Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S

Rinaldi Pratama[1], Dedy Syamsuar[2] , Yesi Novaria Kunang[3]

Fakultas Ilmu KomputerUniversitas Bina Darma
email :ph3311rinaldi@gmail.com[1], ,dedy_syamsuar@binadarma.ac.id[2],
yesinovariakunang@binadarma.ac.id[3]
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Peranan teknologi informasi sangat penting bagi suatu pemerintahan.Salah satu bentuk pemanfaatan teknologi informasi adalah sistem informasi manajemen. Sistem informasi manajemen adalah pengelolaan transaksi yang dapat memberikan informasi penting dengan cepat sehingga memudahkan manajemen dalam mengambil keputusan untuk kepentingan perusahaan. Aspek penting yang sering terlupakan dalam menggunakan sistem informasi adalah masalah keamanan informasi.Keamanan informasi adalah perlindungan terhadap informasi yang bertujuan melindungi dari segala sumber ancaman. Prinsip utama keamanan informasi yaitu kerahasiaan, integritas dan ketersediaan data. Inspektorat Daerah Kabupaten OKU Timur merupakan badan pengawasan yang menggunakan sistem inforomasi manajemen tindak lanjut hasil pengawasan untuk memonitoring hasil temuan pelanggaran dan kegiatan tindak lanjut dari pelanggaran yang ditemukan. Upaya dalam menjaga informasi agar tetap aman diperlukan evaluasi untuk risiko keamanan informasi yang bertujuan untuk mengidentifikasi ancaman dan membuat rencana mitigasi untuk mengurangi risiko. Evaluasi menggunakan *framework* OCTAVE-S yang terdiri dari 3 fase dengan pengumpulan data menggunakan wawancara terhadap 4 orang informan. Hasil dari evaluasi mengungkapkan instansi tidak menerapkan praktek keamanan yang baik sehingga memiliki kelemahan di beberapa area seperti kesadaran keamanan dan pelatihan, manajemen keamanan, kebijakan dan peraturan keamanan, pemantauan dan audit TI, autentifikasi dan otorisasi serta manajemen kerentanan. Strategi perlindungan instansi kurang berjalan baik dikarenakan pegawai belum mendapatkan pelatihan mengenai keamanan informasi.

Kata kunci : Keamanan informasi, Sistem Informasi Manajemen, kerangka kerja OCTAVE-S

1 PENDAHULUAN

Teknologi informasi saat ini sudah menjadi kebutuhan mendasar dan mempunyai peranan penting untuk menjalankan aktivitas-aktivitas pendukung instansi. Demi mencapai tujuan bisnisnya perusahaan saat ini banyak bergantung pada teknologi informasi. Komunikasi dan teknologi informasi merupakan faktor kunci pengembangan masyarakat global. Inovasi dalam teknologi informasi dan komunikasi selalu ada untuk peningkatan produktivitas, mengubah cara kita bekerja, menumbuhkan ekonomi bisnis, dan berbagi pengetahuan global serta untuk memiliki proses bisnis dan komunikasi otomatis(Veljanovska & Zdravevska, 2013).

Peranan sistem informasi/teknologi informasi (SI/TI) dalam mendukung aktivitas bisnis instansi terasa semakin meluas, bukan hanya memberikan peningkatan effisiensi dan effektifitas kinerja suatu

instansi tetapi juga sudah menjadi pemberdaya bagi instansi untuk menjalankan proses bisnisnya dalam mencapai dari tujuan proses bisnis tersebut. Peran SI/TI mampu menunjang pertumbuhan pembangunan seperti dilingkungan pemerintahan melaui e-goverment dan penerapan di dunia bisnis (Maslan, 2013).

Keamanan informasi adalah seperangkat prosedur, proses, teknologi dan manusia yang bertujuan untuk melindungi aset instansi (Syalim, Hori, & Sakurai, 2009). Keamanan Informasi untuk melindungi akses informasi terhadap orang yang tidak berwenang, dan juga melindungi mereka dari pengungkapan, perubahan, atau menghancurkan informasi. Tidak ada metodologi dan standar yang harus digunakan oleh instansi dalam penilaian risiko dan yang paling bermanfaat untuk instansi dalam penilaian risiko mengukur tingkat keparahan risiko dan menggembangkan kontrol keamanan untuk mengurangi keruginan dan mendapatkan keuntungan maksimal dari investasi yang dilakukan pada tindakan keamanan (Saleh & Alfantookh, 2011). Melihat pentingnya evaluasi keamanan informasi untuk mengetahui dampak risiko serta memberikan rekomendasi untuk mengatasi risiko tersebut.

Penelitian ini difokuskan pada Inspektorat Daerah Kabupaten OKUT yang merupakan Satuan Kerja Perangkat Daerah yang memiliki tugas pokok salah satunya melakukan pengawasan terhadap pelaksanaan urusan pemerintahan di Daerah Kabupaten Ogan Komering Ulu Timur. Oleh karena itu penulis merasa penting untuk melakukan penelitian ini yaitu mengevaluasi risiko keamanan informasi pada sistem informasi manajemen tindak lanjut hasil Pengawasan Inspektorat Daerah Kabupaten OKU Timur untuk mengetahui ancaman risiko keamanan informasi terhadap aset-aset kritis dan membuat rencana mitigasi untuk mengurangi risiko yang mungkin terjadi.

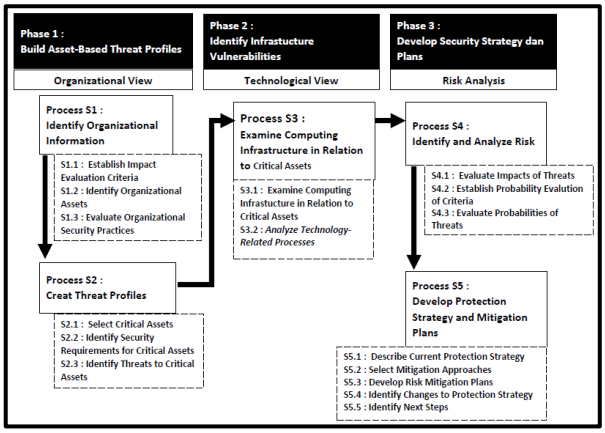
2 METODOLOGI PENELITIAN

Penelitian ini adalah penelitian kualitatif dan menggunakan teknik analisis deksriptif yang melampirkan hasil berupa uraian dari data hasil wawancara yang telah dilakukan terhadap informan. Evaluasi risiko keamanan pada Inspektorat menggunakan OCTAVE-S.. Pada OCTAVE-S memiliki 3 fase utama yang mempunyai beberapa proses dan diturunkan dalam beberapa aktifitas sehingga terdapat langkah-langkah yang harus dilakukan dalam evaluasi risiko keamanan. Adapun pengumpulan data menggunakan teknik wawancara dan observasi. Wawancara dilakukan kepada 4 informan yang dianggap mempunyai kemampuan dan bertanggung jawab terhadap objek yang sedang diteliti.

Tabel 1. Informan Penelitian

No	Bagian	Jumlah
P01	Inspektur	1 Orang
P02	Subbagian Evaluasi dan Pelaporan	1 Orang
P03	Pengelola Teknologi Informasi	2 Orang

Data diperoleh dari pertanyaan yang dijawab informan dengan melakukan perubahan terhadap poin-poin pertanyaan OCTAVE-S disesuaikan dengan lingkungan instansi. Hasil dari pengumpulan data akan dituliskan dalam beberapa worksheet sesuai dengan pendekatan OCTAVE-S



Gambar 1. Fase-Fase Evaluasi OCTAVE-S

2.1. OCTAVE-S

OCTAVE-S adalah variasi dari pendekatan OCTAVE yang dikembangkan untuk kebutuhan instansi yang kecil (kurang dari 100 orang).Untuk mengelola risiko terhadap keamanan sistem informasi, maka perlu dilakukan evaluasi risiko untuk mengurangi kerugian-kerugian yang mungkin terjadi. Salah satu metode evaluasi risiko untuk keamanan sistem informasi suatu instansi atau perusahaan adalah metode OCTAVE-S (The Operationally Critical Threat, Asset, and Vulnerability Evaluation)-Small yang mampu mengelola risiko perusahaan dengan mengenali risiko-risiko yang mugkin terjadi pada perusahaan dan membuat rencana penanggulangan dan mitigasi terhadap masing-masing risiko yang telah diketahui(Alberts, Dorofee, Stevens, & Woody, 2005). Evaluasi terhadap risiko keamanan informasi yang dilakukan oleh metode OCTAVE-S bersifat komprehensif, sistematik, terarah, dan dilakukan sendiri. Untuk mendukung dan memudahkan pelaksanaan analisa risiko dengan menggunakan metode OCTAVE-S. Dengan mengimplementasikan hasil-hasil dari OCTAVE-S, sebuah instansi berusaha melindungi semua informasi dengan lebih baik dan meningkatkan keseluruhan bidang keamanan. Dalam Metode OCTAVE-S memiliki 3 fase untuk mengevaluasi praktek keamanan dan menyusun rencana mitigasi yang dibutuhkan instansi. Pada fase 1 yang terdiri dari membangun aset berdasarkan profil ancaman, mengidentifikasi kerentanan infrastruktur serta membangun strategi perlindungan dan rencana mitigasi. Pada Fase 1, membangun aset berdasarkan profil ancaman, terdapat 2 proses, yaitu: proses mengidentifikasi informasi instansi dan proses membuat profil ancaman. Pada Fase 2, mengidentifikasi kerentanan infrastruktur, terdapat 1 proses yaitu melakukan perhitungan aset kritis yang berhubungan dengan aset instansi. Pada Fase 3, membuat rencana mitigasi dan strategi perlindungan, terdapat 2 proses yaiut membangunn kemungkinan kriteria evaluasi dan mengidentifikasi dan menganalisis risiko.

3. HASIL DAN PEMBAHASAN

Hasil analisis menggunakan pendekatan OCTAVE-S ini berupa ancaman risiko yang dihadapi dan tindakan mitigasi terhadap hasil temuan dengan pendekatan OCTAVE-S.

3.1. Membangun Profil Ancaman

Kriteria evaluasi dampak risiko dari enam area, hanya 3 area dampak yang dapat dianalisa dan dievaluasi. Kriteria dampak pada penelitian ini adalah dampak reputasi, dampak produktifitas dan dampak finansial. Aset yang dimiliki oleh Inspektorat berupa sistem informasi manajemen tindak lanjut hasil pengawasan, personal komputer, laptop, aplikasi antivirus, Inspektur dan staf pengelola

TI instansi.Evaluasi Praktek keamanan yang dilakukan di Inspektorat bisa dilihat pada Tabel 2 dibawah ini:

Tabel 2. Stoplight Status Area Praktek Keamanan

No	Lima Belas Praktik Keamanan	Red	Yellow	Green
1	Kesadaran Keamanan dan Pelatihan	✓		
2	Strategi Keamanan		✓	
3	Manajemen Keamanan	✓		
4	Kebijakan Keamanan dan Peraturan	✓		
5	Manajemen Keamanan Kolaboratif		✓	
6	Perencanan Contingency		✓	
7	Pengendalian Akses Fisik		✓	
8	Pemantauan dan Audit Keamanan Fisik		✓	
9	Sistem dan Manajemen Jaringan		✓	
10	Pemantauan dan Audit Keamanan TI	✓		
11	Pengesahan dan Otorisasi	✓		
12	Manajemen Kerentanan	✓		
13	Enkripsi		✓	
14	Desain dan Arsitektur Keamanan		✓	
15	Manajemen Insiden		✓	

Dilihat pada tabel 2 area praktek keamanan yang memiliki kelemahan yang sangat signifikan terjadi di 6 area sedangkan pada penelitian yang dilakukan(Saragih, 2018) area praktek keamanan pada Badan Pelatihan Kesehatan di Batam evaluasi menggunakan OCTAVE-S mengungkapkan ada 11 praktek keamanan yang memiliki kelemahan yang sangat signifikan. Untuk area yang sudah dilakukan dengan baik tanpa harus diperbaiki Inspektorat belum ada sedangkan untuk BAPELKES Batam area yang sudah dilakukan dengan baik terletak pada praktek keamanan kesadaran dan pelatihan keamanan. Setelah evaluasi praktek keamanan selanjutnya menentukan aset kritis berdasarkan wawancara yang dilakukan kepada informan yang menjadi aset kritis paling penting adalah sistem informasi manajemen tindak lanjut hasil pengawasan yang digunaakn oleh operator tim auditor dan user-user SKPD. kebutuhan keamanan menurut staf TI adalah kerahasiaan dari sebuah informasi yang akan berbahaya bila diketahui oleh orang yang tidak punya wewenang.

Ancaman yang dapat terjadi terhadap aset kritis dari pihak internal yaitu pegawai meminjam komputer pegawai lain yang akses sistem belum di logout akan berakibat pegawai yang tidak punya akses dapat mengetahui informasi sensitif, admin yang merasa tidak puas bisa melakukan perubahan terhadap hak akses sehingga menyebabkan akes ke sistem terganggu. Untuk pihak eksternal ancaman yang dapat terjadi petugas kebersihan yang membersihkan ruangan server tanpa sepengetahuannya membuat salah satu komponen terlepas sehingga membuat kerja server terganggu. Ancaman untuk virus bisa menimbulkan masalah karena staf pengelola TI Inspektorat jarang melakukan update antivirus dan masih menggunakan sistem operasi windows. Untuk ancaman sistem yang mengalami gangguan bisa disebabkan kurang efisiennya pengkodingan aplikasi sehingga membuat proses kerjanya lambat. Untuk ancaman power supply masih cukup menganggu karena belum adanya ups atau cadangan listrik lain.

3.2. Mengidentifikasi kerentanan infrastruktur

Jalur aset kritis berkaitan dengan database. Database sendiri masih menggunakan server inforkom yang terletak di DISKOMINFO, sedangkan untuk sistem operasi menggunakan windows dengan jaringan lokal yang menggunakan layanan internet yang disediakan pihak ketiga. Komponen penting yang terkait dengan sistem terdiri dari server, laptop, pc, on-site workstation dan storateg device yang semua itu merupakan tanggung jawab staf pengelola TI Inspektorat.

3.3. Mengembangkan strategi perlindungan dan rencana mitigasi.

Evaluasi dampak ancaman merupakan proses selanjutnya, berikut ancaman risiko yang mempunyai dampak besar untuk instansi:

Tabel 3 Hasil evaluasi dampak ancaman

Aset	*Hasil*	*Impact Description*	*Values*
Sistem Informasi Manajemen Tindak Lanjut Hasil Pengawasan	Kehilangan / Kerusakan	Terjadinya bencana alam yang tidak bisa diprediksi mengakibatkan aset fisik menjadi rusak sehingga data rusak dan tidak dapat dikembalikan	Tinggi
		Antivirus yang digunakan untuk melindungi sistem tidak secara rutin diupdate bahkan menggunakan antivirus bajakan mengakibatkan sistem sangat mudah disusupi *malicious kode* yang berbahaya menyebabkan data menjadi rusak dan tidak dapat dikembalikan lagi	Tinggi
	Interupsi	Pegawai yang tidak puas dan mempunyai akses masuk ke ruang server dapat melakukan tindakan ilegal yang mengancam sistem	Tinggi

Setelah menganalisis ancaman risiko selanjutnya mengevaluasi peluang dari ancaman yang bisa dilihat pada tabel 3. Untuk ancaman kehilangan / kerusakan oleh bencana alam memiliki peluang yang rendah dengan tingkat keyakinan tinggi. Untuk ancaman kehilangan / kerusakan oleh virus memiliki peluang yang rendah dengan tingkat keyakinan rendah. Untuk ancaman gangguan oleh pegawai yang berusaha melakukan tindakan ilegal diruang server memiliki peluang rendah dengan tingkat keyakinan tinggi. Selanjutnya membuat rencana mitigasi risiko dibuat untuk mengurangi risiko yang ada seperti menyediakan pelatihan keamanan informasi, membuat kebijakan untuk menindak tegas pihak internal yang sengaja melakukan tindakan mengancam sistem, membuat SOP untuk pemberian, pembuatan, perubahan dan penghapusan hak akses user, membuat SOP untuk hak akses pegawai ke ruangan server bila perlu menerapkan teknologi scan kartu, sidik jari atau retina untuk masuk ruangan server agar lebih aman.

Dalam menerapkan rencana mitigasi perlu perubahan strategi yang ingin dilakukan instansi adalah memberikan kesempatan kepada staf pengelola TI untuk mengikuti pelatihan terkait keamanan informasi secara rutin sehingga meningkatkan kesadaran dan kemampuan pegawai lebih kompeten dan menjalankan keamanan informasi menggunakan teknologi informasi sesuai kebutuhan.

Langkah selanjutnya dalam implementasi hasil evaluasi ada beberapa hal yang harus dipertimbangkan, seperti: melakukan pemantauan terhadap kemajuan implementasi hasil evaluasi dengan mengakan rapat mingguan, bulanan, merencanakan kegiatan mitigasi yang matang, apabila kegiatan mitigasi sekarang belum diterapkan secara menyeluruh maka instansi tidak akan melakukan evaluasi tambahan untuk aset kritis yang penting lainnya.

4. KESIMPULAN DAN SARAN

Sistem Informasi Manajemen Tindak Lanjut Hasil Pengawasan adalah sistem informasi yang digunakan oleh pihak inspektorat dalam mengontrol hasil pengawasan yang telah mereka lalukan dan merupakan aset penting.

Dari 15 area praktek keamanan, terdapat 6 area praktek keamanan yang mempunyai kelemahan yang sangat signifikan dimana terletak pada area yaitu: kesadaran keamanan dan pelatihan, manajemen keamanan, kebijakan keamanan dan peraturan, pemantauan dan audit keamanan TI,

pengesahan otorisasi dan manajemen kerentanan. Masih terdapat banyak kegiatan yang belum dilakukan oleh pihak Inspektorat Daerah Kab. OKU Timur yang sudah ditetapkan oleh OCTAVE-S.

Perubahan strategi perlindungan perlu dilakukan untuk mendukung rencana mitigasi terdapat pada area praktek keamanan bidang kesadaran dan pelatihan keamanan serta area autentifikasi dan otorisasi

Pihak Inspektorat Daerah Kab. OKU Timur harus membuat kebijakan, mekanisme atau prosedur terkait dengan pengendalian keamanan informasi terhadap sistem informasi manajemen tindak lanjut hasil pengawasan maupun untuk instansi yang terdokumentasi dan resmi. Pejabat struktural harus mulai mempertimbangkan membuat anggaran khusus untuk manajemen risiko keamanan informasi dalam mengadakan pelatihan-pelatihan keamanan teknologi informasi secara teratur baik dari segi peningkatan pemahaman atau peningkatan skill dan kemampuan sehingga dapat meminimalisir ancaman risiko yang mungkin terjadi.

Referensi

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE R OS Implementation Guide, Version 1.0. Handbook: CMU*. Retrieved from

Maslan, A. (2013). Analisis Kelayakan Implementasi Cloud Computing dengan Metode Ranti's Generic IS/IT Business Value pada Badan Pengusahaan Batam. *1*.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied computing and informatics, 9*(2), 107-118.

Saragih, S. P. (2018). Implementasi Octave-S Dalam Evaluasi Manajemen Resiko Sistem Informasi Pada Balai Pelatihan Kesehatan Batam. *Jurnal Ilmiah Informatika (JIF)*.

Syalim, A., Hori, Y., & Sakurai, K. (2009). *Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide.* Paper presented at the Availability, Reliability and Security, 2009. ARES'09. International Conference on.

Veljanovska, K., & Zdravevska, V. (2013). E-government based on cloud computing. *Journal of Emerging Trends in Computing and Information Sciences, 4*(4), 377-381.