat dengan pihak BAPPEDA.

Gambar 3.2 Halaman Utama (*bappeda.slemankab.go.id*)

Admin/ pengelola dari Website BAPPEDA dibantu beberapa wakil dari bidang yang berada di kantor BAPPEDA untuk mengupload/ mengupdate informasi terkait berita tentang BAPPEDA. Beberapa bidang yang diberi kewenangan untuk membantu Admin adalah bidang sarana dan prasarana, bidang data informasi dan statistik, bidang ekonomi, bidang sosial dan pemerintahan, bidang pengendalian dan evaluasi,dan sekretariat. Perbaruan informasi dilakukan berdasarkan bidang, dan untuk bidang yang belum diberikan kewenangan, informasi dikirim manual ke admin BAPPEDA. Selanjutnya Admin melakukan pengecekan (*checking*) 3x sehari untuk informasi terbaru (pertanyaan, peminat informasi, ijin penelitian, dll).

3.2 OCTAVE-S

Hasil analisis menggunakan Metode OCTAVE-S ini nantinya adalah berupa temuan, prosentase risiko yang dihadapi, dan tindakan mitigasi terhadap hasil temuan dengan metode OCTAVE-S. analisis OCTAVE-S bisa dilihat dalam 3 fase pada bahasan selanjutnya.

3.2.1 Membangun Profil Ancaman

Pada proses ini menggunakan kertas kerja Establish *Impact Evaluation Criteria* untuk menentukan range dari sebuah dampak risiko yang mungkin terjadi pada kantor BAPPEDA Kabupaten Sleman dan menetapkan ukuran (rendah, sedang, tinggi) sebagai tolok ukur. Tabel dibawah merupakan pendefinisian bobot yang dibangun.

Area dampak ditetapkan menggunakan parameter yang telah disediakan oleh OCTAVE-S (reputasi, customer loss, biaya operasi dan investigasi) dan untuk area dampak data loss dan availability ditentukan/ dibangun berdasarkan kasus website (dibangun sendiri).

Tabel 1. Kertas Kerja *Establish Impact Evaluation Criteria*

Lembar Kerja 1	**KRITERIA RISIKO PENGUKURAN**		
Area Dampak	**Rendah**	**Sedang**	**Tinggi**
Reputasi	Reputasi terpengaruh sedikit atau tidak adanya upaya atau beban yang diperlukan untuk memulihkan.	Reputasi rusak, dan beberapa usaha serta adanya beban yang diperlukan untuk mengembalikan	Reputasi tidak dapat ditarik kembali (hancur atau rusak)
Customer Loss	Kurang dari **1 %** penurunan pelanggan karena hilangnya kepercayaan	**2 %** sampai **7 %** penurunan pelanggan karena hilangnya kepercayaan	Lebih dari **9 %** penurunan pelanggan karena hilangnya kepercayaan
Biaya Operasi	Kenaikan kurang dari **50 %** biaya perbaikan sistem	Biaya perbaikan sistem meningkat **50% - 70 %**.	Biaya perbaikan sistem meningkat lebih dari **75 %**.
Data Loss	Kurang dari **1 %** data hilang	**3 % - 9 %** data hilang	Lebih besar dari **10 %** data hilang
Availability	Terganggunya sistem membuat sistem tidak bisa diakses **1 – 2** kali dalam setahun	Terganggunya sistem membuat sistem tidak bisa diakses **3 – 6** kali dalam setahun	Terganggunya sistem membuat sistem tidak bisa diakses lebih dari **10** kali dalam setahun
Investigasi	Tidak ada pertanyaan	Pemerintah atau organisasi	Pemerintah atau organisasi

	dari pemerintah atau investigasi lainnya dalam organisasi	investigasi lain meminta informasi atau catatan (rendah profil).	investigasi lain memulai praktek. investigasi mendalam sebuah organisasi (high profil)

3.2.2 Identifikasi Celah infrastruktur

Dokumentasi dan pencatatan aset kritis dilakukan penulis terkait komponen utama yang mendukung proses bisnis. Pencatatan dilakukan agar memudahkan melanjutkan ke langkah selanjutnya seperti penentuan Sumber Daya Manusia yang bertanggung jawab setiap komponennya. Penulis juga berusaha menilai seberapa amankah komponen yang terkait dengan pendukung proses bisnis. Dari pencatatan dan dokumentasi tersebut penulis mencoba menilai dengan kertas kerja *Security Practices* dan kertas kerja *Risk Profiles* sebagai langkah penilaian/ penentuan tingkatan keamanan sistem BAPPEDA.

Tabel 2. Elemen terkait

Elemen	Sub-elemen	Sumber Daya Manusia yang bertanggung jawab
Sistem	Web Server Sistem	Kepala Web Development
	Database sistem	
	Email Server	
	Network Sistem	
Informasi	User Information	Kepala Sistem Informasi BAPPEDA
Aplikasi dan Service	Aplikasi Web	Administrator
	Koneksi Internet	
	Email	

Analisis selanjutnya menggunakan kertas kerja *Network Access Paths.* Peneliti melakukan pengamatan langsung/ melihat bagaimana seorang staff atau karyawan BAPPEDA mengakses aset kritis.

Proses ini adalah mengidentifikasi elemen – elemen yang terkandung di web applikasi BAPPEDA. Bentuk identifikasi dipisah menjadi *internal access* dan *external access.* Tetapi dalam identifikasi kali inihanya *internal access* yang ada pada sistem informasi BAPPEDA. *Internal access* melipusi akses karyawan ke halaman administrator aplikasi web. Sementara itu *external access* adalah antarmuka yang diakses oleh masyarakat. Aplikasi web BAPPEDA dikelola oleh KOMINFO Kabupaten Sleman, segala data yang ada pada aplikasi web BAPPEDA tersimpan secara lokal di server lokal KOMINFO dan tersimpan *cloud/ online.* Aplikasi web BAPPEDA yang dikelola oleh KOMINFO terhubung melalui internet langsung, tidak melalui jaringan lokal. Sehingga jarak kantor BAPPEDA dan KOMINFO yang bisa dikatakan agak jauh bisa diminimalisir dengan akses internet langsung. Aplikasi web BAPPEDA mempunyai Web server dan Email server, sehingga masyarakat bisa melakukan kontak langsung dengan BAPPEDA tanpa curiga email palsu.

Impact evaluation criteria merupakan proses selanjutnya. Setiap tindakan yang dilakukan untuk menanggulangi risiko dicatatat dan di tinjau kembali agar pengolahan data benar – benar valid/ sama persis dengan keadaan yang ada saat ini. Level dampak dikelompokkan menjadi tiga : tinggi (H), sedang (M), dan rendah (L). Penetapan nilai kuantitatif pada tabel dampak risiko diberikan

pada setiap dampak, 100 untuk tinggi (H), 50 untuk sedang (M), dan 10 untuk rendah (L).

Tabel 3. Dampak Risiko

Area	Faktor			Reputasi	Customer loss	Biaya operasi	Data loss	Availability	Investigation
Sistem		sistem crash	kerugian/ kerusakan	M	H	H	L	L	L
			gangguan	M	H	H	L	L	L
		gangguan / cacat software	kerugian/ kerusakan	M	L	H	L	L	L
			gangguan	M	L	H	L	L	L
		gangguan / cacat hardware	kerugian/ kerusakan	L	M	H	L	L	L
			gangguan	L	M	H	L	L	L
		kode berbahaya	kerugian/ kerusakan	H	L	M	L	L	L
			gangguan	H	L	M	L	L	L
Akses Fisik	inside factor	tidak sengaja	perubahan	M	L	M	L	L	L
			kerugian/ kerusakan	L	L	L	L	L	L
			gangguan	L	M	M	L	L	L
	inside factor	sengaja	perubahan	H	M	M	H	L	L
			kerugian/ kerusakan	H	M	M	M	L	L
			gangguan	H	L	M	L	L	L
Akses Jaringan	inside factor	tidak sengaja	perubahan	M	L	M	L	L	L
			kerugian/ kerusakan	L	L	L	L	M	L
			gangguan	M	L	M	L	M	L
	inside factor	sengaja	perubahan	H	M	H	M	L	L
			kerugian/ kerusakan	H	L	H	M	M	L
			gangguan	H	L	H	L	M	L
	outside factor	sengaja	perubahan	H	M	H	M	M	L
			kerugian/ kerusakan	H	L	H	M	M	L
			gangguan	H	L	H	L	M	L
Faktor Lain		masalah komunikasi	kerugian/ kerusakan	M	M	L	L	L	L
			gangguan	M	M	L	L	L	L
		masalah pihak ketiga	kerugian/ kerusakan	L	L	H	M	L	L
			gangguan	L	L	H	M	L	L

Kertas kerja *Risk Profile* yang telah dibuat diawal memberikan informasi setiap risiko yang paling sering terjadi. Dengan mengevaluasi menggunakan *Frequency Evaluation Criteria* penulis menentukan nilai probabilitas risiko seperti terlihat pada tabel 4. Bobot probabilitas dibawah ditentukan untuk mendapatkan nilai yang bersifat kuantitatif. Bobot yang ditentukan oleh penulis adalah 0,1 untuk bobot terendah (L), 0,5 untuk bobot sedang (M), dan bobot tertinggi diberikan nilai 1,0. Penetuan bobot digunakan untuk

pengolahan matrik dampak risiko dan probabilitas risiko.

Tabel 4. Probabilitas Risiko

Sistem		sistem crash	kerugian/ kerusakan	M
			gangguan	M
		gangguan/ cacat software	kerugian/ kerusakan	L
			gangguan	L
		gangguan/ cacat hardware	kerugian/ kerusakan	L
			gangguan	L
		kode berbahaya	kerugian/ kerusakan	M
			gangguan	M
Akses Fisik	inside factor	tidak sengaja	perubahan	L
			kerugian/ kerusakan	L
			gangguan	L
	inside factor	sengaja	perubahan	M
			kerugian/ kerusakan	M
			gangguan	M
Akses Jaringan	inside factor	tidak sengaja	perubahan	M
			kerugian/ kerusakan	L
			gangguan	M
	inside factor	sengaja	perubahan	L
			kerugian/ kerusakan	L
			gangguan	M
	outside factor	sengaja	perubahan	M
			kerugian/ kerusakan	L
			gangguan	H
Faktor Lain		masalah komunikasi	kerugian/ kerusakan	L
			gangguan	L
		masalah pihak ketiga	kerugian/ kerusakan	M
			gangguan	M

‘

. Pencarian *risk exposure* didapat dari gabungan antara *impact* dan *probabilitas* yang telah dikonversi dan dibuat matrik. Maka dengan rumus tersebut, akan didapatkan matrix sebagai berikut

Tabel 5. Matrix Risiko

				reputasi		kehilangan pelanggan		biaya operasi		Data Loss		Availibility		investigation		risk exposure	
				impact	prob	impact	prob	impact	prob	impact	prob	impact	prob	impact	prob		
Sistem		sistem crash	kerugian/ kerusaka	50	0.5	100	0.5	100	0.5	10	0.5	10	0.5	10	0.1	136	**22.67**
			gangguan	50	0.5	100	0.5	100	0.5	10	0.5	10	0.5	10	0.1	136	**22.67**
		gangguan/ cacat	kerugian/ kerusaka	50	0.1	10	0.1	100	0.1	10	0.1	10	0.1	10	0.1	19	3.17
			gangguan	50	0.1	10	0.1	100	0.1	10	0.1	10	0.1	10	0.1	19	3.17
		gangguan/ cacat	kerugian/ kerusaka	10	0.1	50	0.1	100	0.1	10	0.1	10	0.1	10	0.1	19	3.17
			gangguan	10	0.1	50	0.1	100	0.1	10	0.1	10	0.1	10	0.1	19	3.17
		kode berbahaya	kerugian/ kerusaka	100	0.5	10	0.5	50	0.5	10	0.5	10	0.5	10	0.1	91	**15.17**
			gangguan	100	0.5	10	0.5	50	0.5	10	0.5	10	0.5	10	0.1	91	**15.17**
Akses Fisik	inside factor	tidak sengaja	perubahan	50	0.1	10	0.1	50	0.1	10	0.1	10	0.1	10	0.1	14	2.33
			kerugian/ kerusaka	10	0.1	10	0.1	10	0.1	10	0.1	10	0.1	10	0.1	6	1.00
			gangguan	10	0.1	50	0.1	50	0.1	10	0.1	10	0.1	10	0.1	14	2.33
	inside factor	sengaja	perubahan	100	0.5	50	0.5	50	0.5	100	0.5	10	0.5	10	0.1	156	**26.00**
			kerugian/ kerusaka	100	0.5	50	0.5	50	0.5	50	0.5	10	0.5	10	0.1	131	**21.83**
			gangguan	100	0.5	10	0.5	50	0.5	10	0.5	10	0.5	10	0.1	91	**15.17**
Akses Jaringa	inside factor	tidak sengaja	perubahan	50	0.5	10	0.5	50	0.5	10	0.5	10	0.5	10	0.1	66	**11.00**
			kerugian/ kerusaka	10	0.1	10	0.1	10	0.1	10	0.1	50	0.1	10	0.1	10	1.67
			gangguan	50	0.5	10	0.5	50	0.5	10	0.5	50	0.5	10	0.1	86	**14.33**
	inside factor	sengaja	perubahan	100	0.1	50	0.1	100	0.1	50	0.1	10	0.1	10	0.1	32	5.33
			kerugian/ kerusaka	100	0.1	10	0.1	100	0.1	50	0.1	50	0.1	10	0.1	32	5.33
			gangguan	100	0.5	10	0.5	100	0.5	10	0.5	50	0.5	10	0.1	136	**22.67**
	outsid e	sengaja	perubahan	100	0.5	50	0.5	100	0.5	50	0.5	50	0.5	10	0.1	176	**29.33**
			kerugian/ kerusaka	100	0.1	10	0.1	100	0.1	50	0.1	50	0.1	10	0.1	32	5.33
			gangguan	100	1	10	1	100	1	10	1	50	1	10	0.1	271	**45.17**
Faktor Lain		masalah komunikasi	kerugian/ kerusaka	50	0.1	50	0.1	10	0.1	10	0.1	10	0.1	10	0.1	14	2.33
			gangguan	50	0.1	50	0.1	10	0.1	10	0.1	10	0.1	10	0.1	14	2.33
		masalah pihak ketiga	kerugian/ kerusaka	10	0.5	10	0.5	100	0.5	50	0.5	10	0.5	10	0.1	91	**15.17**
			gangguan	10	0.5	10	0.5	100	0.5	50	0.5	10	0.5	10	0.1	91	**15.17**

3.2.3 Mengembangun rencana strategi pengaman

Dari data tabel 5, maka didapati beberapa risk exposure yang nilainya berada diatas 10 (medium), dengan hasil tersebut maka dibuatlah beberapa kebijakan/saran guna mengurangi tingkat resiko yang mungkin terjadi.

1. Saran Pengamanan Sistem Informasi

Saran pengamanan sistem informasi diberikan penulis karena berdasarkan *risk exposure* sistem *crash* mempunyai risiko diatas angka 10. Kebijakan ini digunakan untuk penanggulangan atau mitigasi yang dilakukan jika sewaktu waktu sistem mengalami gagal proses/ *crash.* Pendeteksian dan prosedur perbaikan difokuskan untuk pengontrolan sistem informasi setiap saat. Pengontrolan sistem informasi ini diharapkan mencakup pengembangan sistem/ pembaharuan,(*development*) dan evaluasi berkala pada sistem informasi BAPPEDA, seperti melakukan uji keamanan (*penetrating system*). Sehingga risiko gagal proses/ *crash* yang

menimbulkan celah keamanan dapat diminimalisir dengan adanya pengembangan dan evaluasi ini. Saran ini juga diberikan mengingat bahwa kode berbahaya dalam sistem juga memberikan dampak negatif terhadap sistem. Untuk penanganan kode berbahaya (virus, trojan, worm) penulis menyarankan:

a. Pendeteksian sistem

   Pendeteksian sistem bisa berupa *scanning* terhadap sistem secara keseluruhan dengan menggunakan aplikasi atau software yang disarankan tentunya secara berkala

b. Backup Data

   Guna mengurangi risiko kehilangan data, maka disarankan melakukan backup data secara berkala. Backup dilakukan secara local maupun cloud.

c. Open Source

   Untuk menanggulangi kode berbahaya (virus, trojan, worm) penulis sangat menyarankan untuk migrasi ke sistem operasi berbasis opensource (linux)

2. Saran Akses Jaringan

Akses jaringan yang mempunyai risk exposure tertingi dari yang lain memaksa penulis memberikan peringatan keras atas hasil analisa ini. Faktor internal dan eksternal sama – sama turut mempunyai andil dalam tingginya nilai risk exposure. Penulis selanjutnya menyarankan tindakan:

a. Dilakukannya identifikasi secara menyeluruh dan mendalam.

   Identifikasi ini dilakukan agar dapat mendeteksi perilaku yang tidak wajar yang terjadi dari faktor internal maupun faktor external. Untuk faktor internal bisa dengan cara identifikasi semua level manajemen dan karyawan atas kebijakan yang telah dibuat, apakah sesuai prosedur atau belum, selanjutnya diberikan teguran atas hal yang tidak sesuai prosedur seperti contohnya penggunakan password yang tidak sesuai standar yang diberlakukan, penggunaan internet tidak berdasarkan kebutuhan, dan lain- lain. Identifikasi eksternal bisa dilihat dari dari perilaku logs ada sistem, dan melakukan evaluasi terhadap perilaku yang dianggap tidak wajar.

b. Otentifikasi terhadap Sumber Daya Manusia

   Otentifikasi ini diharapkan dapat mengontrol penuh terhadap pengakses sistem informasi. Identifikasi pengakses sistem dapat berupa username atau password yang telah dibuat sebelumnya. Sehingga informasi pengakses dipastikan adalah orang yang benar – benar mempunyai hak akses terhadap sistem. Saran selanjutnya untuk otentifikasi adalah berupa pembuatan laporan/ *logs* tentang informasi sumber daya manusia yang login/ memakai sistem informasi (website).

c. Kontrol terhadap jalur akses

   Walaupun sistem sudah memiliki firewall, update perlu dilakukan

untuk mencegah penyusup masuk, tidak hanya itu, konfigurasi enkripsi WEP, pengaturan PORT dan penutupan akses DOS meminimalkan resiko penyusup.

d. Penetrating Testing

Upaya ini dilakukan guna mengetahui cara berfikir *cracker* yang ingin merusak sistem dengan menggunakan akses jaringan. Upaya ini dilakukan guna mengetahui jalur akses mana yang dimungkinkan terdapat celah yang dapat di *exploit* oleh *attacker*

3. Kebijakan Masalah Pihak ketiga.

Saran pembuatan kebijakan terhadap masalah pihak ketiga diberikan penulis, karena dalam prakteknya pihak ketiga ada/ datang tanpa melalui prosedur yang ada. Sehingga terkesan hanya seperti mencari mudahnya dalam melakukan apapun terkait hal yang terjadi. Sebagai contoh sederhana: printer rusak, dari karyawan biasanya langsung mengkontak teman yang bisa memperbaiki printer, padahal sudah ada alur seperti pelaporan dan pencatatan terlebih dahulu selanjutnya bagian terkait menunjuk pihak ketiga yang bisa dipercaya untuk penyelesaian printer.

Saran selanjutnya untuk masalah ketiga adalah dengan upaya mempermudah prosedur. Tentunya dengan mudahnya prosedur membuat pihak BAPPEDA tidak akan malas melaksanakan prosedur jika ingin menggunakan jasa pihak ketiga.

KESIMPULAN

Berdasarkan penelitian yang penulis lakukan dan berdasarkan dari rumusan masalah yang ada, maka dapat diambil kesimpulan sebagai berikut :

a. Sistem informasi BAPPEDA Sleman (website) merupakan sub domain dari *slemankab.go.id* dengan template Wordpress yang diberikan KOMINFO kepada BAPPEDA untuk dikelola. Sistem ini merupakan wadah untuk interaksi masyarakat dengan BAPPEDA (pertanyaan, peminat informasi, ijin penelitian, dll). Segala informasi tentang BAPPEDA dapat dilihat pada website resmi ini.

b. Berdasarkan analisa OCTAVE-S, matrix resiko memperlihatkan beberapa bagian yang menunjukkan diatas MEDIUM (>10), dengan artian perlu mendapatkan perhatian yang lebih khusus. Bagian tersebut adalah sistem crash dan kode berbahaya pada bagian sistem 22,67% , faktor kesengajaan pada akses fisik rata- rata 21% , akses jaringan rata- rata 24,51%, dan masalah pihak ketiga pada faktor lainnya sebesar 15,17%.

c. Beberapa mitigasi yang disarankan terhadap temuan adalah rekomendasi/ saran dokumentasi, saran perencanaan darurat/ penanggulangan bencana, rekomendasi/ saran pemantauan dan audit keamanan fisik, rekomendasi/ saran pengamanan sistem informasi,

rekomendasi terkait akses jaringan dan kebijakan masalah pihak ketiga.

DAFTAR PUSTAKA

[1] Pearson, L,2007, *Sistem Informasi Manajemen 1 (ed.10)*,Ed.10, Salemba, Jakarta

[2] Calder, A, dan Watkins, S, 2005, *IT governance: A manager's guide to data security and BS 7799/ISO 17799*. Kogan Page Publishers.

[3] Tria Pramudya, R., Okto Susilo, D., Aulia Puspita, A., Gunawan, S. E., ST, M., 2013, *Pengukuran Risiko Teknologi Informasi Pada Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Menggunkan Metode Octave-S*. BINUS.

[4] Disa, S, 2011, Analisis Resiko Keamanan Sistem Informasi Menggunakan Metode OCTAVE-S (Studi Kasus: Sistem Informasi Akademik STMIK AKBA Makassar). *Jurnal Inspiration*, (1).

[5] Lewin, K, 1973, *Princípios de psicologia topológica*. Editora da Universidade de Sao Paolo.

[6] Hasibuan, Z. A, 2007, Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi. Fakultas Ilmu Komputer, Universitas Indonesia.

[7] Mettetal, G, 2002, Improving teaching through classroom action research. *Essays on Teaching Excellence*, *14* (7).

[8] Disa, S, 2011, Analisis Resiko Keamanan Sistem Informasi Menggunakan Metode OCTAVE-S (Studi Kasus: Sistem Informasi Akademik STMIK AKBA Makassar). *Jurnal Inspiration*, (1).

[9] Alberts, C. J., Dorofee, A. J., & Allen, J. H, 2001, *OCTAVE Catalog of Practices, Version 2.0*. DTIC Document.

[10] Alberts, C. J., Dorofee, A. J., & Allen, J. H, 2001, *OCTAVE Catalog of Practices, Version 2.0*. DTIC Document.