Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Implementasi Octave-S Dalam Evaluasi Manajemen Resiko Sistem Informasi Pada Balai Pelatihan Kesehatan Batam

Saut Pintubipar Saragih

Universitas Putera Batam, Batu Aji, Batam, 29432, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 1 Februari 2018
Revisi Akhir: 10 Maret 2018
Diterbitkan *Online*: 23 Maret 2018

KATA KUNCI

Octave-s, manajemen_resiko, resiko_it, sistem_informasi

KORESPONDENSI

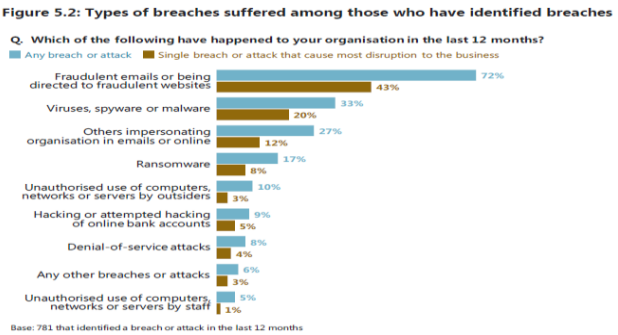
No HP: 08117777003
E-mail: pb11396@upbatam.aca.id

A B S T R A C T

Information systems security is currently one of the most important needs in an institution, agency or company. At the same time information security is also a very important thing to be managed through information system risk management since information has turned into a valuable asset for the company or institution. In Batam health training center (Bapelkes) which has also implemented information system in business process and organization also accept threats to information system. Information system risk management can use several methods to conduct evaluation or assessment of one of them is by using OCTAVE-S method. Octave-s has three main assessment phases followed by each process. The IT security procedure which is implemented by Bapelkes is authorized to the headquarters of Bapelkes which is remotely controlled by the system administration thoroughly. The result of the research shows that the institution has not implement all the IT risk management in appropriate path, it is found that some standard procedure like IT policy, collaborating system, information system audit, architecture, mitigation management is not managed very well. In addition, that all employees that work in IT area whether end user or IT administrator have not been well trained.

1. PENDAHULUAN

Ancaman terhadap keamanan sistem informasi sangat nyata terjadi dan harus dilakukan sebuah tahapan atau prosedur penanggulangan yang baik. Bahkan sebuah perusahaan yang baik sekalipun masih memiliki resiko ancaman yang sangat terbuka [1]. Beberapa hal yang menjadi prioritas keamanan sistem informasi berdasarkan hasil survey yang diberikan oleh universitas Portsmouth di Inggris [1] mengukuhkan keberadaan manajemen resiko teknologi dan sistem informasi sangat penting. Ditambahkan dalam sebuah penelitian di Inggris bahwa walalupun hanya 4 persen dari lembaga pemerintahan yang terancam namun terlihat bahwa kesadaran akan manajemen resiko sistem informasi sangatlah rendah [1] Keamanan Informasi sangat kritis atau penting untuk individu maupun organisasi karena hal tersebut memicu kerugian secara finansial [2]. Ancaman sistem informasi bahkan bisa menyerang semua jenis komunikasi yang terjadi pada sistem informasi seperti teknologi cloud computing yang sedang menanjak pamor dan keberadaannya [3]



Gambar 1. Kegiatan yang mengalami serangan siber

Setiap organisasi saat ini menyadari penuh akan berharganya informasi. Bahkan seharusnya kualitas informasi harus sudah terjaga sejak dari pembangunan project [4]. Balai Pusat pelatihan tenaga kesehatan (BAPELKES) ini merupakan sebuah Unit Pelaksana Teknis (UPT) bertaraf internasional yang dimiliki oleh kementerian kesehatan yang dibangun untuk mampu memberikan pelatihan berkelas internasional juga agar sumber daya manusia yang dihasilkan juga lebih baik. Pusat pelatihan ini berada di pulau Batam tepatnya terletak di Jalan Marina, Tanjung Uncang, Sekupang kota Batam, provinsi Kepulauan Riau. BAPELKES ini memiliki tugas utama untuk mendidik dan mberikan sertifikasi kepada tenaga kesehatan yang akan bekerja diluar negeri.

Pusat pelatihan ini memiliki seksi (department/subbag) yaitu seksi tata usaha (TU), seksi pendidikan dan pelatihan (Diklat), seksi pengendalian mutu (Dalmut) dan seksi pengkajian dan pengembangan (Kajibang). Kemudian seksi-seksi yang ada tersebut akan membawahi beberapa unit seperti unit asrama, sarana prasana (sarpras), transportasi, keuangan, pemasaran dan kepegawaian. Badan pusat pelatihan kesehatan ini sejak tahun 2015 mulai menerapkan sistem informasi yang masing-masing dipasang (install) di masing-masing department dan sejak tahun 2016 pihak Bapelkes sudah mulai menerapkan integrasi sistem (system integration). Sistem integrasi ini memungkinkan untuk melakukan kontrol dan memastikan performa sistem informasi yang dijalankan [5].

Resiko sistem informasi bisa datang dari semua pihak, in iberarti kesalahan kecil yang dilakukan oleh satu user sistem informasi bisa berakibat besar kepada sistem informasi secara keseluruhan dan bisa mengakibatkan kerugian dalam bentuk penurunan kinerja sistem ataupun secara finansial akan membuat biaya perbaikan (maintenance) akan meningkat yang secara otomatis akan meningkatkan cost of maintenance. Pada awal berdiri BAPELKES ini tidak memiliki sistem terpadu seperti yang ada saat ini sehingga resiko sistem informasi secara otomatis juga sangat kecil atau bahkan tidak ada, kemudian pada tahun 2013 pihak BAPELKES mulai membangun sistem independen pada masing-masing seksi yang juga diikuti oleh permintaan keahlian para karyawan untuk mengerti sistem informasi yang mereka gunakan, kemudian pada tahun 2016 BAPELKES mulai menerapkan sebuah sistem yang terintegrasi walaupun masih dalam tahap pengembangan untuk menyempurnakan tetapi sistem tersebut telah dijalankan. Dari data dan sejarah yang ada pada lembaga tersebut maka ada kemungkinan resiko yang akan diadapatkan oleh pihak BAPELKES.

2. TINJAUAN PUSTAKA

2.1 Keamanan dan Ancaman Risiko Sistem Informasi

Partisipasi pengguna meningkatkan kesadaran organisasi akan risiko dan pengendalian keamanan dalam proses bisnis, yang pada gilirannya memberikan kontribusi terhadap pengendalian keamanan yang lebih efektif Pengembangan dan kinerja [6].

Ancaman dan kerentanan merupakan dua faktor yang sangat menentukan didalam keamanan sistem informasi. Melakukan peninjauan pada data ancaman dan kerentanan yang ada merupakan salah satu aktifitas yang dilakukan dalam manajemen resiko [7]. Ancaman adalah indikasi kemungkinan munculnya kejadian yang tidak diharapkan. Ancaman juga mengacu pada situasi dimana seseorang dapat melakukan tindakan yang tidak diharapkan atau kejadian alam dapat menyebabkan hasil yang tidak diinginkan. Memang, ancaman keamanan begitu banyak sehingga sama sekali tidak mungkin untuk bertindak atas semuanya, karena setiap solusi keamanan teknologi memiliki biaya dan perusahaan memiliki sumber daya yang terbatas [9]. Pada umumnya sebuah ancaman diciptakan ketika seorang aktor mengeksploitasi celah kerentanan dari sebuah sistem untuk mendapatkan hak akses masuk untuk melakukan tujuan yang diinginkan.

2.2 Manajemen Risiko

Manajemen resiko merupakan sebuah kegiatan yang esensial untuk perusahaan atau lembaga maupun institusi. Proses bisnis yang dilaksanakan ataupun kegiatan.-kegiatan yang terkait dengan informati teknologi dipastikan memiliki resiko yang harus dinilai dan diatur *(manage)*. Tujuan dari pelaksanaan manajemen resiko agar seluruh proses bisnis yang dilakukan secara offline dan online dapat dikendalikan [8]. Suatu pengukuran terhadap risiko yang ada diperlukan dalam penerapan teknologi informasi. Pengukuran risiko TI berguna untuk mengetahui profil risiko TI; melakukan analisis terhadap risiko dan juga melakukan respons terhadap risiko, sehingga tidak terjadi dampak-dampak yang mungkin muncul dari risiko tersebut [9]. Manajemen risiko adalah suatu proses identifikasi, mengatur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain: mentransfer risiko pada pihak lain, menghindari risiko, mengurangi efek buruk dari risiko, dan menerima sebagian maupun seluruh konsekuensi dari risiko tertentu [10].

2.2.1 Manajemen Risiko Sistem Informasi

Manajemen risiko dalam konteks keamanan informasi bukanlah domain penelitian baru. Saat itu 1975 ketika USA National Bureau of Standards [11] . Menurut Steve Elkey Risiko sistem informasi merupakan potensi bahaya yang mungkin timbul dari beberapa proses yang dilakukan saat ini ataupun dari beberapa peristiwa di masa depan. Risiko hadir dalam setiap aspek kehidupan kita dan banyak disiplin ilmu yang berbeda fokus pada risiko yang berlaku untuk mereka. Dari perspektif keamanan IT, manajemen risiko adalah proses memahami dan menanggapi faktor-faktor yang dapat menyebabkan kegagalan dalam hal yang confidential, integritas, atau ketersediaan sistem informasi. Risiko keamanan IT Dari penjelasan diatas, maka dapat diambil kesimpulan bahwa manajemen risiko sistem informasi adalah suatu proses manajemen untuk mengidentifikasi, mengukur, dan mengurangi risiko yang terjadi pada organisasi yang berhubungan pada penerapan sistem informasi pada perusahaan. Pada umumnya kerangka kerja manajemen resiko sistem informasi memiliki dua bagian utama yaitu satu bagian berkaitan dengan pandangan struktural sementara yang lainnya dikaitkan dengan tampilan proseduralnya [8].

2.3 Octave-s

OCTAVE-S adalah sebuah pendekatan terhadap evaluasi resiko keamanan informasi yang komprehensif, sistematik, terarah, dan dilakukan sendiri. Octave adalah metodologi yang dikembangkan oleh institusi universitas rekayasa perangkat lunak Carnegie Mellon, digunakan untuk melakukan penilaian risiko yang menggabungkan tiga hal yaitu analisis organisasi, perilaku dan kelemahan teknologi [12]. Perilaku, dan kelemahan teknologi Octave merupakan singkatan dari Operationally Critical Threat, Asset, and Vulnerability Evaluation dimana metode evaluasi keamanan sistem informasi yang diperkenalkan oleh universitas Carnegie mellon ini merupakan sebuah framework (keranga kerja) yang memfokuskan kedalam tiga hal yaitu Ancaman kritis terhadap operasional (Operationally Critical Threat), Aset (Asset), dan evaluasi Kerentanan Keamanan (Vulnerability Evaluation). Metode octave-s menggunakan pendekatan tiga fase untuk menguji isu-isu teknologi, menyusun sebuah gambaran komprehensif keamanan informasi yang dibutuhkan oleh organisasi. Pada Fase 1, membangun aset berdasarkan profil ancaman, terdapat 2 proses, yaitu: proses mengidentifikasi informasi perusahaan dan proses menciptakan profil ancaman. Dalam proses pertama terdapat 3 aktivitas, Kemudian pada proses kedua terdapat 3 aktivitas Pada Fase 2, mengidentifikasi tingkat

kerentanan infrastruktur, terdapat 1 proses yaitu melakukan penghitungan aset kritis yang berhubungan dengan aset perusahaan, Pada Fase 3, mengembangkan rencana dan strategi keamanan, terdapat 2 proses, yaitu membangun kemungkinan kriteria evaluasi dan mengidentifikasi dan menganalisis risiko-risiko. Dalam proses pertama terdapat 3 aktivitas Metode ini menggunakan lokakarya untuk melakukan diskusi dan pertukaran informasi mengenai aset, praktek keamanan informasi dan strategi keamanan informasi. Setiap fase terdiri dari beberapa proses dan setiap proses memiliki satu atau lebih lokakarya yang dipimpin oleh tim analisis [13].

3. METODOLOGI

Metode evaluasi risk management yang akan digunakan pada assessment di Balai Pelatihan Kesehatan ini maka variabel penelitian yang akan digunakan pada penelitian ini adalah berdasarkan framework (kerangka kerja) yang telah ditetapkan oleh Octave-S itu sendiri. Pada Octave secara spesifik akan melakukan penilaian pada 3 fase utama yaitu: 1.Fase pada Organisasi (organization view), 2.Fase pada teknologi (technology view), 3.Fase pada strategi dan pengembangan (strategy and plan development). Masing-masing fase yang akan dilaksanakan nantinya akan mengevaluasi area keamanan informasi yang mencakup Aset, Ancaman, Penerapan yang sedang dilakukan, Kerentanan organisasi terhadap keamanan, Syarat dan standard keamanan sistem informasi, Komponen kunci Kerentanan secara teknikal (praktik), Resiko Strategi perlindungan, Rencana mitigasi. Adapun yang menjadi populasi dalam penelitian ini adalah pegawai Balai Pusat Pelatihan Kesehatan yang terlibat secara langsung dalam penggunaan system informasi, dari populasi yang ada tersebut diambil sampel dari karyawan yang berada pada Balai Pusat Pelatihan Kesehatan dari staff, supervisor, manajer dan direksi serta pegawai yang memilki akses terhadap sistem informasi secara mandiri (independent user) seperti administrator atau system/program developer. Dalam penelitian ini jumlah sampel adalah seluruh pengguna aktif sistem informasi yang dimiliki oleh balai pelatihan kesehatan batam (user).

Gambar 2. Desain penelitian

Dalam melakukan analisis data akan digunakan evaluasi keamanan sistem informasi akan digunakan pendekatan OCTAVE-S dalam penelitian ini karena OCTAVE-S memiliki keunggulan *self-driven* dan *flexible* sehingga pengunaannya tidak kaku. Dalam hal ini, karena OCTAVE-S hanya untuk perusahaan kecil dengan dibawah 100 pegawai dan penelitian ini fokus kepada bagian sistem informasi yang ada yang jumlahnya kurang dari 100 orang, karena itu kami memilih menggunakan metode OCTAVE-S maupun itu bukan satu-satunya pertimbangan melainkan melihat dari kapabilitas perusahaan/organisasi tersebut

Gambar 3. Model penelitian

4. HASIL DAN PEMBAHASAN

4.1. 4.1 Hasil Penelitian

Kriteria Evaluasi Dampak Risiko (Langkah 1), Dilihat dari segi keuangan, biaya operasional BAPELKES tidak mengalami peningkatan setiap tahunnya namun angggaran operasional tetap dipertahankan dan cenderung naik tidak signifikan hal ini disebabk an oleh anggaran operasional ditetapkan oleh bapelkes pusat (Jakarta). Jam kerja di BAPELKES mengalami peningkatan tetapi tidak signifikan sejak penerapan sistem informasi di bapekes. Kenaikan tersebut hanya berkisar 5%. Hal ini disebabkan oleh penggunaan informasi teknologi yang belum maksimal pada seluruh unit kerja. Kemungkinan ancaman terhadap kehidupan karyawan di BAPELKES tergolong sedang, dikarenakan pekerjaan yang dilakukan BAPELKES adalah pekerjaan infoor (office job desk) sedangakan pegawai yang bekerja diluar kantor sangat sedikit. Aset Sistem pada Organisasi (Langkah 2), Aset yang dimiliki oleh balai pusat pelatihan Batam meliputi sebuah sistem informasi manajemen pelatihan kesehatan (simpelkes), personal computer (pc), aplikasi persediaan, Kepala Tata usaha dan Tim IT pada organisasi. Evaluasi Praktek Keamanan (Langkah 3-4), Evaluasi praktek keamanan yang diberlakukan dan dilakukan oleh bapelkes adalah sebagai berikut: Kesadaran keamanan yang dimiliki oleh pegawai di bapelkes masih kurang. Hal ini sejalan dengan tidak pernah mendapatkan pelatihan tentang keamanan sistem informasi yang diberikan oleh organisasi kepada karyawan, belum memiliki sebuah strategi keamanan yang diterapkan, tetapi hal ini sudah masuk kedalam rencana tim IT di bapelkes, belum memiliki sebuah manajemen keamanan yang diterapkan, tetapi hal ini sudah masuk kedalam rencana tim IT di bapelkes, kebijakan keamanan yang terdokumentasi termasuk atas manajemen kreasi, administrasi dan juga komunikasi, belum memiliki sebuah kolaborasi keamanan yang diterapkan tetapi hal ini sudah masuk kedalam rencana tim IT di bapelkes, Kolaborasi keamanan hanya dilakukan dengan bapelkes pusat (Jakarta, belum secara maksimal menyusun rencana dalam menghadapi risiko atau bencana alam ataupun menghadapi kemungkinan terburuk atas terjadinya bencana dan bentuk rencana pemulihan yang dilakukan setelahnya untuk aset fisik yang ada di kantor, Bentuk pengendalian yang dilakukan bapelkes seperti prosedur, dan rencana fasilitas keamanan dalam menjaga lokasi, bangunan, serta aset fisik yang dimiliki instansi. (seperti pengendalian tamu

yang berkunjung ke instansi, pengendalian ruang server dll) belum diterapkan secara maksimal tetapi dalam hal ini bagian iistem informasi (IT) bertanggung jawab mengontrol keamanan aset fisik hardware dan software unuk setiap komputer User dan menangani langsung setiap ada keluhan, belum memiliki tim audit dan pemantau serta belum pernah melakukan audit keamanan, Bapelkes memiliki manajemen jaringan computer local dengan menggunakan sebuah perngkat lunak tambahan yang dibuat oleh mikrotik, tidak melakukan pemantauan dengan maksimal kemanan teknologi informasi dan fisik, menerapakan otorisasi pada sistem simpelkes sebagai bentuk pengendalian dan kontrol yang diterapkan oleh tim IT dalam mengatur hal perizinan dan konfigurasi jaringan sudah dilaksanakan, Manajemen kerentanan bapelkes terhadap informasi peringatan dan keamanan informasi serta pemberitahuan atas informasi-informasi penting yang perlu diinformasikan kepada internal instansi sebagai bentuk upaya dalam meminimalisisr segala bentuk risiko yang mungkin akan terjadi masih sangat rendah, Proses enkripsi di jaringan bapelkes tidak dilakukan, Bapelkes memiliki desain topologi jaringan tersendiri tetapi belum tetapi belum dimaksimalkan dengan mengkonfigurasi sistem keamanan pada jaringan tersebut, belum secara maksimal mengelola dugaan pelanggaran keamanan yang terjadi dalam setiap aktivitas.

Tabel 1. Status Spotlight (red,yellow,green)

Evaluasi praktek keamanan Sistem informasi?	Red	Yellow	Green
1. Kesadaran Keamanan dan Pelatihan		x	
2. Strategi Keamanan	x		
3. Manajemen keamanan	x		
4. Kebijakan Keamanan dan Peraturan	x		
5. Manajemen Keamanan Kolaboratif	x		
6. Perencanaan Contingency	x		
7. Pengendalian Akses Fisik		x	
8. Pemantauan dan Audit Keamanan Fisik	x		
9. Sistem dan Manajemen Jaringan		x	
10.Pemantauan dan Audit Keamanan TI	x		
11.Pengesahan dan Otorisasi			x
12.Manajemen Kerentanan	x		
13.Enkripsi	x		
14.Desain dan Arsitektur Keamanan	x		
15.Manajemen Insiden	x		

Aset Kritis (Langkah 5-9), Penilaian utama dalam aset-aset organisasi adalah dampak yang diberikan aset dalam perusahaan. Berdasarkan wawancara yang dilakukan kepada tim IT yang dilakukan ditemukan yang menjadi aset kritis yaitu simpelkes (sistem informasi manajemen pelatihan kesehatan) yang digunakan oleh seluruh pegawai dalam mengorganisir pendidikan dan pelatihan di bapelkes.

Kebutuhan Keamanan untuk Aset (Langkah 10-11), Berdasarkan hasil wawancara dan kuesioner dengan tim IT di bapelkes bahwa kebutuhan keamanan untuk keseluruhan aset perusahaan yaitu kerahasian informasi, integritas data, ketersediaan informasi terhadap peserta pendidikan pelatihan. Bagi walaupun bapelkes belum memberikan penjelasan secara detail tentang kebutuhan keamanan yang paling penting tetapi ketersediaan informasi menjadi sebuah hal yang sangat dibutuhkan dalam mengorganisir kegiatan pelatihan, karena tanpa ketersediaan informasi yang baik, maka proses kerja di masing-masing unit tidak dapat berjalan dengan baik.

Ancaman Terhadap Aset Kritis (Langkah 12-16), Kemungkinan ancaman yang dapat terjadi terhadap aset kritis dari internal yaitu dari pegawai yang menggunakan partisi yang tidak diijinkan dalam melakukan pertukaran data dan melakukan kunjungan pada website di internet yang tidak diketahui keamanannya dan secara eksternal ancaman yang dapat terjadi pada akses jaringan perusahaan biasanya terjadi kesalahan penginputan data ke dalam sistem atau human error dan virus. Ancaman untuk virus tidak terlalu bermasalah dalam perusahaan karena perusahaan mengupdate secara rutin anti virus yang dipunya serta perusahaan menggunakan operating sistem linux agar tidak mudahnya virus masuk ke dalam jaringan.

Fase 2 Mengidentifikasi Kerentanan Infrastruktur. Jalur Aset Kritis (Langkah 17-18), Jalur aset berkaitan langsung dengan sistem dengan database. Database sendiri pada organisasi masih menggunakan database yang ada pada server pusat. Sedangkan sistem operasi yang digunakan pada komputer personal masing-masing user di bapelkes adalah menggunakan sistem operasi windows dengan jaringan komputer lokal yang tersambung dengan jaringan internet yang disediakan oleh pihak ketiga (internet service provider).

Keterkaitan Teknologi (Langkah 19-21), Komponen penting yang terkait dengan sistem penting organisasi terdiri dari server, laptop, on-site workstation, dan storage device.Yang bertanggung jawab untuk menjaga dan mengkonfigurasi server, laptop, on-site workstation, dan storage device adalah divisi IT balai pusat pelatihan Batam.

Fase 3 Mengembangkan strategi keamanan dan perencanaan. Hasil Evaluasi dan dampak ancaman (Langkah 22), Evaluasi dampak ancaman pada aset kritis

Tabel 2. Hasil Evaluasi dan Dampak ancaman

Assets	***Outcome***	***Impact Descripton***	***Values***
SIM PELKES	*Disclosure*	Kegagalan dalam keamanan *privacy* data keuangan akan mengakibatkan pihak yang tidak berkepentingan melihat *content* dari SIMPELKES	*High*
	Modification	Input data yang salah dan berulang-ulang akan mengakibatkan *system records* yang tidak tersimpan dalam database	*High*
	Interuption	Fitur yang belum berjalan sepenuhnya mengakibatkan terhambatnya proses pekerjaan	*High*
	Loss/ Destruction	Kehilangandata kepegawaian akan sangat menghambat dan mengakibatkan melakukan pengulangan pekerjaan	*High*

Kriteria Kemungkinan (Langkah 23). Kemungkinan yang mungkin terjado pada bebrapa aspek setelah aset kritis diketahui dan ancaman yang mungkin muncul adalah sebagai berikut:

Tabel 3. Kriteria Kemungkinan

Impact Area	High	Medium	Low
Reputation	Reputasi dianggaprusak sehinggatidak Dapat dikembalikan seperti semula Tidak lagi dipercayaoleh masyarakat, maupun karyawan.	Reputasi dianggap tercemar dan memerlukan biaya danusaha untuk kembali pulih. Diperlukanusaha danbiayauntuk memulihkan kepercayaan karyawanmaupun masyarakat	Reputasi dianggap berubah dan akan pulihdengan sendirinya. Karyawan dan masyarakat akan kembali percaya dengan sendirinya.
Productivity	Karyawan tidak dapat melakukan pekerjaan mereka Hilangnya data dan tidakbisa dipulihkan (*Irrecoverable)*	Melambatnya Proses pekerjaan karyawan Hilangnya data dan bisa dipulihkan. (*Recoverable)*.	Melambat namun, tidak berpengaruh kepadaproses pekerjaan karyawan Terdapat perubahantapi tidak berpengaruh terhadapdata yang ada.
Finance	Pelaporan keuangansalah dan tidak dapat dipulihkan	Terdapat selisih pada pelaporan keuangan dan dapat dipulihkan	Terdapat perubahantapi tidak berpengaruh terhadap pelaporan keuangan.

Peluang dari Ancaman (Langkah 24), Peluang dari ancaman yang mungkin terjadi pada sistem keamanan bapelkes adalah Peluang terjadinya ancaman yang secara tidak di sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan. Untuk ancaman terjadinya penyingkapan berpeluang sedang dengan tingkat keyakinan sedang terhadap perkiraan kemungkinan yang ada. Peluang terjadinya modifikasi bernilai rendah dengan tingkat keyakinan kecil, peluang terjadinya penghancuran dan interupsi sama-sama bernilai rendah dengan tingkat keyakinan kecil.

Peluang terjadinya ancaman melalui akses jaringan dalam internal perusahaan secara sengaja. Ancaman terjadinya penyingkapan dan modifikasi berpeluang sedang dengan tingkat keyakinan kecil, sedangkan untuk ancaman penghancuran dan interupsi berpeluang sedang dengan tingkat keyakinan kecil. Peluang terjadinya ancaman melalui akses jaringan dalam eksternal perusahaan secara tidak sengaja. Peluang terjadinya penyingkapan, modifikasi, penghancuran dan interupsi bernilai rendah dengan tingkat keyakinan rendah untuk semua ancaman. Peluang terjadinya ancaman melalui akses jaringan dalam eksternal perusahaan secara sengaja. Terjadinya ancaman penyingkapan, modifikasi, penghancuran, dan interupsi berpeluang kecil dengan keyakinan kecil untuk semua ancaman.

Strategi Perlindungan (Langkah 25), Strategi Perlindungan yang harus diterapkan oleh bapelkes didalam memberikan keamanan sistem informasi yang baik dapat dilihat dari status spotlight yang ditemukan bahwa ada 93% area yang harus diperbaiki. Sehingga strategi perlindungan yang harus diterapkan oleh bapelkes dapat mengikuti hasil dari psersenasi status spotlight yang ada.

Pendekatan Mitigasi (Langkah 26-27), Pendekatan mitigasi dapat dilakukan dengan menggunakan hasil penemuan pada presentasi spotlight merah (red). Spotlight merah menunjukan adanya kekurangn dan keharusan untuk membuat strategi untuk melakukan mitigasi pada peristiwa tertentu.

Rencana Mitigasi Resiko (Langkah 28), Berdasarkan pengisian lampiran diketahui area yang perlu dimitigasi oleh perusahaan. Rencana mitigasi risiko yang harus dibuat untuk setiap praktek keamanan seperti menyediakan pelatihan kesadaran keamanan pada seluruh karyawan perusahaan. Dimaksudkan agar dapat membantu perusahaan dalam meminimalkan risiko yang akan terjadi. Agar lebih efektif diperlukan pelatihan kesadaran keamanan secara berkala agar penerapaan keamanan akan lebih berfungsi secara baik. Menyediakan pelatihan pendukung TI secara periodik pada karyawan TI karena perangkat TI selalu berkembang dan perlu adanya pelatihan dalam karyawan TI agar penerapan dalam organisasi lebih baik.

Perubahan Strategi Perlindungan (Langkah 29), Perubahan strategi perlindungan yang ingin dilakukan perusahaan dalam area ini adalah melakukan sistem pembaruan keamanan secara periodik agar keamanan data perusahaan dapat terus diawasi dengan baik. Memberikan kesempatan bagi karyawan teknologi informasi untuk mengikuti pelatihan yang terkait keamanan yang didukung teknologi secara periodik sehingga karyawan lebih handal dalam menjalankan keamanan yang disesuaikan dengan kemajuan teknologi.

Identifikasi Langkah Selanjutnya (Langkah 30), Dalam pengimplementasi hasil dari evaluasi dan sikap keamanan, ada beberapa hal yang menjadi pertimbangan perusahaan, antara lain: 1. Manajemen harus mengutamakan keamanan informasi dalam organisai/perusahaan dalam mendukung pelaksanaan hasil dari octave-s, 2. Menerapkan kegiatan keamanan informasi dengan baik pada pegawai bapelkes, 3. Merencanakan proses mitigiasi yang matang dan terencana, 4.Jika kegiatan mitigasi yang ada sekarang belum diterapkan secara menyeluruh, maka organisasi tidak akan melakukan evaluasi penambahan aset-aset penting.

5. KESIMPULAN DAN SARAN

Sistem keamanan sistem informasi yang dimiliki oleh balai pelatihan kesehatan batam yang memiliki aset penting dan yang paling utama adalah sistem informasi manajemen pelatihan kesehatan (bapelkes) sangat rentan dengan ancaman dari internal maupun eksternal. Hal ini ditemukan dari hasil evaluasi keamanan sistem informasi dengan menggunakan metode octave-s. Kesimpulan yang didapatkan dari evaluasi di bapelkes dapat dibuat seperti berikut ini:

Simpelkes yaitu sistem informasi yang digunakan oleh seluruh pegawai di balai pelatihan kesehatan Batam untuk membantu mengorganisir kegiatan pendidikan dan pelatihan di bapelkes yang dari tahun ke tahun meningkat. Simpelkes juga sebuah aplikasi yang didukung oleh bapelkes pusat dengan intgerasi data dengan menggunakan aplikasi yang dikendalikan dari pusat seperti aplikasi persediaan. Personal komputer merupakan aset penting lainya di bapelkes karena kegiatan input data dan pengolahan data digunakan oleh personal komputer yang ada di tiap-tiap unit kerja.

Dari 15 praktek keamanan yang dievaluasi bapelkes memiliki kelemahan yang sangat signifikasn yaitu Strategi Keamanan Manajemen keamanan, Kebijakan Keamanan dan Peraturan,

Manajemen Keamanan Kolaboratif, Perencanaan Contingency, Pemantauan dan Audit Keamanan Fisik, Pemantauan dan Audit Keamanan TI, Manajemen Kerentanan, Enkripsi, Desain dan Arsitektur Keamanan, Manajemen Insiden. Saat perusahaan mengalami ancaman risiko TI, dampak terhadap reputasi perusahaan tergolong tidak baik, finansial dikategorikan baik karena kegiatan IT tidak terkait langsung dengan proses finansial secra langsung tetapi secara tidak langsung akan mengurangi finansial dari terganggunya sistem IT di bapelkes, produktivitas perusahaaan dikategorikan sedang, perlindungan kesehatan setiap karyawan diperusahaan dikategorikan baik, dan denda perusahaan tergolong rendah. Kurangnya kesadaraan karyawan akan peran keamanan dan tanggung jawab mereka. Kurangnya kesadaran manajemen dalam keamanan sistem informasi karena tidak pernah mengadakan pelatihan keamanan sistem informaasi dan masih belum memaksimalkan peralatan keamanan secara maksimal. Balai Pelatihan kesehatan Batam belum pernah melakukan pengukuran risiko Teknologi Informasi secara menyeluruh sebelumnya. Setelah dilakukan pengukuran risiko menggunakan octave-s ternyata terdapat ancaman yang dapat mengganggu proses krerja dan bisnis di bapelkes Batam. Rendahnya pengarahan tentang pentingnya kesadaran keamanan sehingga kesadaran karyawan menjaga keamanan Teknologi Informasi rendah.

Hasil evaluasi dengan menggunakan octave-s pada balai pelatihan kesehatan (bapelkes) mengungkapkan banyak kelemahan dari sisi keamanan sistem informasi yang mampu meyebabkan kerugian secara finansial, produktifitas hingga reputasi yang dimiliki oleh organisasi sehingga dengan penemuan ini maka pihak pengelola sistem IT dan jajaran struktural di bapelkes disarankan untuk melakukan hal-hal sebagai berikut: Institusi sebaiknya menerapkan manajemen risiko teknologi informasi, sehingga dapat mengetahui risiko-risiko teknologi informasi yang dapat terjadi serta meminimalkan risiko-risiko tersebut, Manajemen atau pejabat struktural sebaiknya nenyediakan pelatihan kesadaraan keamanan kepada seluruh pegawai di bapelkes secara rutin agar pegawai dapat mengerti bagaimana menjaga keamanan serta meminimalkan risiko-risiko yang mungkin muncul, diberikan pengarahan agar pegawai dapat mengetahui pentingnya kesadaran keamanan sistem informasi yang baik dan benar dan diikuti dengan kebiasaan baik dalam menggunakan sumber daya di institusi..

DAFTAR PUSTAKA

[1] R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, and G. Pestell, "Cyber security breaches survey 2017 Main report," no. April, 2017.

[2] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security threats," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 507–514, 2015.

[3] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," *Proc. - 2011 IEEE 4th Int. Conf. Cloud Comput. CLOUD 2011*, pp. 364–371, 2011.

[4] S. Anand and V. Chopra, "Decision Support System for Software Risk Analysis during Software Development," vol. 2, no. 1, pp. 29–35, 2012.

[5] C. S. Chapman and L. A. Kihn, "Information system integration, enabling control and performance," *Accounting, Organ. Soc.*, vol. 34, no. 2, pp. 151–169, 2009.

[6] J. Spears and H. Barki, "User participation in information systems security risk management," *MIS Q.*, vol. 34, no. 3, pp. 503–522, 2010.

[7] H. Nezakati, A. Amidi, Y. Y. Jusoh, S. Moghadas, Y. A. Aziz, and R. Sohrabinezhadtalemi, "Review of Social Media Potential on Knowledge Sharing and Collaboration in Tourism Industry," *Procedia - Soc. Behav. Sci.*, vol. 172, pp. 120–125, 2015.

[8] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Appl. Comput. Informatics*, vol. 9, no. 2, pp. 107–118, 2011.

[9] I. T. Anderes Gui, Sanyoto Gondodiyoto, "PENGUKURAN RESIKO Teknologi Informasi (TI) DENGAN METODE OCTAVE-S," *CommIT*, vol. 2, pp. 33–38, 2009.

[10] A. R. Viyanto, O. S. Latuihamallo, F. M. Tua, and A. Gui, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI: STUDI KASUS PADA PERUSAHAAN JASA," *ComTech*, vol. 4, no. 1, pp. 43–54, 2013.

[11] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Inf. Manag. Comput. Secur.*, vol. 22, no. 5, pp. 410–430, 2014.

[12] Stephanus, "Implementation OCTAVE-S and ISO 27001 Controls in Risk Management Information Systems," *Comtech*, vol. 5, pp. 685–693, 2014.

[13] H. Hendarti and Maryani, "PENGUKURAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI DENGAN METODE OCTTAVE-S," *Comtech*, vol. 5, no. 2, pp. 917–924, 2014.

BIODATA PENULIS

Saut Pintubipar Saragih

Penulis merupakan pengajar aktif di universitas putera batam dengan spesialisasi pada information system engineering, software design, system analyse. Menyelesaikan pendidikan sarjana di stmik putera batam, kemudian pendidikan master di universitas bina nusantara pada bidang yang sama. Penulis telah mempublikasi beberapa artikel ilmiah pada topik knowledge sharing behavior dan inovasi teknologi informasi, penggunaan teknologi informasi. Penulis juga menyelesaikan beberapa pelayanan kepada masyarakat melalui program pengabdian kepada masyarakat dengan beberapa topik seperti penyuluhah penggunaan internet, keamanan dokumen micrsoft office, bantuan sosial dan pembinaan pembuatan website.