MANAJEMEN RISIKO PADA LEARNING MANAGEMENT SYSTEM MENGGUNAKAN KERANGKA KERJA OCTAVE ALLEGRO

Putri Aristasari[1], Imam Riadi[2]
[1]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan
Universitas Ahmad Dahlan
Email: putri1500016061@webmail.uad.ac.id
[2] Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan
Universitas Ahmad Dahlan
Email: imam.riadi@is.uad.ac.id

Submitted :..... Reviewed :..... Accepted:.....

ABSTRAK

Learning Management System merupakan contoh dari penerapan teknologi informasi yang berfungsi sebagai penunjang kegiatan belajar mengajar konvensional antara siswa dengan guru. Selain manfaat yang dapat dirasakan, penerapan teknologi juga dapat menimbulkan berbagai hambatan yang umumnya disebut sebagai risiko. Risiko jika benar-benar terjadi, dapat menimbulkan kerugian bagi instansi. Diperlukan kesadaran dari pihak instansi untuk meminimalkan risiko tersebut dengan melakukan penilaian risiko. Tujuan dari penelitian ini adalah menilai risiko berdasarkan aspek *technical container* (TC), *physical container* (PhC) dan *people container* (PC) pada aset infromasi kritis *Learning Management System* menggunakan kerangka kerja OCTAVE Allegro. Penilaian risiko dengan OCTAVE Allegro terdapat 8 tahap yang harus diselesaikan yang diklasifikasikan ke dalam 4 fase. Hasil utama penelitian ini adalah berupa prioritas risiko yang harus di mitigasi dari setiap *container* dan rekomendasi strategi mitigasi risiko berdasarkan *relative risk score*. Dari penelitian yang dilakukan menghasilkan 7 *area of concern* dengan pendekatan mitigasi menghasilkan mitigate berjumlah 3, *defer* berjumlah 3, *accept* berjumlah 1. Prioritas risiko dari aspek *technical container* memiliki *relative risk score* 39 dengan strategi pengurangan risiko *mitigate*. Prioritas risiko dari aspek *physical container* memiliki *relative risk score* 19 dengan strategi pengurangan risiko *defer*. Prioritas risiko dari aspek *people container* memiliki *relative risk score* 20 dengan strategi pengurangan risiko *accept*.

Kata kunci: *Penilaian Risiko, Manajemen Risiko, Learning Management System, OCTAVE Allegro*

PENDAHULUAN

Perkembangan teknologi informasi yang terjadi saat ini, membuat banyak instansi yang memanfaatkan perkembangannya untuk mendorong proses bisnis. Banyak instansi yang telah menerapkan teknologi informasi tersebut termasuk sekolah. Salah satu yang telah diterapkan yaitu Learning *Management System* atau biasa disingkat LMS. LMS merupakan sistem pembelajaran elektronik yang digunakan untuk membantu pola pembelajaran konvensional yang memungkinkan siswa untuk belajar kapanpun dan dimanapun dengan fitur-fitur yang

disediakan, sehingga tuntutan pemahaman siswa terhadap materi pembelajaran dapat terpenuhi dengan terbatasnya waktu belajar di kelas.

Banyak manfaat yang didapatkan dari pemanfaatan sistem informasi, selain berupa kecepatan dan kemudahan akses, penggunaan sistem informasi juga rentan terhadap kerusakan, sabotase serta tindak kejahatan (Suduc, 2010). Dampak kerusakan sistem informasi dapat menyebabkan kerugian secara finansial, menurunya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan (Maulana&Supangkat, 2006). Berdasarkan hasil observasi pendahuluan yang dilakukan sebelumnya, gangguan yang pernah terjadi selama proses pembelajaran berlangsung adalah gangguan pada server LMS yang mengakibatkan pelayanan LMS menjadi terhenti. Perbaikan yang dilakukan oleh Administrator IT hanya melaksanakan kegiatan perbaikan berdasarkan kejadian yang saat itu terjadi.

Diperlukan kesadaran pihak sekolah untuk mengelola dan meminimalkan risiko dengan melakukan penilaian risiko. Metode OCTAVE Allegro dipilih sebagai kerangka kerja proses penilaian risiko yang akan dilakukan pada penelitian ini.

Adapun rumusan maslah dari penelitian ini yaitu (1) bagaimana penilaian risiko dari aspek technical, physical dan people pada LMS (2) Bagaimana menentukan prioritas risiko dan membuat rekomendasi strategi mitigasi risiko pada LMS.

METODE PENELITIAN

Alat dan Bahan

Penelitian ini memerlukan alat dan bahan yang digunakan untuk proses penelitian seperti pada tabel I

Tabel I. Alat dan Bahan Penelitian

Alat	Bahan
Framework OCTAVE Allegro yang dikeluarkan oleh SEI Caeneige Mellon University.	Data yang diperoleh langsung dari hasil survei, yaitu wawancara dan kuesioner.
Perangkat keras *(hardware)* Processor : Intel Celeron N3350 – 64 bit RAM : 4GB Memory : SSD 128 GB Perekam suara dan kamera pada *smartphone*	
Software Sistem Operasi : Microsoft Windows 10 Pro 64-bit Pengolah data : Microsoft Word 2016	

Jalannya Penelitian

Penelitian ini menggunakan dua pendekatan, yaitu kualitatif dan kuantitatif. Kualitatif dilakukan dengan wawancara dan analisis dokumen yang dimiliki instansi. Pendekatan kuantitatif dilakukan dengan *scoring* terhadap risiko-risiko yang teridentifikasi berdasarkan hasil data kualitatif yang di dapatkan agar pendekatan mitigasi yang sesuai dapat ditentukan untuk masing-masing risiko. Penelitian ini dilakukan dengan menggunakan acuan dalam langkah-langkah OCTAVE Allegro. OCTAVE Allegro terdiri dari delapan langkah yang diklasifikasikan menjadi empat fase kategori.

1. Fase 1 (*Establish Driver*)

   Pada fase 1 ini memuat langkah ke-1 OCTAVE Allegro

   1) Langkah 1 (Membangun *Risk Measurement Criteria*)

      Aktivitas pertama dengan menentapkan drivers yang akan direfleksikan dalam *risk measurement criteria*. Untuk memfasilitasi kegiatan ini, terdapat lima standar kerja dari impact area reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan dan denda/ hukuman dengan penilaian low, mediun atau high. Aktvitas kedua yaitu dengan membuat prioritas *impact area* yang terpenting mendapatkan skor tertinggi dan yang tidak begitu penting mendapatkan skor terendah.

2. Fase 2 (*Profile Assets*)

   Fase ini memuat dua langkah, yaitu langkah kedua dan langkah ketiga.

   1) Langkah-2 (Mengembangkan Profil Aset Informasi)

      Aktivitas pertama dan kedua yang dilakukan adalah mengidentifikasi aset informasi paling penting dalam organisasi dengan mengajukan beberapa pertanyaan kepada pihak terkait. Aktivitas ketiga sampai aktivitas kedelapan adalah melakukan pengisian *Information Assets Profile* untuk mengumpulkan informasi tentang aset informasi yang diperlukan untuk memulai penilaian risiko.

   2) Langkah-3 (Mengidentifikasi *Containers* dari Aset Informasi)

      Melakukan identifikasi terhadap setiap *container* aset informasi. *Container* tersebut meliputi *technical container*, *physical container* dan *people container*. Langkah ini di dokumentasikan menggunakan *Information Risk Environtment Map*.

3. Fase 3 (*Identify Threats*)

   Fase ini memuat 2 langkah yaitu langkah keempat dan kelima.

   1) Langkah-4 (Mengidentifikasi *Areas of Concern*)

      Mengidentifikasi *areas of concern* berdasarkan *container* yang sudah ditentukan pada proses sebelumnya dengan mengacu pada dokumen *Information Assets Risk*

Environment Maps. Setelah itu *mereview* dari *container* untuk menentukan *Areas of Concern* dan mendokumentasikan setiap *Areas of concern*.

2) Langkah-5 (Mengidentifikasi *Threat Scenario*)

Aktifitas pertama yang dilakukan adalah mengidentifikasi *threat scenario* tambahan yang belum ada pada *area of concern* dengan menggunakan kuesioner *Appendix C-Threat Scenarios Questionares*. Aktivitas kedua yaitu memperjelas ancaman dengan mengidentifikasi *threat scenario* dengan memberikan gambaran secara rinci mengenai properti dari *threat*, antara lain *actor, means, motives, outcome* dan *securtiy*. Aktivitas ketiga adalah mementukan *probabilitas* dari deskripsi *threat scenario* yang telah dibuat.

4. Fase 4

Fase keempat memuat tiga langkah, yaitu langkah keenam, langkah ketujuh dan langkah kedelapan.

1) Langkah-6 (Mengidentifikasi Risiko)

Menentukan *threat scenario* terhadap gambaran risiko secara rinci dan menentukan tingkat level dari level *low*, *medium*, atau *high*. *Threat scenario* tersebut di dokumentasikan dalam bentuk *Information Asset Risk Worksheet*. Aktifitas berikutnya dilanjutkan dengan penghitungan *relative score*. *Relative score* digunakan untuk membantu menganalisis risiko serta menentukan strategi mitigasi yang tepat.

2) Langkah-7 (Menganalisis Risiko)

Mengukur seberapa jauh dampak yang ditimbulkan dari sebuah ancaman dengan menghitung *relative risk score*. *Relative risk score* didapatkan dengan menentukan *value* dari setiap *impact area* dan memberikan *score* terhadap masing-masing *impact value*, kemudian djumlahkan.

3) Langkah-8 (Memilih Pendekatan Mitigasi)

Aktivitas pertama adalah mengklasifikasikan setiap risiko yang telah diidentifikasi berdasarkan skor risikonya. Pengklasifikasian menggunakan acuan *relative risk matrix*. Aktivitas kedua yaitu menentukan pendekatan mitigasi untuk setiap risiko berdasarkan *relative risk matrix*.

HASIL DAN PEMBAHASAN

1. Fase 1 (*Establish Drivers*)

1) Langkah-1 (Membangun *Risk Measurement Criteria*)

Aktivitas pertama adalah menetapkan *drivers* sebuah organisasi atau instansi terkait dengan mengajukan beberapa pertanyaan untuk memilih *impact area* yang terpenting. Dalam OCTAVE Allegro terdapat 5 *impact area* yang diukur dengan ukuran *low, medium* atau *high*. Reputasi dan kepercayaan user, finansial dan produktivitas dipilih sebagai *impact area*. Contoh *impact area* pada produktivitas dapat dilihat pada tabel II

Tabel II. *Allegro Worksheet*-1 (*Impact Area* – Reputasi dan Kepercayaan *user*)

Allegro Worksheet 1	***Risk Measurement Criteria – Rreputasi dan Kepercayaan User***		
Impact Area	***Low***	***Medium***	***High***
Reputasi dan kepercayaan *customer*	1. Kepercayaan guru dan siswa terhadap LMS sedikit sekali atau tidak terpengaruh. 2. Dibutuhkan usaha kecil atau tidak ada usaha untuk perbaikan. 3. Reputasi dan kepercayaan *user* menurun sebanyak 40%.	1. Kepercayaan guru dan siswa terhadap LMS terpengaruh. 2. Dibutuhkan usaha untuk perbaikan relatif lama. 3. Reputasi dan kepercayaan *user* menurun sebanyak 40% hingga 70%.	1. Kepercayaan guru dan siswa terhadap LMS sangat terpengaruh. 2. Dibutuhkan usaha perbaikan sangat lama. 3. Reputasi dan kepercayaan *user* menurun sebanyak lebih dari 70%.
Kehilangan user	Dampak kehilangan *user* tidak ada, karena LMS hanya *tool* pendamping dan penggunanya merupakan *intern* sekolah. Di sisi lain penggunaan LMS di sekolah sudah terikat dengan peraturan bahwa guru dan siswa wajib menggunakan LMS.		

Aktvitas kedua yaitu dengan membuat prioritas *impact area* yang terpenting mendapatkan skor tertinggi dan yang tidak begitu penting mendapatkan skor terendah. Tabel III menunjukan hasil dari penetapan skor *impact area*

Tabel III. *Impact Area Prioritization*

Allegro Worksheet 7	***Worksheet Skor Prioritas Impact Area***
Skor Prioritas	***Impact Areas***
4	Reputasi dan Kepercayaan *Customer*
3	Finansial
5	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Fase 2 (*Profile Assets*)

Fase ini memuat dua langkah, yaitu langkah kedua dan langkah ketiga.

1) Langkah-2 (Mengembangkan Profil Aset Informasi)

Aktivitas pertama diawali dengan mengidentifikasi kumpulan aset-aset kritis LMS. Hasil dari indentifikasi dapat dilihat pada tabel IV

Tabel IV. Daftar aset kritis LMS

NO	Aset-aset	Aset-Aset Kritis
1.	Informasi	*Database* Informasi a. Data Siswa b. Data Guru c. Data Admin d. Konten-konten pembelajaran (Materi Pembelajaran, Soal-soal ujian, Tugas-tugas) e. Data Penilaian (Nilai tugas, Nilai *quiz*, Nilai ujian) f. Forum g. Pesan
2.	Sistem	Aplikasi LMS
3.	*Hardware*	*Server, Router, Switch/Hub, Acces Point Wireless*, Komputer
4.	*Software*	Sistem Operasi Linux
5.	Sumber Daya Manusia	Administrator TI, Guru, Siswa

Aktivitas selanjutnya yaitu mendokumentasikan hasil dari *profilling* masing-masing aset infromasi kritis mengacu pada aset-aset informasi kritis pada tabel IV. Berikut contoh dari *profilling* aset informasi seperti pada tabel V dibawah ini

Tabel V. *Profilling* Aset Informasi

Aset Kritis	Aset Informasi
Deskripsi	Database Infromasi: a) Data Siswa b) Data Guru c) Data Admin d) Konten-konten pembelajaran (Materi Pembelajaran, Soal-soal ujian, Tugas-tugas) e) Data Penilaian (Nilai tugas, Nilai quiz, Nilai ujian) f) Forum g) Pesan
Pemilik	Guru,Siswa dan Administrator TI
Security* : *Confidentiality	Layanan infromasi LMS hanya boleh diakses digunakan oleh pihak yang mendapatkan hak akses, yaitu seluruh guru, siswa dan administrator TI.

	Integrity	Layanan informasi LMS harus jelas, benar dan akurat. Dapat diganti dan diubah hanya oleh pihak yang berwenang saja seperti guru untuk kepentingan pembelajaran dan administrator TI untuk menginput atau memodifikasi value dari database server.
	Availability	Layanan infromasi LMS harus tersedia untuk seluruh guru, seluruh siswa dan administrator TI selama 24 jam 7 hari.

2) Langkah-3 (Mengidentifikasi *Containers* dari Aset Informasi)

Melakukan identifikasi terhadap setiap *container* aset informasi. *Container* tersebut meliputi *technical container (Software, hardware*, sistem, *server*, perangkat jaringan), *physical container* (meliputi item-item dalam bentuk fisik seperti file folder) dan *people container* yang berasal dari internal atau *eksternal* instansi dengan melakukan wawancara pihak terkait. Kemudian dilanjutkan merangkum dan di dokumentasikan menggunakan *Information Risk Environtment Map*. Tabel VI s/d tabel VIII merupakan tabel *information asset risk environtmap* masing-masing *container.*

Tabel VI. *Information Asset Risk Environtment Map (Technical)*

Allegro Worksheet 9a	*Information Asset Risk Environtment Map (Technical)*
Internal	
Container Description	**Owner(s)**
Module : *Database* layanan LMS di dalam server yang didalamnya terdiri dari aset informasi yang digunakan oleh Administrator TI, guru dan siswa dalam menggunakan layanan	Sekolah
Server: digunakan untuk pemyimpanan *database* dengan menggunakan jaringan internet.	Sekolah
Perangkat jaringan : *router, acces point, switch/hub*	Sekolah
Komputer : perangkat komputer *server*	Sekolah
Jaringan internet *internal*: seluruh jaringan yang terhubung ke dalam jaringan intranet dalam gedung sekolah SMA Muhammadiyah 1.	Sekolah
Sistem Operasi *server* Linux	Sekolah
Aplikasi: Learning Management System SMA Muhammadiyah 1 Yogyakarta	Sekolah
Eksternal	
Container Description	**Owner(s)**
Jaringan Internet: Jaringan internet menggunakan vendor pihak ketiga	Telkom
Perangkat jaringan guru, siswa dan administrator TI sebagai penghubung dari dan ke LMS	Guru, siswa dan administrator TI
Antena: untuk terkoneksi ke pihak ketiga	Telkom

Tabel VII. *Information Asset Risk Environtment Map* (*Physical*)

Allegro Worksheet 9a	*Information Asset Risk Environtment Map (Physical)*

Internal	
Container Description	**Owner(s)**
Hardisk Eksternal: Tempat *backup* penyimpanan data siswa dan guru	Administrator TI, Sekolah
Folder File: tempat penyimpanan data siswa dan guru dalam komputer administrator TI	Administrator TI
Eksternal	
Container Description	**Owner(s)**
Tidak ada	Tidak ada

Tabel VIII. *Information Asset Risk Environtment Map* (*People)*

Allegro Worksheet 9a	*Information Asset Risk Environtment Map (People)*
Internal	
Container Description	**Owner(s)**
Administrator TI: Pengelola LMS	Sekolah
Eksternal	
Container Description	**Owner(s)**
Guru: pengguna LMS	Sekolah
Siswa: pengguna LMS	Sekolah
Pihak ketiga penyedia jaringan	Telkom

3. Fase 3 (*Identify Threats*)

Fase ini memuat 2 langkah yaitu langkah keempat dan kelima.

1) Langkah-4 (Mengidentifikasi *Areas of Concern*)

Langkah yang dilakukan adalah mengidentifikasi *areas of concern* di sisi *technical* (TC), *physical* (PC) dan *people* (PC). *Areas of concern* adalah pernyataan deskriptif yang menjabarkan kondisi atau situasi yang sebenarnya yang dapat mempengaruhi aset informasi LMS. Pencatatan *areas of concern* berpedoman pada dokumen *Information Assets Risk Environment Maps*. Tabel IX berikut ini menunjukan daftar *area of concern* yang teridentifikasi.

Tabel IX. *Area of concern*

Area of concern	**Kode**	**Jenis serangan yang terjadi**	***Security Requirments***
Berhentinya layanan LMS dikarenakan *supply* listrik terhenti	TC-1	-	*1) Avaibility*
Pengeksplotasian celah keamanan LMS oleh pihak luar atau dalam sekolah.	TC-2	1) Virus 2) Trojan 3) Worm 4) Spyware 5) DdoS 6) Deface 7) Sistem Crash	*1) Confidentiality* *2) Integrity* *3) Avaibility*

Bocornya hak akses seperti *username* dan *password*.	TC-3	1) SQL-Injection 2) Sniffing Jaringan	*1) Confidentiality* *2) Integrity*
Ruangan *server* yang mudah diakses dapat mengakibatkan server dapat diakses oleh pihak yang tidak berwenang	TC-4	1) Password Cracking 2) Rootkit	*1) Confidentiality* *2) Integrity* *3) Avaibility*
Penyalahgunaan *Hardisk eksternal* dan file folder *back up* data guru, siswa dan admin oleh pihak yang tidak bertanggung jawab.	PC-1	-	*1) Confidentiality* *2) Integrity*

3) Langkah-5 (Mengidentifikasi *Threat Scenario*)

1) Aktifitas pertama yang dilakukan adalah mengidentifikasi *area of concern* tambahan yang yang sudah ada pada tabel IX dengan menggunakan kuesioner *Appendix C-Threat Scenarios Questionares*. Tabel X merupakan hasil identifikasi tambahan *areas of concern*.

Tabel X. *Area of concern*

Area of concern	**Kode**	**Jenis serangan yang terjadi**	***Security Requirments***
Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat yang terkait dengan LMS	TC-5	-	1) *Avaibility*
Sosial Enginering terhadap administrator TI yang mengakibatkan terungkapnya hak akses ke server.	PC-1	1)Spam E-mail 2)Pop-Up Windows 3)Komunikasi langsung melalui internet atau percakapan langsung.	*1) Confidentiality* 2) *Integrity*

Aktivitas selanjutnya adalah memperluas masing-masing *areas of concern* aspek *technical containers* (TC), *physical containers* (PhC), *people containers* (PC) menjadi *threat scenarios* dengan mengidentifikasi *properties of threat* dari masing-masing *area of concern*. Tabel XI Merupakan contoh dari tabel *properties of threat* TC-2

Tabel XI. *Properties of Threat* – TC 2

Area of Concern	***Threat of Properties***	
Pengeksplotasian celah keamanan LMS	**Aktor**	*Hacker*
	Means	Gangguanyang terjadi karena adanya *malicious code*, *software*

oleh pihak luar atau dalam sekolah.		*deffect*, *hardware deffect*, sistem *crash*, DdoS, *Deface*.
	Motives	Secara disengaja atau tidak disengaja
	Outcome	Modifikasi, Kerusakan/ Kehilangan, Gangguan, Penyingkapan
	Security Requirments	Dari client dan server harus selalu mengupdate antivirus asli yang update dan memperhatikan kesehatan hardware.
Kemungkinan/ Probabilitas	High (Sering Terjadi) – Setiap bulan dapat terjadi karena banyaknya celah keamanan yang dapat ditembus.	

4. Fase 4 (*Identify and Mitigate Risks*)

Fase keempat memuat tiga langkah, yaitu langkah keenam, langkah ketujuh dan langkah kedelapan

1) Langkah-6 (Mengidentifikasi Risiko)

Aktivitas yang dilakukan pada langkah ini adalah bagaimana *threat scenario* dapat memberi dampak pada instansi yang dicatat dalam *Information Assets worksheet* bagian ke-7. Tabel XII merupakan contoh hasil identifikasi pada TC-2

Tabel XII. Tabel identifikasi TC-2

Skenario Ancaman	**Konsekuensi**
Pengeksplotasian celah keamanan LMS oleh pihak luar atau dalam sekolah: 1) *Malicious code* 2) *Software deffect* 3) *Hardware deffect* 4) Sistem *crash* 5) DdoS 6) *Deface*	*1)Malicious code* Hal ini dapat berdampak gangguan, modifikasi bahkan kehilangan. *2)Software Defect* Aplikasi *open source* seperti yang digunakan LMS yang tidak selalu update dapat terjadi bug dan patch yang berdampak gangguan, kerusakan dan kehilangan. *3)Hardware Defect* Hal tersebut dapat menimbulkan ketersediaan LMS yang berdampak gangguan, kerusakan dan kehilangan aplikasi dan *database*. *4)Sistem crash* Hal ini dapat mengakibatkan terhentinya layanan LMS *5)DdoS* dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan sehingga LMS tidak dapat di akses. *8)Deface* Hal ini bertujuan untuk merubah tampilan pada LMS dengan tampilan yang dimiliki oleh *defacer*.

Aktivitas selanjutnya adalah dengan penentuan *relative score* setiap *impact area*. Tabel XIII merupakan hasil perhitungan *score impact area*.

Tabel XIII. Penentuan score *impact area*

Impact Areas	Prioritas (nP)	*Impact Score*		
		Low (nL=(1))	*Medium* (nL=(2)	*High* (nL=(3))
Produktifitas	5	5	10	15
Reputasi dan Kepercayaan *user*	4	4	8	12
Finansial	3	3	6	9
Denda dan Penalti	2	2	4	6
Keamanan dan kesehatan	1	1	2	3

2) Langkah-7 (Menganalisis Risiko)

Melakukan analisis risiko pada setiap *areas of concern* serta konsekuensi yang terjadi berdasarkan *relative risk score* dengan mempertimbangkan *risk measurement criteria* yang di ciptakan pada langkah 1. Tabel XIV merupakan hasil analisis risiko *areas of concern* TC-2 yang menghasilkan *relative risk score*.

Tabel XIV. Analisis risiko *areas of concern* TC-2

Area of Concern	***Risk***			
Pengeksplotasian celah keamanan LMS oleh pihak luar atau dalam sekolah	***Consequences***	Dampak gangguan, kehilangan dan modifikasi yang disebabkan oleh pihak luar yang dapat mengeksploitasi celah keamanan LMS.		
	Saverity	***Impact Area***	***Value***	***Score***
		Reputasi dan Kepercayaan pelanggan	*High*	12
		Finansial	*Low*	9
		Produktivitas	*High*	15
		Keamanan dan Kesehatan	*Low*	1
		Denda dan Penalti	*Low*	2
		Relative Risk Score		39

3) Langkah-8 (Memilih Pendekatan Mitigasi)

Aktivitas pertama yang dilakukan pada langkah ini adalah melakukan pendekatan mitigasi dengan melakukan klasifikasi pada setiap *areas of concern* yang telah diidentifikasi berdasarkan *relative risk score*. Tabel XV merupakan *matrix* penentuan nilai risiko

Tabel XV. *Relative Risk Matrix*

Relative Risk Matrix			
	Risk Score		
Probability	**30 to 45**	**16 to 29**	**0 to 15**
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

Aktivitas selanjutnya adalah menentukan pendekatan mitigasi yang sesuai untuk setiap *areas of concern* dengan berpedoman pada tabel XVI pendekatan mitigasi berikut

Tabel XVI. Pendekatan Mitigasi

Pool	*Mitigation Approach*
Pool 1	*Mitigate*
Pool 2	*Mitigate or Defer*
Pool 3	*Defer or Accept*
Pool 4	*Accept*

Tabel XVII berikut merupakan hasil pemilihan pendekatan mitigasi untuk setiap *area of concern*

Tabel XVII. Penentuan mitigasi

No.	**Kode**	**Area of Concern**	**Relative Risk Score**	**Probabilitas**	**POOL**	**Pendekatan Mitigasi**
1.	TC-1	Berhentinya layanan LMS yang dikarenakan *supply* listrik terhenti pada server dan akibat serangan.	25	*Low*	Pool 2	*Defer*
2.	TC-2	Pengeksplotasian celah keamanan LMS oleh pihak luar atau dalam sekolah	39	*High*	Pool 1	*Mitigate*
3.	TC-3	Bocornya hak akses seperti *username* dan *password*.	29	*Low*	Pool 2	*Defer*
4.	TC-4	Ruangan server yang mudah diakses dapat mengakibatkan server dapat diakses oleh pihak yang tidak berwenang.	33	*Medium*	Pool 2	*Mitigate*
5.	TC-5	Terjadinya bencana alam yang menyebabkan kerusakan pada perangkat-perangkat	31	*Low*	Pool 2	*Mitigate*

		yang terkait dengan LMS.				
6.	PhC-1	Penyalahgunaan *Hardisk eksternal* dan file folder *back up* data guru, siswa dan admin oleh pihak yang tidak bertanggung jawab.	19	*High*	Pool 3	*Accept*
7.	PC-1	*Sosial Enginering* terhadap administrator TI yang mengakibatkan terungkapnya hak server administrator TI.	20	*Low*	Pool 3	*Defer*

Berdasarkan tabel XVII diatas, pada *area of concern* TC-2 (Pengeksplotasian celah keamanan LMS oleh pihak luar atau dalam sekolah) mitigasi yang dilakukan adalah *Mitigate* . Hal ini dikarenakan risiko tersebut menempati POOL 1 berdasarkan *relative risk matrix* dengan *relative risk score* 39. *Mitigate* dipilih karena risiko ini mungkin saja dapat terjadi setiap bulan karena banyaknya celah keamanan yang dapat di eksploitasi.

Rekomendasi Mitigasi yang dapat dilakukan anatara lain sebagai berikut:

1) Menata ulang konfigurasi desain jaringan yang rawan terhadap keamanan.
2) Mengonfigurasi, mengupgrade dan melakukan *patching* konfigurasi *default* pada perangkat jaringan.
3) Menutup port yang tidak dibutuhkan sebagai upaya mengamankan server, jika perlu dilakukan penggantian port asli.

KESIMPULAN

Dari penelitian yang dilakukan menghasilkan 7 *area of concern* dengan pendekatan mitigasi menghasilkan *mitigate* berjumlah 3, *defer* berjumlah 3, *accept* berjumlah 1. Prioritas risiko dari aspek *technical container* memiliki *relative risk score* 39 dengan strategi pengurangan risiko *mitigate*. Prioritas risiko dari aspek *physical container* memiliki *relative risk score* 19 dengan strategi pengurangan risiko *defer*. Prioritas risiko dari aspek *people container* memiliki *relative risk score* 20 dengan strategi pengurangan risiko *accept*.

DAFTAR PUSTAKA

Arum, Kalkim. 2018. *Analisis Penilaian Risiko Menggunakan Framework Octave Allegro Studi Kasus Sistem Informasi Manajemen Perpustakaan SMA Muhammadiyah 1 Ypgyakarta*. Skripsi, Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta.

Caralli, R.A., Steven, J. F., Young, L.R. Wilson, R. W. 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assesment Process.* Ditemukenali 10 Oktober 2019, dari http://www.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf.

Catherine., Aangela., Chatrine Sylfia., dan Handoko. 2019. Analisis Manajemen Risiko Sistem Pembelajaran Berbasis Elektronik pada Perguruan Tinggi XYZ. *Seminar Nasional Teknologi Informasi dan Komunikasi 2019 (SENTIKA 2019).* Pp. 9-18.

Deni, Ahmad Zakaria, R. t.D., H. 2013. "Manajemen Risiko Sitem Informasi Akademik pada Perguruan Tinggi menggunakan Metode Octave Allegro". *Seminar Nasional Aplikasi Teknologi Informasi (SNATI).* Pp. 1-7.

Dewi, Nila.NY, I Gusti Putu Hhardi Yudana. 2016. "Analisa Manajemen Risiko Pada Sitem Akedemik STIKOM BALI". *Seminar Nasional Teknologi Informasi dan Multimedia 2016.*

Djojosoedarso, S. ***2003***. *Prinsip-Prinsip Manajemen Resiko dan Asuransi, Edisi. Revisi*. Jakarta: Salemba Empat.

Kuntari, Laras.N, Yulison Herry Chrisnanto, Asep Id Hadiana. 2018. "Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro". *Seminar Nasional Teknologi Informasi Universitas Ibn Khaldun Bogor 2018.* Pp-1-8

Matondang, N., Ika Murlaili Isnainiyah, Anita Muliiawati. 2018. *Analisis Manajemen Risiko Keamanan Data Sistem Informasi.* Vol. 2 No.1 282-287.

Henderson, Allan J. 2003. *E-Learning edisi 1*. New York: Amacom. Husein, Gilang.M, Radiant Victor M. 2015. "Analisis Manajemen Resiko Teknologi Informasi Penerapan pada Document Management System di PT. Jabar Telematika (JATEL)". *Jurnal Teknik Informatika dan Sistem Informasi.* Volume 1 Nomor 2 Agustus 2015.

Indrajit, Eko R. (2012). *Aset Utama Teknologi Informasi.* E-Artikel Sistem dan Teknologi Informasi seri 999 Jakaria, DA. 2016. *Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metode Octave Allegro.* Tesis, Teknik Informatika, Universitas Islam Indonesia, Yogyakarta.

Jogiyanto. (2005). *Analisis dan Desain Informasi.* Yogyakarta: Penerbit Andi.

McLeod, Raymond Jr., dan Schell. 2004. *Sistem Informasi Manajemen (Terjemahan)*. Jakarta: Salemba Empat.

McLeod, Raymond Jr., dan Schell. 2011. *Sistem Informasi Manajemen (Terjemahan).* Jakarta: Salemba Empat.

Moekijat. 2005. *Pengantar Sistem Informasi Manajemen.* Bandung: Mandar Maju.

Materi Keamanan Sistem Informasi, Ditemukenali 13 Januari 2019, dari *Materi Keamanan Informasi*, Ditemukenali 13 Januari 2019, dari https://www.slideshare.net/audi15Ar/bab-9-keamanan-informasi-29170789

O'Brein, James A. 2005. *Pengantar Sistem Informasi(terjemahan).* Jakarta: Salemba Empat.

Rahmandani, Obby. 2017. *Analisis Penilaian Risiko pada Sistem Informasi Manajemen Penilaian Menggunakan Kerangka Kerja OCTAVE Allegro (Studi Kasus SMA Muhammadiyah 1 Yogyakarta).* Skripsi, Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta.

Rochaety, Eti. 2006. *Sistem Informasi Manajemen.* Jakarta: Bumi Aksara.

Rosini, M. R (n.d). *Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro*. Jurnal Pustakawan Indonesia Volume 14. No.1 1-9

Sarno, R dan Iffano. I. 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya: Itspress.

Uno, Hamzah.B dan Nina Lamatenggo. 2011. *Teknologi Komunikasi dan Informasi Pembelajaran*. Jakarta: PT Bumi Aksara.

Wulansari, A. 2013. *Analisa Penilaian Risiko Keamanan untuk Aset Informasi pada Usaha Kecil dan Menengah Bidang Finansial B2B: Studi Kasus Ngaturduit.com.* Skripsi, Sistem Informasi, Universitas Indonesia, Depok.

Warsita, Bambang. 2018**.** *Teknologi Pembelajaran: Landasan &Aplikasinya*. Jakarta: Rineka.

Atmaja, Surya Tri R S; Dr. Ir. Rudy Hartanto, M.T.; Dr. Ir. Eko Nugroho, M.Si. 2018. *Manajemen Risiko Keamanan Informasi Dengan Kerangka Kerja Octave Allegro*: *Studi Pemerintah Kabupaten Kulonprogo*. Tesis. Teknik Elektro, Universitas Gajah Mada, Yogyakarta.