

BAB II

TINJAUAN PUSTAKA

2.1. Keamanan Informasi

Keamanan informasi menjadi suatu perhatian mendasar bagi bisnis, organisasi, dan pemerintah. Upaya untuk mengamankan aset informasi dari potensi ancaman telah menjadi suatu keharusan. Keamanan informasi, pada dasarnya, membantu menjamin kelangsungan usaha, mengurangi risiko yang mungkin timbul, serta mengoptimalkan laba atas investasi. [7] Dengan semakin banyaknya informasi perusahaan yang disimpan, dikelola, dan dibagikan, risiko kerusakan, kehilangan, atau paparan data kepada pihak eksternal yang tidak diinginkan pun semakin besar. Implementasi keamanan informasi diarahkan untuk mengatasi tantangan dan hambatan, baik yang bersifat teknis maupun non-teknis, seperti memastikan ketersediaan, kerahasiaan, dan integritas informasi, sehingga dapat dinilai tingkat keamanan informasi yang tercapai.[8]

2.2. Website

Website adalah kumpulan halaman yang berisikan informasi, video, audio, gambar maupun sejenisnya yang saling berhubungan dan dapat diakses melalui halaman utama menggunakan browser yang terhubung dengan internet. Website statis terdiri dari informasi yang tidak pernah berubah, sedangkan website dinamis berisikan informasi yang selalu berubah. [9].

2.3. Octave Allegro

Metode OCTAVE Allegro mengikuti delapan langkah yang diungkapkan ke dalam empat fase [10]. Fase awal, yaitu menentukan penggerak, melibatkan satu langkah, yakni menetapkan kriteria pengukuran risiko. Dalam langkah ini, penulis menyusun kriteria pengukuran risiko berdasarkan hasil wawancara, yang bertujuan menjadi pedoman dalam penilaian risiko. Setelah menetapkan kriteria tersebut, langkah berikutnya adalah menetapkan prioritas untuk kawasan dampak. Nilai

tertinggi diberikan pada kategori yang memiliki dampak besar, sedangkan nilai rendah diberikan pada yang memiliki dampak lebih kecil.

Fase kedua meliputi pembuatan profil aset, yang terdiri dari dua langkah, yaitu mengembangkan profil aset informasi dan mengidentifikasi kontainer aset informasi. Pada langkah pengembangan profil aset informasi, semua aset diidentifikasi, dan fokus kemudian ditempatkan pada aset yang dianggap krusial. Selain itu, kontainer aset informasi, yang dapat berupa teknologi (seperti perangkat lunak, perangkat keras, dan aplikasi) maupun non-teknologi (seperti dokumen, lembaran kertas penting, dan karyawan), juga diidentifikasi.

Langkah selanjutnya adalah tahap pemberitahuan ancaman, yang terdiri dari area pemberitahuan perhatian dan pemberitahuan ancaman. Area identifikasi bertujuan untuk mencakup semua potensi ancaman dan kerentanan. Seluruh kemungkinan yang mungkin terjadi pada setiap kontainer aset didokumentasikan. Setelah itu, dokumen ini digunakan untuk mengidentifikasi skenario ancaman yang mencakup pelaku, tujuan, motif, hasil ancaman, kebutuhan keamanan, dan tingkat kemungkinan ancaman terjadi.

Fase terakhir dalam metode ini adalah identifikasi dan mitigasi risiko, yang mencakup identifikasi risiko, analisis risiko, dan pemilihan pendekatan mitigasi. Pada langkah pengenalan risiko, konsekuensi yang mungkin terjadi ditambahkan ke dalam dokumen skenario ancaman. Perkembangan tersebut kemudian dijelaskan untuk menentukan tindakan yang dapat diambil oleh organisasi terhadap risiko yang dihadapi. Hasil analisis pengukuran tingkat keparahan menggunakan perhitungan nilai skor relatif, yang dapat membimbing organisasi dalam melakukan pengurangan risiko.

2.3.1. Tahapan Octave Allegro

Menurut [11] pada OCTAVE Allegro ada langkah- langkah yang dipakai guna mengukur risiko ialah:

Tabel 2.1. Rincian Tahapan Metode OCTAVE Allegro

TAHAP	AKTIVITAS	OUTPUT	WORKSHEET / ACUAN
1	Menetapkan kriteria pengukuran risiko	<ul style="list-style-type: none"> ● Kriteria pengukuran risiko terhadap arahan organisasi ● Peringkat area dampak dari yang paling penting hingga yang tidak penting 	Allegro Worksheet 1-6 dan 7
2	Mengembangkan profil aset informasi	Profil aset informasi kritis	Allegro Worksheet 8
3	Mengidentifikasi container aset informasi	Pemetaan lingkungan risiko aset informasi	Worksheets 9a, 9b, dan 9c
4	Mengidentifikasi area yang di perhatikan	Peta lingkungan risiko aset informasi	Worksheet 10
5	Mengidentifikasi skenario ancaman	<ul style="list-style-type: none"> ● Informasi detail dan hasil pengembangan skenario ancaman dari area yang di perhatikan ● Daftar risiko aset informasi ● Deskripsi tambahan untuk kolom 6 worksheets aset informasi dan container 	<ul style="list-style-type: none"> ● Output tahap 4 (Information Asset Risk Environment Maps) ● Worksheet 10 ● Information Asset Risk Worksheets ● Column (6) worksheets aset informasi dan container
6	Mengidentifikasi risiko	Konsekuensi dari skenario ancaman (kondisi) Tahap 6 Risiko Total = Ancaman kondisi dan konsekuensi di tahap $[4 + 5] + [6]$	Information Asset Risk Worksheet
7	Menganalisis risiko	<ul style="list-style-type: none"> ● Tabel nilai area dampak 	<ul style="list-style-type: none"> ● Risk Measurement

TAHAP	AKTIVITAS	OUTPUT	WORKSHEET / ACUAN
		<ul style="list-style-type: none"> • Tabel skor risiko 	Criteria Step 1 <ul style="list-style-type: none"> • Information Asset Risk Worksheets 10
8	Memilih pendekatan mitigasi	<ul style="list-style-type: none"> • Matriks risiko relatif • Tingkat kerawanan informasi • Mitigasi untuk semua daftar risiko • Strategi mitigasi untuk risiko yang telah diputuskan maka dilakukan mitigasi 	

Sumber: Assessment of Information System Risk Management with Octave Allegro at Education Institution. Suroso J, Fakhrozi MProcedia Computer Science (2018) 135 202-213

1) Membangun Kriteria Pengukuran Risiko

Pada Langkah 1 terdapat dua aktivitas yang dilakukan pada tahap ini, menetapkan penggerak organisasi yang akan digunakan untuk mengevaluasi dampak risiko terhadap misi dan tujuan bisnis organisasi.[12] Driver ini tercermin dalam seperangkat kriteria pengukuran risiko yang akan dikembangkan. Dalam evaluasi Allegro akan menghasilkan serangkaian tolak ukur pengukuran risiko yang menggambarkan bermacam zona imbas yang bernilai (serta bisa jadi spesial) guna lembaga. Misalnya, zona imbas bisa meliputi kesehatan serta keamanan klien serta pegawai, finansial, reputasi, hukum serta peraturan. Satu standar template lembar kegiatan akan dipakai guna membuat tolak ukur ini di sebagian zona imbas serta sesudah itu memprioritaskannya.

A. Langkah 1 Kegiatan 1

Tetapkan selengkap ukuran kualitatif (tolak ukur pengukuran risiko) yang dengannya bisa menilai akibat resiko kepada misi serta tujuan bidang usaha lembaga. Dokumentasikan tolak ukur di Lembar Kegiatan tolak ukur Pengukuran Risiko. Minimum, cermati zona imbas berikut ini:

Tabel 2.2. Urutan Prioritas Area Dampak

Prioritas	Area Dampak
1	Reputasi dan Kepercayaan Pengguna
2	Keamanan
3	Produktivitas
4	Hukum dan Peraturan
5	Keuangan atau Biaya operasional
6	Kesehatan dan Keselamatan

B. Langkah 1 Kegiatan 2

Memprioritaskan zona imbas dari yang sangat bernilai sampai yang tidak bernilai dengan mengenakan lembar kegiatan tingkatan zona imbas (Lembar Kegiatan 7, Lampiran B). Jenis yang sangat bernilai wajib menemukan angka paling tinggi serta sangat tidak bernilai yang sangat kecil.

2) Mengembangkan Profil Aset Informasi

Evaluasi resiko yang dilakukan difokuskan pada aset informasi lembaga. Pada tahap 2 ada 8 kegiatan yang dilakukan, mengawali teknik mendeskripsikan aset informasi tersebut. Setelah itu, mengenali media di mana aset informasi hidup serta lembaga dari kontainer tersebut. Ini akan menunjang untuk seluruhnya mengenali seluruh nilai di mana aset informasi barangkali rentan pada pengungkapan, perubahan, kehilangan atau penghancuran, ataupun kendala. Profil terbuat guna tiap aset informasi, membuat pengenalan bahaya serta resiko dalam strategi berikutnya [13].

A. Langkah 2 Kegiatan 1

Aktivitas awal dalam langkah evaluasi resiko ini mengaitkan pengenalan berkas aset informasi dimana evaluasi bisa dilakukan. Evaluasi tersebut membagikan beberapa besar manfaat apabila berpusat pada aset informasi yang sangat berarti untuk organisasi. Bergantung pada tingkat di mana akan melakukan penilaian risiko ini, organisasi mungkin diganti oleh departemen, divisi, atau sublevel organisasi lainnya.

B. Langkah 2 Kegiatan 2

Berfokus pada beberapa kritis adalah prinsip manajemen risiko yang penting. Dengan demikian, harus melakukan penilaian risiko terstruktur hanya pada aset-aset yang penting untuk mencapai tujuan dan mencapai misi organisasi, dan juga hal-hal yang penting karena faktor-faktor seperti kepatuhan terhadap peraturan.

C. Langkah 2 Kegiatan 3

Dalam kegiatan berikut harus mengumpulkan informasi tentang aset informasi yang diperlukan untuk memulai proses penilaian risiko terstruktur. Gunakan Critical Information Asset Profile (Lembar Kerja 8, Lampiran B) untuk mencatat informasi ini. Untuk memulai, catat nama aset informasi penting di kolom (1) dari Critical Information Asset Profile.

D. Langkah 2 Kegiatan 4

Dokumentasikan dasar pemikiran untuk memilih aset informasi penting di kolom (2) dari Critical Information Asset Profile.

E. Langkah 2 Kegiatan 5

Catatlah deskripsi untuk aset informasi penting di kolom (3) profil aset informasi kritis. Menentukan ruang lingkup aset informasi dan menggunakan definisi umum yang disepakati.

F. Langkah 2 Kegiatan 6

Mengidentifikasi dan mendokumentasikan pemilik aset informasi penting. Lihat definisi yang diberikan di atas untuk menentukan siapa pemiliknya. Catatlah informasi ini di kolom (4) dari Critical Information Asset Profile.

G. Langkah 2 Kegiatan 7

Tulis persyaratan keamanan guna kerahasiaan, integritas, serta ketersediaan di kolom (5) Lembar kegiatan data kritis. Mulailah dengan meninjau persyaratan yang resmi guna aset informasi, serta lanjutkan dengan memuat data yang memenuhi tiap statement persyaratan keamanan.

H. Langkah 2 Kegiatan 8

Identifikasi persyaratan keamanan terpenting untuk aset informasi dengan menandai 'X' di kotak di samping kategori persyaratan keamanan di kolom (6) Lembar kerja informasi kritis. Menggunakan informasi ini saat anda menentukan dampak potensial dari risiko, jadi penting untuk memilih persyaratan keamanan ini dengan hati-hati.

3) **Mengidentifikasi Informasi Wadah Aset**

Ada tahap 3 hanya terdapat satu kegiatan yang dicoba. Tempat penyimpanan aset, penyimpanan, ataupun pemrosesan data dapat sebagai titik kerentanan serta bahaya yang mematikan aset data. Media rata-rata dikenali selaku sebagian tipe aset teknis, piranti keras, dan lunak, ataupun sistem, namun media juga bisa jadi barang wujud semacam selembur kertas ataupun orang yang berarti untuk lembaga. Media orang sungguh bernilai sehubungan dengan kekayaan intelektual ataupun data yang biasanya sensitif ataupun rahasia. Dalam evaluasi risiko keamanan informasi, pengenalan container amat bernilai guna mengenali resiko kepada aset data itu sendiri. Dengan menggambarkan aset data ke seluruh container yang dilewatinya, aktivitas ini mendeskripsikan batas area serta prasarana teknis yang wajib diusut guna ancaman [14].

A. Langkah 3 Kegiatan 1

Memakai denah area risiko aset data (Lembar Kegiatan 9a, 9b, serta 9c, Lampiran B) mengenali serta mengabadikan media dimana aset data dikemas, dikirim, ataupun diproses sebagai berikut:

1. Memakai Lembar Kegiatan 9a guna mengenali media teknis yang terletak di dasar pengawasan langsung lembaga (intern) ataupun lembaga yang diatur di luar institusi (eksternal).
2. Manfaatkan Lembar Kegiatan 9b guna mengenali posisi wujud tempat peninggalan data terdapat di dalam maupun di luar organisasi.
3. Lembar Kegiatan Konsumen 9c buat mengenali banyak orang dalam maupun eksternal lembaga yang barangkali mempunyai wawasan mendetail mengenai aset data.

4) Mengidentifikasi Area yang diperhatikan

Hanya terdapat satu kegiatan di tahap 4, mengawali teknik pengembangan profil risiko aset data. Zona ini sebagai karakteristik bahaya yang istimewa untuk lembaga serta situasi pengoperasiannya yang istimewa. Tujuan dari tahap ini bukan buat menjaring himpunan sempurna seluruh skema bahaya yang bisa jadi guna aset data.

A. Langkah 4 Kegiatan 1

Guna melaksanakan kegiatan ini, manfaatkan denah area data aset resiko guna rekomendasi serta lembar kegiatan risiko aset data (Lembar Kegiatan 10, Lampiran A) guna menulis aspek kepedulian. Buat mengenali zona yang jadi kepedulian, lakukan langkah-langkah selanjutnya:

1. Memakai denah area risiko aset data, meninjau lagi tiap container yang dicantumkan guna membuat dialog mengenai zona potensial yang jadi kepedulian.

2. Dokumentasikan setiap aspek kepedulian yang diidentifikasi di lembar kegiatan risiko aset data. Pada lembar kegiatan, catat sebutan aset data serta dokumentasikan zona yang jadi kepedulian sedetail mungkin. Lengkapi kolom yang diberi identitas "Aset Data" serta "Zona Perhatian" pada lembar kegiatan serta ketahuilah guna memakai lembar kegiatan terpisah guna tiap zona kepedulian yang di pengenalan.
3. Perluas aspek kepedulian buat menghasilkan sketsa bahaya. skema bahaya merupakan ungkapan sifat bahaya yang lebih rinci. Guna tiap zona kepedulian yang sudah di tulis di lembar kegiatan risiko aset data, kolom utuh (1) hingga (4) dengan merekam aktor, arti, corak, serta hasil. Apabila tidak bisa menuntaskan sebagian bagian ini, perkenankan kosong.
4. Dalam kolom (5) mengabadikan gimana bahaya ini hendak pengaruhi persyaratan keamanan yang sudah diresmikan guna aset data. Lalu jalani kegiatan ini guna tiap lembar kegiatan risiko aset data hingga seluruh zona kepedulian yang sudah diperluas. Data resiko yang tertinggal hendak digabungkan pada tahap berikutnya.
5. Lanjutkan melalui tiap- tiap media yang tertera di denah area risiko aset data serta daftarkan sebesar bisa jadi aspek yang jadi kepedulian. Ingat, satu media bisa menimbulkan pengenalan satu ataupun lebih zona yang jadi perhatian.

5) Identifikasi Skenario Ancaman

Pada Langkah 5 ada tiga aktivitas yang dilakukan yaitu mencatat area kekhawatiran yang dapat mempengaruhi aset informasi. Dalam langkah ini, area yang menjadi perhatian diperluas menjadi skenario ancaman yang lebih jauh menjelaskan sifat ancaman. Untuk memperluas area yang menjadi perhatian dalam skenario ancaman, harus terlebih dahulu memahami komponen dasar dari sebuah ancaman.

Langkah ini berguna untuk memberikan pertimbangan atas kemungkinan dalam skenario ancaman. Kemungkinan ini kemudian dibagi ke dalam high, medium, atau low.

Tabel 2.3 Pelaku Ancaman

ASET INFORMASI	PELAKU		
	Internal		External
	WEB	Sekolah Darma Bangsa	
Data kebutuhan koleksi baru	Kepala sekolah Staff	Guru Staff Tidak diketahui	Tidak diketahui
Informasi proses pembelian koleksi baru	Staff Tidak diketahui	Kepala sekolah Tidak diketahui	Tidak diketahui
Data koleksi	Kepala IT Staff	WEB	Pihak pengembang
Dokumen elektronik	Staff Tidak diketahui	Tidak diketahui Pembuat dokumen	Tidak diketahui
Sistem pengelolaan infrastruktur dan penanggulangan bencana	Kepala sekolah Staff Tidak diketahui	Kepala sekolah Staff Tidak diketahui	Pihak pengembang
Data anggota	Staff	Operator Anggota	Pihak pengembang
Data koleksi siacad	Kepala sekolah Staff	Anggota	

A. Langkah 5 Kegiatan 1

Dalam aktivitas ini, akan mengenali skema bahaya ekstra yang belum diunggulkan oleh zona yang jadi kepedulian. Guna menerapkan ini,

Manfaatkan" Appendix C- Threat Scenarios Questionnaires." Terdapat satu angket guna tiap kategori media (teknis, wujud, serta insan). Tiap angket bermuatan gabungan skema yang diiringi oleh persoalan yang didesain guna menolong bibit pengenalan bahaya ekstra. Buat menuntaskan kegiatan ini, manfaatkan denah area aset data yang untuk di Tahap 4 (Lembar Kegiatan 9a, 9b, serta 9c) sebagai panduan.

1. Lanjutkan ke skenario- skenario bahaya 1- Wadah Teknis. Mengenang media teknis yang dicantumkan di Lembar Kegiatan 9a, jawablah pertanyaannya. Lingkari reaksi yang pas.
2. Lanjutkan melalui scenario- skenario bahaya 2- skenario wujud serta sketsa bahaya 3- Orang. Manfaatkan lembar kegiatan 9b serta 9c guna menolong dalam menuntaskan angket.

Tabel 2.4. Ancaman pada Area yang diperhatikan

Area yang diperhatikan	Ancaman	
Usulan kebutuhan siacad baru yang disampaikan kepada Kepala IT tidak mempunyai data yang jelas	<i>Actor</i>	Guru, Staff
	<i>Means / Cara</i>	Mengusulkan kebutuhan siacad baru yang tidak lengkap data sehingga sekolah bisa salah mendata
	<i>Motif</i>	Ketidaksengajaan karena tidak mengetahui data yang lengkap
	Hasil	Penghancuran Modifikasi
	Persyaratan Keamanan	Memastikan usulan semua pihak disertai dengan data yang lengkap
	Kemungkinan	Sedang

B. Langkah 5 Kegiatan 2

Dalam aktivitas ini, memenuhi lembar kegiatan risiko aset data guna tiap-tiap skema bahaya generik yang di pengenalan guna dipikirkan pada daftar pertanyaan.

1. Meninjau asumsi pada scenario- skenario bahaya. Tidak perlu melaksanakan apapun lebih jauh guna tiap skema di mana Anda memutar" tidak".
2. Guna seluruh tanggapan" benar", tulis lembar kegiatan risiko aset data terkini. Lengkapi bagian(1) hingga(5) pada lembar kegiatan ini. Bila menciptakan jika yang sudah menanggapi" benar" guna suatu persoalan, tetapi tidak bisa menciptakan suasana kehidupan nyata yang serupa, lanjutkan.
3. Lalu hingga paling tidak terdapat satu Lembar Kegiatan Risiko Aset Data yang dituntaskan guna tiap tanggapan" benar" pada tiap angket skema bahaya.

C. Langkah 5 Kegiatan 3

Aktivitas ini bersifat opsional guna seluruh profil risiko aset data. Apabila memilah guna melaksanakannya, Jalani di seluruh profil. Serta pula wajib mengakhirkan guna meningkatkan mungkin pada cerita skema bahaya yang di ambil di lembar kegiatan risiko aset informasi peluang menunjang memastikan skema mana yang lebih mungkin diserahkan pada kondisi operasi spesial. Ini akan bermanfaat sesudah itu dalam memastikan bagaimana memprioritaskan aktivitas mitigasi risiko. Sebab seringkali sungguh susah guna mengukur peluang dengan cara tepat(paling utama bertepatan dengan kerentanan serta peristiwa keamanan), peluang diumumkan dalam evaluasi resiko ini dengan cara kualitatif seperti tinggi, sedang, maupun kecil. Dengan kata lain, memastikan apakah terdapat kemungkinan(tinggi) yang kokoh jika skema yang sudah di dokumentasikan bisa terjalin, kesempatan menengah(adil), ataupun bila

skema tidak mungkin(kecil). Bila memilah guna membuat ketetapan ini, wajib mengecek kotak peluang yang serupa di kolom(6) guna masing-masing lembar kegiatan resiko yang terbuat.

6) Identifikasi Risiko

Pada tahap keenam, akibat untuk lembaga seandainya suatu bahaya terjaln dicatat, dalam memperoleh cerminan resiko dengan cara komplit. Suatu bahaya bisa memiliki dampak– dampak yang potensial untuk lembaga.

Tabel 2.5. Cara Menghitung Skor terhadap Area Dampak

Area dampak	Prioritas	Nilai Prioritas	Dampak Nilai		
			Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi serta Keyakinan Konsumen					
Keamanan					
Produktivitas					
Hukum dan Peraturan					
Finansial maupun Anggaran operasional					
Kesehatan serta Keamanan					

A. Langkah 6 Kegiatan 1

Dalam aktivitas ini, memastikan bagaimana skema bahaya yang ditulis di lembar kegiatan risiko aset informasi masing- masing bisa mempengaruhi lembaga.

1. Guna tiap skema bahaya yang didokumentasikan di lembar kegiatan risiko aset informasi, ditetapkan bagaimana lembaga hendak terserang

akibat bila skema bahaya ini terakumulasi. Inilah akibat dari bahaya serta memenuhi pertemuan resiko.

2. Dokumentasikan minimal satu akibat dalam bagian(7) lembar kegiatan risiko aset informasi. Akibat catatan sanggup didokumentasikan sekecilnya. Guna memikirkan zona imbas dari patokan penilaian resiko guna memikirkan konsekuensinya. Cermati serta hasil yang dipikirkan di Tahap 5, Kegiatan 5.

7) Analisis Risiko

Pada Langkah 7, secara kualitatif mengukur sejauh mana organisasi dipengaruhi oleh ancaman dengan menghitung nilai risiko untuk setiap risiko terhadap setiap aset informasi. Informasi penilaian ini digunakan untuk menentukan risiko yang harus segera diatasi dan untuk memprioritaskan tindakan mitigasi untuk sisa risiko pada Langkah 8. Dalam aktivitas ini, akan menciptakan angka risiko relatif. Angka risiko relatif didapat dengan memikirkan sepanjang mana akibat dari risiko pengaruh lembaga dibandingkan dengan kebutuhan relatif dari bermacam zona imbas. Dengan tutur lain, bila zona " nama baik" sangat berarti untuk lembaga serta akibat dari sesuatu risiko menimbulkan akibat yang besar kepada nama baik, bisa jadi butuh mengutip kegiatan guna membenarkan kalau risiko ini dikurangi. Dengan memakai standar ini, membenarkan kalau risiko ditaksir dalam kondisi pengantar lembaga.

Tabel 2.6. Skor Risiko Relatif

Aset Informasi	Skor Risiko Relatif	
	Terendah	Tertinggi
Data kebutuhan		
Koleksi baru		
Pembelian koleksi baru		
Data koleksi baru		
Dokumen elektronik		
Sistem pengelolaan infrastruktur dan penanggulangan bencana		
Data anggota		
Data WEB		

A. Langkah 7 Kegiatan 1

Mulailah dengan meninjau standar pengukuran risiko yang untuk di Tahap 1, Kegiatan 1. Fokus pada bagaimana mendeskripsikan imbas besar, menengah, serta kecil guna lembaga. Dengan memakai standar pengukuran risiko selaku bimbingan, penilaian akibat relatif kepada tiap-tiap zona akibat serta tulis angka " besar," " lagi," ataupun " kecil" di kolom " Angka" kolom(8). Bila sudah menulis lebih dari satu statement akibat, yakinkan guna memikirkan seluruhnya sebab wajib membebaskan angka ke zona akibat. setelah itu menulis angka di tiap- tiap zona imbas.

B. Langkah 7 Kegiatan 2

Pada tahap ini, angka resiko relatif akan dihitung yang bisa dipakai guna menganalisa resiko serta menunjang lembaga memastikan strategi risiko

yang tepat. Anda akan melaksanakan tahap ini di kolom " Angka" kolom(8) pada tiap- tiap Lembar Kegiatan Risiko Aset Data.

1. Jumlah angka guna tiap zona imbas dengan memperbanyak besar zona akibat dengan angka akibat.(Amati lembar kegiatan tingkatan zona imbas yang untuk di Tahap 1, Kegiatan 2.) Tulis hasilnya di kolom" angka". Angka akibat diberi angka kuantitatif sebagai berikut: Tinggi- 3, Sedang- 2, serta Rendah- 1. Yakinkan guna melindungi nilai- nilai ini senantiasa tidak berubah- ubah di semua lembar kegiatan resiko.
2. Keseluruhan kolom angka. Keseluruhan ini merupakan angka resiko relatif.
3. Cermati ilustrasi selanjutnya. lembaga itu meletakkan zona akibatnya semacam yang ditunjukkan di dasar ini. Zona finansial dikira selaku zona imbas yang sangat berarti serta keamanan serta kesehatan yang sangat tidak bernilai. Angka akibat diserahkan di Aktivitas 1 sebab konsekuensinya dipikirkan.

8) Pendekatan Mitigasi

Pendekatan mitigasi adalah metode bagaimana website sekolah hendak memutuskan untuk menanggulangi resikonya. OCTAVE Allegro membagikan pendekatan mitigasi yang bisa diseleksi, ialah: menerima (accept), mitigasi atau mengurangi (mitigate), serta menunda (defer). Untuk mengawali mitigasi, awal menyusunkan tiap-tiap resiko angka relatifnya. Setelah itu terbuat pengkategorian buat mempermudah melaksanakan pendekatan mitigasi tiap resiko. Pengelompokan bersumber pada angka resiko relatif hasil analisa resiko langkah 7 serta kebolehjadian terbentuknya bahaya hasil langkah 5.

Tabel 2.7. Matriks Risiko Relatif dengan Probabilitas Ancaman

Probabilitas	Skor risiko relatif		
	(30-45)	(16-29)	(0-15)
Tinggi	<i>POOL 1</i>	<i>POOL 2</i>	<i>POOL 2</i>
Sedang	<i>POOL 2</i>	<i>POOL 2</i>	<i>POOL 3</i>
Rendah	<i>POOL 3</i>	<i>POOL 3</i>	<i>POOL 3</i>

Masing-masing kategori tersebut di atas dapat menggambarkan tingkat kerawanan informasi, yaitu sebagai berikut:

1. Kategori 1 merupakan tingkat yang paling rawan informasinya.
2. Kategori 2 merupakan tingkat yang rawan informasinya.
3. Kategori 3 merupakan tingkat yang cukup rawan informasinya.
4. Kategori 4 merupakan tingkat yang tidak rawan informasinya.

A. Langkah 8 Kegiatan 1

Aktivitas awal di Tahap 8 merupakan memisahkan tiap- tiap resiko yang sudah Anda pengenalan dengan angka resikonya. Mengkategorikan risiko dengan cara teratur hendak menunjang buat mulai membuat ketetapan hal status mitigasi. Terdapat banyak metode untuk suatu lembaga guna mengkategorikan resikonya. Salah satu metode mudahnya merupakan mengawali dengan memilah resikonya dari yang paling tinggi ke yang terendah. Setelah itu pisahkan resikonya jadi 4 kolam dengan jumlah resiko yang serupa. Resiko dengan angka paling tinggi wajib terletak di zona awal(Pool 1), resiko dengan angka paling tinggi selanjutnya di antrian kedua(Pool 2), paling tinggi selanjutnya di ketiga(Pool 3), serta

angka terendah di Keempat (kolam 4). Desain klasifikasi yang lain bisa jadi masuk ide untuk lembaga. Bila lembaga memakai peluang, bisa jadi ingin memikirkan buat meningkatkan matriks resiko guna mengkategorikan risiko yang teridentifikasi. diagram matrik risiko relatif di dasar ini membuktikan ilustrasi gimana melaksanakan perihal ini. Berikut menetapkan pendekatan mitigasi untuk setiap risiko. Berdasarkan analisis di atas, maka ditetapkan status mitigasi untuk SIAKAD, yaitu:

Tabel 2.8. Pendekatan dan Pengurangan Risiko

<i>Risk Relative Matrix</i>		
<i>Risk Score</i>	<i>POOL</i>	<i>Mitigation Approach</i>
30-45	1	<i>Mitigasi</i>
16-29	2	<i>Defer</i>
0-15	3	<i>Accept</i>

B. Langkah 8 Kegiatan 2

Tetapkan pendekatan mitigasi guna tiap resiko. Pikirkan guna memakai yang selanjutnya selaku pedoman, tetapi ketahuilah kalau ketetapan mengenai pendekatan mitigasi amat tergantung pada suasana pembedahan istimewa lembaga, jadi janganlah memanfaatkan denah ini sekedar guna menyudahi bagaimana menanggulangi resiko yang sudah diidentifikasi.

C. Langkah 8 Kegiatan 3

Guna seluruh profil risiko yang diputuskan guna dikurangi, setelah itu meningkatkan strategi mitigasi. Dengan mengenang aksi yang bisa dicoba guna kurangi resiko, mulailah memikirkan strategi mitigasi guna tiap resiko yang sudah diputuskan buat kurangi, selaku selanjutnya:

1. Cermati media dimana pengawasan hendak diimplementasikan. (Media ini bisa ditemui di Denah Area Risiko Aset Data).
2. Jelaskan pengawasan yang hendak dilaksanakan serta risiko residual kepada peninggalan sehabis pengawasan diaplikasikan.

Selanjutnya sebagian persoalan yang butuh dipikirkan pada dikala meningkatkan strategi mitigasi risiko:

1. Bagaimana pemeran dilindungi guna tidak memanfaatkan kelemahan?
2. Bagaimana metode yang bisa dicoba pemeran itu dilindungi?
3. Bagaimana pola dilindungi?
4. Bagaimana hasilnya dapat dilindungi?
5. Bisakah peluang bahaya dikurangi?
6. Bila tidak terdapat aktivitas proaktif yang bisa dicoba, dapatkah akibat dari bahaya itu dikurangi?
7. Dapatkah lembaga meminimalkan akibat ataupun akibat dari resiko yang direalisasikan?
8. Bagaimana persyaratan keamanan guna peninggalan data ini dipadati oleh strategi mitigasi?

2.4. PENELITIAN YANG RELEVAN

Penelitian ini mengacu pada beberapa penelitian sebelumnya menggunakan metode yang sama terdapat pada tabel 2.3.9.

Tabel 2.9. Penelitian Terdahulu

No	Nama Peneliti	Judul Penelitian	Hasil Penelitian
1	Awad A, Shokry M, Khalaf A et al. (2023)	ASSESSMENT OF POTENTIAL SECURITY RISKS IN ADVANCED METERING INFRASTRUCTURE USING THE OCTAVE ALLEGRO APPROACH [15]	Dalam studi ini, sistem AMI (<i>Advanced Metering Infrastructure</i>) akan dinilai dengan lembar kerja OA (<i>Octave Allegro</i>) versi 1. Setiap lembar kerja digunakan dalam satu tahap pendekatan OA. Tahap pertama pendekatan penilaian risiko OA adalah menetapkan area pengukuran dan memeringkatnya berdasarkan tingkat signifikansi. Lembar kerja 1 menyarankan

No	Nama Peneliti	Judul Penelitian	Hasil Penelitian
			<p>beberapa area dampak, tiga di antaranya dipilih karena terkena dampak serangan siber terhadap sumber daya informasi penting sistem AMI: keuangan, produktivitas, serta reputasi dan kepercayaan pelanggan. OA dipilih sebagai pendekatan yang tepat berdasarkan studi perbandingan metode ISRA. Proses perbandingan menyelaraskan persyaratan AMI dengan kemampuan metode ISRA (<i>Information Security Risk Assessment</i>). Untuk menganalisis risiko keamanan potensial apa pun, sistem AMI dievaluasi melalui delapan langkah metodologi OA. Melalui implementasi OA, sebelas skenario risiko diidentifikasi yang memengaruhi kerahasiaan, integritas, atau ketersediaan sistem AMI. Untuk kelengkapan, studi ini merekomendasikan pendekatan mitigasi risiko untuk membatasi risiko yang teridentifikasi terkait dengan sistem AMI.</p>
2	Nadiya K, Choirun Nisa N, Annafi' S et al. (2024)	ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK OCTAVE ALLEGRO [16]	<p>Dalam penelitian ini ditentukan 5 impact areas diantaranya yaitu reputasi dan kepercayaan pengguna, keamanan dan kesehatan, produktivitas, finansial, serta denda dan penalti, serta berfokus pada 5 areas of concern. Hasil penilaian risiko tersebut dapat dijadikan panduan untuk membuat perencanaan strategis guna menjaga aset informasi dengan tepat.</p>
3	Wini Astuti R, Putra R, Putra I (2023)	PENILAIAN RISIKO PENGGUNAAN SISTEM INFORMASI AKADEMIK PADA STIQ AL-LATHIFIYYAH PALEMBANG DENGAN METODE OCTAVE ALLEGRO [17]	<p>Disimpulkan bahwa penelitian dilakukan dengan metode Octave Allegro cocok untuk penilaian risiko. Penelitian ini menggunakan lima impact areas yaitu: reputasi dan kepercayaan pengguna, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan hukum. Penelitian ini menunjukkan</p>

No	Nama Peneliti	Judul Penelitian	Hasil Penelitian
			adanya 5 ancaman risiko. 4 risiko dengan pendekatan mitigasi yang harus dikurangi (mitigate) dan 1 risiko dengan pendekatan diterima (Accept).
4	Indrayani N, Amalia N	RISK ANALYSIS OF INFORMATION SECURITY IN BALIKPAPAN INTERNATIONAL AIRPORT SERVICE DESK PLUS (SDP) USING THE OCTAVE ALLEGRO METHOD [18]	Mengatasi kesalahan kata sandi data pengguna, pemadaman internet, dan risiko infiltrasi file, organisasi telah melakukan hal ini secara signifikan mengurangi potensi insiden keamanan. Selain itu, penerapan pengendalian dan tindakan yang tepat, seperti kebijakan kata sandi, rencana redundansi, dan sistem antivirus, telah memperkuat postur keamanan SDP secara keseluruhan.