Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik

Raihan Ramadhintia A[1], Rahadian Bisma[2]

[1,2] Program Studi Sistem Informasi, Universitas Negeri Surabaya
[1]raihanafrininda16051214020@mhs.unesa.ac.id
[2]rahadianbisma@unesa.ac.id

Abstrak*— Penggunaan teknologi informasi sangat diperlukan untuk menunjang lembaga pendidikan. SMA Semen Gresik sebagai lembaga pendidikan telah menerapkannya dengan menggunakan sebuah aplikasi ujian online khusus untuk siswa dan guru. Dalam penerapan teknologi informasi tersebut tentu akan menimbulkan sebuah risiko. Sebagai bentuk usaha meminimalisir risiko maka dibutuhkan analisis risiko dan penilaian risiko. Tujuan dari penelitian ini adalah untuk membuat rencana mitigasi dari risiko yang telah diidentifikasi dengan menggunakan metode OCTAVE Allegro. Metode OCTAVE Allegro terdiri dari 8 tahapan yang dibagi kedalam 4 fase. Pada OCTAVE Allegro ini dimulai dari membuat kriteria pengukuran risiko, analisis aset teknologi informasi, analisis risko dan mitigasi risiko. Hasil dari penelitian ini ditemukan area dampak yang paling penting adalah reputasi dan kepercayaan pelanggan dan ditemukan *area of concerns* kesalahan dalam *input* soal, listrik mati, dan penyalahgunaan file folder *back up* data siswa dan guru. Hasil *area of concerns* kesalahan dalam *input* soal termasuk kedalam pendekatan *mitigate,* listrik mati dan penyalahgunaan file folder *back up* siswa dan guru termasuk pada pendekatan *accept.

***Kata Kunci*— Analisis risiko, Mitigasi Risiko, Keamanan Informasi, Sekolah , OCTAVE Allegro.**

I. PENDAHULUAN

Teknologi informasi saat ini sangat berkembang dan banyak organisasi telah menerapkannya untuk membantu proses bisnis. Tidak hanya sebuah perusahaan tetapi instansi pendidikan juga menerapkan teknologi informasi. Dari proses belajar mengajar hingga ujian semester secara online. Penerapan teknologi informasi ini tentu dapat menimbulkan sebuah risiko.

Risiko adalah ketidaktentuan (*uncertainty*) yang mungkin melahirkan peristiwa kerugian [1]. Untuk itu diperlukan analisis risiko dan mitigasi risiko. Hasil dari analisis risiko tersebut kemudian diberi pertimbangan untuk pendekatan mitigasi yang diperlukan untuk mengurangi kemungkinan risiko.

SMA Semen Gresik merupakan instansi pendidikan yang telah menerapkan teknologi informasi namun dalam penerapannya belum pernah melakukan analisis risiko. Permasalahan yang pernah terjadi adalah gangguan pada server sehingga aplikasi yang tidak dapat digunakan. Dibutuhkan kesadaran sekolah untuk melakukan analisis risiko sebagai upaya untuk meminimalisir risiko tersebut. Analisis risiko pada penelitian ini menggunakan metode OCTAVE Allegro.

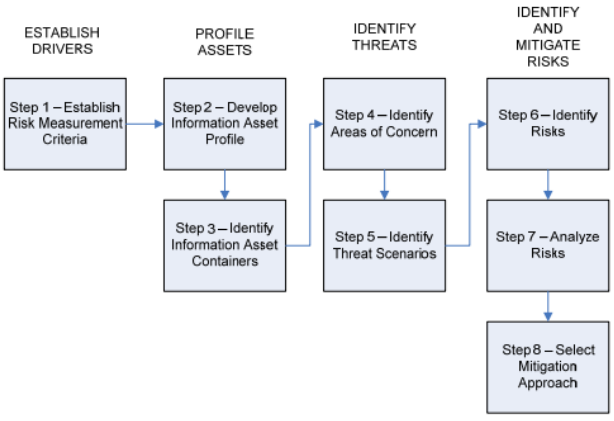
Ada beberapa metode untuk menganalisis risiko namun pada penelitian ini menggunakan metode OCTAVE Allegro. Metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) memiliki 3 varian, yaitu OCTAVE, OCTAVE-S, OCTAVE Allegro. Metode yang digunakan dalam penulisan ini adalah OCTAVE Allegro. Metode ini berfokus pada aset informasi organisasi. OCTAVE Allegro telah dilengkapi dengan *guidance*, lembar kerja hingga kuesioner[2]. OCTAVE Allegro adalah proses yang disederhanakan dengan memberikan hasil penilaian risiko yang kuat dengan investasi waktu dan sumber daya yang lebih kecil dan tidak memerlukan keamanan sistem informasi yang luas atau pengalaman manajemen risiko [3].

OCTAVE Allegro dikembangkan oleh tim *CERT® Survivable Enterprise Management* dengan tujuan utama untuk membantu organisasi memastikan bahwa kegiatan keamanan informasi mereka selaras dengan tujuan organisasi [4].

Dari permasalahan diatas dibutuhkan analisis risiko. Hasil dari penelitian ini adalah sebuah rekomendasi dari risiko yang telah diidentifikasi.

II. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode OCTAVE Allegro. OCTAVE Allegro terdiri dari 8 langkah dibagi dalam 4 fase.



Gbr. 1 OCTAVE Allegro

Keterangan gambar :

A. *Establish Risk Measurement Criteria* (Membangun Kriteria Pengukuran Risiko)

Untuk membuat kriteria pengukuran risiko terdapat 2 aktivitas, diawali dengan identifikasi kriteria pengukuran risiko dan memberikan prioritas sesuai tingkat kepentingan menggunakan *impact area ranking worksheet* [5].

B. *Develop an Information Asset Profile* (Pembutan Profil Aset)

Untuk pembuatan profil aset terdapat 8 aktivitas,aktivitas pertama identifikasi aset informasi pada organisasi kemudian melakukan penilaian risiko pada aset yang memiliki dampak buruk pada organisasi [6]. Aktivitas ketiga adalah mengumpulkan informasi tentang aset informasi kritis bagi organisasi dan membuat dokumentasi mengenai aset informasi kritis tersebut. Aktivitas lima mendeskripsikan ruang lingkup aset informasi seperti apakah nama untuk aset informasi tersebut dan mencatat kebutuhan kemanan informasi.

C. *Identify Information Asset Containers* (Mengidentifikasi Kontainer dari Aset Informasi)

Pada langkah ketiga ini mengidentifikasi keamanan dan penyimpanan aset informasi dilindungi serta ancaman terhadap kontainer dari aset informasi.

D. *Identify Areas of Concern* (Mengindentifikasi Area Masalah)

Pada langkah keempat memulai proses pengembangan profil aset informasi. Langkah keempat ini mulai membahas komponen ancaman dari risiko dengan memikirkan mengenai kemungkinan kondisi yang dapat mengancam aset informasi.

E. *Identify Threat Scenarios* (Mengidentifikasi Skenario Ancaman)

Dalam mengidentifikasi skenario ancaman terdapat 2 aktivitas, diawali dengan mengidentifikasi skenario ancaman tambahan. Aktivitas dua melengkapi lembar kerja OCTAVE Allegro untuk skenario ancaman yang umum [7].

F. *Identify Risks* (Mengidentifikasi Risiko)

Pada langkah keenam yaitu menentukan dampak dari skenario ancaman yang telah didokumentasikan pada *Information Asset Risk Worksheets*. Dari skenario yang telah dibuat akan ditemukan konsekuensi jika ancaman tersebut terjadi.

G. *Analyze Risks* (Menganalisis Risiko)

Dalam aktivitas ini akan menghasilkan skor risiko relative yang diperoleh dengan mempertimbangkan sejauh mana konsekuensi risiko mempengaruhi organisasi dibandingkan dengan kepentingan relatif dari berbagai bidang dampak.

H. Select Mitigation Approach

Pada langkah 8 mempertimbangkan risiko mana yang perlu mitigasi dan strategi mitigasi. Ini dilakukan dengan memprioritaskan risiko, memutuskan pendekatan untuk memitigasi risiko penting berdasarkan sejumlah faktor organisasi, dan mengembangkan strategi mitigasi yang mempertimbangkan nilai aset.

III. *HASIL DAN PEMBAHASAN*

Pada penelitian ini dilakukan untuk perencanaan mitigasi dengan melakukan analisa dan penilaian risiko aplikasi ujian online pada SMA Semen Gresik. Hasil dari pengumpulan data selanjutnya dilakukan penilaian risiko menggunakan metode OCTAVE Allegro yang terdiri dari delapan langkah :

A. *Establish Risk Measurement Criteria* (Membangun Kriteria Pengukuran Risiko)

Pada tahap ini dilakukan wawancara kepada guru dan operator IT untuk menetapkan kriteria pengukuran risiko. Langkah pertama adalah menentukan kriteria pengukuran risiko dan menetapkan prioritas pada area dampak. Kriteria pengukuran risiko dibuat berdasarkan *guidance* dan hasil wawancara. OCTAVE Allegro telah memberikan contoh untuk pengisian setiap lembar kerja sehingga memudahkan dalam pengerjaannya. Berikut kriteria pengukuran risiko:

TABEL I
KRITERIA PENGUKURAN RISIKO I

Reputasi dan Kepercayaan Pelanggan			
Impact Area	***Low***	***Medium***	***High***
Reputasi	Keperca-yaan guru dan siswa terhadp aplikasi ujian online sedikit sekali atau tidak terpenga-ruh.	Keperca-yaan guru dan siswa terhadap aplikasi ujian online terpenga-ruh.	Keperca-yaan guru dan siswa terhadap aplikasi ujian online sangat terpengaruh
Kehilangan *user*	Tidak ada dampak kehilangan *user* karena aplikasi ujian online hanya digunakan untuk internal sekolah		

TABEL III
KRITERIA PENGUKURAN RISIKO II

Keuangan			
Impact Area	***Low***	***Medium***	***High***
Biaya Operasional	Peningkatan biaya operasional saat implementasi aplikasi ujian online kurang dari 2.5%	Peningkatan biaya operasional saat implementasi aplikasi ujian online sebesar 2.5%-5%	Peningkatan biaya operasional saat implementasi aplikasi ujian online lebih dari 5%
Kerugian	Kurang dari 2 juta kerugian tahunan jika aplikasi ujian online terjadi gangguan	Antara 2 juta – 5 juta kerugian tahunan jika aplikasi ujian online terjadi gangguan	Lebih dari 5 juta kerugian tahunan jika aplikasi ujian online terjadi gangguan

Langkah selanjutnya adalah membuat prioritas dari area dampak yang paling penting. Nilai tertinggi akan diberikan untuk area dampak yang dianggap paling berpengaruh.

TABEL IIIII
PRIORITAS AREA DAMPAK

Area yang berdampak	**Prioritas**
Keamanan dan kesehatan	1
Keuangan	2
Produktivitas	3
Reputasi dan kepercayaan siswa	4

B. *Develop an Information Asset Profile* (Mengembangkan profil aset informasi)

Pada langkah kedua ini mendata mengenai profil aset informasi yang dimiliki organisasi dengan mendokumentasikan hasil profil aset kritis ke lembar kerja. Profil aset ini dilengkapi dengan alasan rasionalis aset kritis dan persyaratan kemanan aset tersebut. Pengisian lembar kerja profil aset sebagai berikut:

TABEL IVV
PROFIL ASET KRITIS I

Allegro Worksheet 7		**Profil Aset Kritis**
Aset Kritikal		Data Guru
Rasional Seleksi		Guru sebagai pengguna aplikasi ujian online.
Deskripsi		Aset ini berisi informasi guru seperti nama, nomer induk pegawai, mata pelajaran, jadwal ujian.
Owner		Operator IT
Security Requirements	*Confidentiality*	Hanya operator IT yang memiliki akses untuk menambahkan data guru
	Integrity	Perubahan data guru pada aplikasi ujian online yang dilakukan oleh operator IT
	Availability	Aset informasi ini harus tersedia untuk setiap guru dan operator IT
Most Important Security Requirement		Integrity Data guru harus sesuai karena jika terjadi kesalahan guru tidak dapat *input* soal ke dalam aplikasi ujian online.

Data guru dianggap aset kritis karena guru merupakan pengguna aplikasi ujian online dan data tersebut berisi informasi mengenai nama, nomer induk pegawai, mata pelajaran, dan jadwal ujian. Pada aset kritis orang yang memiliki hak akses adalah operator IT dan setelah dilakukan identifikasi persyaratan keamanan yang paling penting adalah *integrity*.

TABEL V
PROFIL ASET RISIKO II

Allegro Worksheet 7		**Profil Aset Kritis**
Aset Kritikal		Data Siswa
Rasional Seleksi		Siswa sebagai pengguna aplikasi ujian online.
Deskripsi		Aset ini berisi informasi siswa seperti nama, nomer induk siswa, kelas, tahun angkatan.
Owner		Operator IT
Security Requirements	*Confidentiality*	Hanya operator IT yang memiliki akses untuk menambahkan data siswa
	Integrity	Perubahan data siswa pada aplikasi ujian online yang dilakukan oleh operator IT
	Availability	Aset informasi ini harus tersedia untuk setiap siswa, guru, dan operator IT
Most Important Security Requirement		*Integrity* Data siswa harus sesuai jika terjadi kesalahan dapat mempengaruhi penggunaan aplikasi ujian tersebut, karena dalam data siswa mencakup kelas, mata pelajaran, dan jadwal ujian.

Data siswa dianggap aset kritis karena siswa merupakan pengguna aplikasi ujian online dan data tersebut berisi informasi mengenai nama, nomer induk siswa, kelas dan jadwal ujian. Pada aset kritis orang yang memiliki hak akses adalah operator IT dan setelah dilakukan identifikasi persyaratan keamanan yang paling penting adalah *integrity*.

C. Identify Information Asset Containers

Pada langkah ini mengidentifikasi setiap kontainer aset informasi. Kontainer biasanya diidentifikasi sebagai beberapa jenis aset teknis, objek fisik(kertas), dan orang penting bagi organisasi [8]. Setiap kontainer aset didokumentasikan pada tabel *information asset risk environment map* sebagai berikut :

TABEL VI
INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	*Owner*
Server	Sekolah
PC	Sekolah
Switch/hub	Sekolah
Database (data siswa, data guru, data soal, data nilai)	Sekolah
Sistem operasi windows 10	Sekolah
External	
Container Description	*Owner*
Jaringan Internet	Telkom

TABEL VII
INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)

Information Asset Risk Environment Map(physical)	
Internal	
Container Description	*Owner*
Folder file	Guru
External	
Container Description	*Owner*
-	-

D. *Identify Areas of Concern* (Mengindentifikasi Area Masalah)

Pada langkah keempat ini mulai membahas komponen ancaman dengan memikirkan tentang kemungkinan kondisi atau situasi yang dapat mengancam aset informasi. Berikut *areas of concern* yang telah diidentifikasi :

TABEL VIII
AREAS OF CONCERN

No	***Areas of concern***	**Aset terkait**
1	Kesalahan input data soal	Aplikasi
2	Listrik Mati	Aplikasi
3	Penyalahgunaan file folder *back up* data siswa dan guru	*File Folder*

Areas of concern merupakan pernyataan deskriptif yang menggambarkan suatu kondisi yang dapat mempengaruhi aset informasi. *Areas of concern* diidentifikasi berdasarkan pada profil aset pada langkah sebelumnya. Sebagai contoh pada situasi pertama kesalahan input data soal berpengaruh pada aset aplikasi yang termasuk pada *technical asset.*

E. *Identify Threat Scenarios* (Mengidentifikasi Skenario Ancaman)

Pada langkah kelima memperluas *areas of concern* menjadi sebuah *threat scenario*. Setiap *areas of concern* diidentifikasi kemudian didokumentasikan ke lembar kerja OCTAVE Allegro. *Information asset risk worksheets* ini berisi ancaman dan dampak yang terkait risiko dicatat, *relative risk score* dihitung dan rencana mitigasi dicatat. Pada *information asset risks worksheet* terdiri dari :

1. Aset informasi :aset yang penting bagi organisasi.
2. *Actor* :siapa pelaku dari ancaman tersebut .
3. *Means* : bagaimana cara pelaku mengakses aset tersebut (hanya berlaku untuk *human actor*)
4. *Motive* : Apa maksud dari pelaku terhadap ancaman apakah dilakukan secara sengaja atau tidak sengaja (hanya berlaku untuk *human actor)*
5. *Outcome* : hasil langsung dari pelanggaran persyaratan keamanan terhadap aset terdapat 4 pilihan (*disclosure, modification, interruption,loss)*
6. *Security requirements*: apa pelanggaran persyaratan keamanan yang dilanggar.
7. *Probability* : kemungkinan terjadinya ancaman tersebut termasuk pada kategori *low, medium* atau *high*.

Berikut lembar kerja yang berisi *threat scenario* :

TABEL IX
INFORMATION ASSET RISK WORKSHEET I

Allegro Worksheet 9	***Information Asset Risk worksheet***
Aset Informasi	Aplikasi ujian online
Areas of concern	Kesalahan dalam input soal
Actor (siapa yang melakukan *area of concern* atau ancaman?)	Guru
Means (bagaimana cara aktor melakukannya?)	Adanya kesalahan dalam *input* soal sehingga terdapat soal yang sama
Motive (Apa alasan aktor melakukannya?)	*Human Error*
Outcome (apa dampak terhadap aset informasi?)	*Disclosure*✓ *Modification Interruption Loss*
Security Requirements (*Security Requirements* apa yang dilanggar?)	Guru dapat mengakses dan memodifikasi data soal
Probability	Med - Karena kemungkinan kesalahan saat *input* soal sering terjadi

Pada *areas of concern* kesalahan *input* soal yang sama dilakukan oleh guru karenya adanya *human error*. Dampak yang ditimbulkan adalah *modification* karena terjadi perubahan pada aset informasi. Pelanggaran persyaratan keamanan termasuk dalam *integrity* karena informasi mengenai soal harus benar. Kemungkinan terjadinya ancaman ini berada pada kategori *medium.*

TABEL X
INFORMATION ASSET RISK WORKSHEET II

Allegro Worksheet 9	***Information Asset Risk worksheet***
Aset Informasi	Aplikasi
Areas of concern	Listrik mati yang menghambat jalannya aplikasi
Actor (siapa yang mel akukan *area of concern* atau ancaman?)	Pihak Luar
Means (bagaimana cara aktor melakukannya?)	Tidak adanya pasokan listrik sehingga menghambat jalannya aplikasi
Motive (Apa alasan aktor	Sengaja

Allegro Worksheet 9	***Information Asset Risk worksheet***
melakukannya?)	
Outcome (apa dampak terhadap aset informasi?)	*Disclosure Modification* ✓ *Interruption Loss*
Security Requirements (*Security Requirements* apa yang dilanggar?)	Aset ini harus tersedia
Probability	Low – kemungkinan terjadinya listrik mati jarang terjadi

Pada *areas of concern* listrik mati merupakan hal yang dilakukan oleh pihak luar. Motif dari ancaman berikut karena adanya gangguan sehingga terjadi pemadaman listrik dan dampak terhadap aset adalah *interruption* karena aplikasi menjadi tidak tersedia atau tidak dapat digunakan dan melakukan pelanggaran persyaratan keamanan *avalilability*. Kemungkinan ancaman tersebut berada pada kategori *low* karena pemadaman listrik jarang terjadi.

F. *Identify Risks* (Mengidentifikasi Risiko)

Pada langkah keenam ini adalah mengidentifikasi konsekuensi yang mungkin akan timbul ketika ancaman terjadi. Hasil dari identifikasi risiko sebagai berikut:

TABEL XI
IDENTIFY RISKS

No	***Threat Scenarios***	**Konsekuensi**
1	Kesalahan input data soal	Dibutuhkan waktu tambahan untuk mengganti soal yang sama
2	Listrik mati	Aplikasi terganggu karena tidak adanya pasokan listrik
3	Penyalahgunaan file folder *back up* data siswa dan guru.	Dapat mempengaruhi reputasi dan kepercayaan karena data mengenai siswa atau guru terungkap

G. *Analyze Risks* (Menganalisis Risiko)

Langkah ketujuh ini diawali dengan meninjau kriteria pengukuran risiko dengan mengukur dampak yang ditimbulkan dari *threats*. Sebelum melakukan penilaian perlu mengulas kembali kriteria pengukuran risiko pada langkah 1 aktivitas 1. Dalam menentukan nilai dampak nilai prioritas dikali dengan nilai *Low(1), Medium (2), dan High(3)*

TABEL XII
IMPACT SCORE

Areas of concern	***Priority***	***Impact Score***		
		***Low* (1)**	***Med* (2)**	***High* (3)**
Keamanan dan kesehatan	1	1	2	3
Keuangan	2	2	4	6
Produktivitas	3	3	6	9
Reputasi dan kepercayaan siswa	4	4	8	12

Nilai *priority* dapat ditinjau kembali dari langkah pertama dimana area dampak diberikan nilai. Nilai *impact score* didapatkan dari nilai prioritas yang dikalikan dengan nilai setiap kategori seperti kategori *low* bernilai 1, kategori *medium* bernilai 2, dan kategori *high* bernilai 3. Untuk mendapatkan nilai *impact value* diperlukan pertimbangan sejauh mana konsekuensi tersebut mempengaruhi area dampak berdasarkan kriteria pengukuran risiko pada langkah pertama kemudian nilai tersebut dijumlahkan untuk mengetahui *relative risk score* [9]. Hasil dari analisis risiko dari *areas of concern* yang telah diidentifikasi sebagai berikut:

TABEL XIII
ANALYZE RISKS I

Areas of concern	**Risiko**			
Kesalahan dalam input soal	*Consequences*	Dibutuhkan waktu tambahan untuk mengganti soal yang sama		
	Severity	*Impact Area*	*Impact Value*	*Score*
		Keamanan dan kesehatan	*Low*	1
		Keuangan	*Low*	2
		Produktivitas	*Med*	6
		Reputasi dan kepercayaan pelanggan	*Med*	8
	Relative Risk Score			17

Pada *areas of concern* kesalahan input soal setelah dilakukan analisis merupakan kejadian yang kemungkinannya besar terjadi. Setelah dilakukan pertimbangan dari konsekuensi dengan kriteria pengukuran risiko menghasilkan pada area dampak yang terpengaruh adalah produktivitas dan reputasi dan kepercayaan pelanggan pada kategori *medium* kemudian area keuangan, produktivitas, dan keamanan dan kesehatan pada kategori *low*. *Areas of concern* ini menghasilkan *Relative Risk Score* bernilai *17*.

TABEL XIV
ANALYZE RISKS II

Areas of concern	**Risiko**			
Listrik Mati	*Consequences*	Memberikan dampak gangguan atau terhentinya aplikasi ujian online		
	Severity	*Impact Area*	*Impact Value*	*Score*
		Keamanan dan kesehatan	*Low*	1
		Keuangan	*Low*	2
		Produktivitas	*Med*	6
		Reputasi dan kepercayaan pelanggan	*Med*	8
	Relative Risk Score			17

Pada *areas of concern* listrik mati dapat menyebabkan berhentinya layanan aplikasi ujian online. Hal ini dapat mempengaruhi jalannya aplikasi sehingga setelah dilakukan pertimbangan dari konsekuensi tersebut dengan kriteria pengukuran risiko pada area dampak produktivitas dan reputasi dan kepercayaan pelanggan termasuk pada kategori medium. Untuk keamanan dan kesehatan dan keuangan berada pada kategori *low*. *Areas of concern* ini menghasilkan *Relative Risk Score* bernilai 17.

TABEL XV
ANALYZE RISKS III

Areas of concern	**Risiko**			
Penyalah gunaan file folder *back up* data siswa dan guru	*Consequences*	Dapat mempengaruhi reputasi dan kepercayaan karena data mengenai siswa atau guru terungkap		
	Severity	*Impact Area*	*Impact Value*	*Score*
		Keamanan dan kesehatan	*Low*	1
		Keuangan	*Low*	2
		Produktivitas	*Low*	6
		Reputasi dan kepercayaan pelanggan	*Med*	8
	Relative Risk Score			14

Pada *areas of concern* penyalahgunaan file folder *back* up data guru dan siswa tentu memiliki konsekuensi yang mempengaruhi reputasi dan kepercayaan pelanggan dan untuk *impact area* lain berada pada kategori *low*. *Areas of concern* ini menghasilkan *Relative Risk Score* bernilai *14.*

H. Select Mitigation Approach

Pemilihan risiko yang akan dilakukan mitigasi hanya risiko yang memiliki prioritas tinggi. Dalam klasifikasi risiko digunakan *Relative Risk Matrix.*

TABEL XVI
RELATIVE RISK MATRIX

Relative Risk Matrix			
Probability	***Risk Score***		
	30 to 45	***16 to 29***	***6 to 15***
High	*Pool 1*	*Pool 2*	*Pool 2*
Medium	*Pool 2*	*Pool 2*	*Pool 3*
Low	*Pool 3*	*Pool 3*	*Pool 4*

Pada setiap *areas of concern* terdapat kategori *probability* pada langkah kelima yaitu menentukan skenario risiko. Dari nilai *probability* dan hasil *relative risk score* termasuk pada *pool* 1,2,3,4.

TABEL XVII
MITIGATION APPROACH

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

Aktivitas kedua menentukan pendekatan mitigasi setiap *areas of concern* dari kategori probabilitas dan hasil analisis risiko. Untuk pemilihan pada pendekatan mitigasi perlu didiskusikan dengan pihak organisasi [10]. Hasil dari pendekatan mitigasi setiap *areas of concern* telah diidentifikasi sebagai berikut:

TABEL XVIII
PENDEKATAN MITIGASI

No	***Areas of concern***	***Relative Risk Score***	***Probability***	***Pool***	**Pendekatan Mitigasi**
1	Kesalahan *input* data soal	17	*Med*	*Pool 2*	*Mitigate*
2	Listrik mati	17	*Low*	*Pool 3*	*Accept*
3	Penyalah-gunaan file folder *back up* data siswa dan guru.	14	*Med*	*Pool 3*	*Accept*

Untuk menentukan pendekatan mitigasi pertama melihat dari probabilitas risiko tersebut kemudian nilai *relative risk score* termasuk ke dalam *pool* berapa. Pada kesalahan *input* data soal memiliki kategori probabilitas *medium* dengan *relative risk score* 17 dari nilai tersebut termasuk ke dalam *pool* 2 yang berarti *mitigate* atau diperlukan penanganan mengenai risiko tersebut. *Areas of concern* listrik mati juga memiliki nilai yang sama yaitu 17 tetapi termasuk pada pendekatan mitigasi *accept* karena kategori probabilitas *low* dan berada pada *pool 3*.

Pendekatan *accept* berarti risiko dapat diterima oleh organisasi dan tidak dibutuhkan penanganan. Penyalahgunaan file folder *back up* data siswa dan guru memiliki nilai 14 dengan kategori probabilitas *medium* dan termasuk pada *pool* 3. Untuk *areas of concern* yang membutuhkan mitigasi telah diidentifikasi sebagai berikut:

TABEL XIX
MITIGASI I

Risk Mitigation	
Areas of Concern	Kesalahan *input* data soal
Action	*Mitigate*
Container	Kontrol
Aplikasi ujian online	Menambahkan *coding* untuk pengecekan data yang sama dengan memberikan identifikasi mengenai data yang sebelumnya telah dimasukkan pada sistem

IV. KESIMPULAN

Hasil dari penelitian ini diketahui area dampak yang paling penting adalah reputasi dan kepercayaan pelanggan, produktivitas, keuangan, dan keamanan dan kesehatan. Ditemukan aset kritis *database,server, switch* dan file folder. Terdapat 3 *areas concern* yaitu kesalahan *input* data soal, listrik mati dan penyalahgunaan file folder *back up* data siswa

dan guru. *Relative risk score* masing-masing memiliki nilai 17,17, dan 14. Terdapat 2 risiko yang masuk ke pendekatan mitigasi *accept* dan 1 risiko yang masuk ke pendekatan mitigasi *mitigate*.

Saran yang dapat diberikan untuk penelitian yaitu dapat memberikan masukan untuk SMA Semen Gresik mengenai kemungkinan adanya risiko dan upaya dalam meminimalisir terjadinya risiko pada aplikasi ujian online. Selain itu,untuk penelitian selanjutnya diharapkan dapat memperluas risiko mengenai keamanan informasi pada aset informasi yang dimiliki organisasi.

REFERENSI

[1] Joshua Jenriwan L Tobing, A. K. P., 2015. "Analisis Manajemen Resiko untuk Evaluasi Asset menggunakan Metode Octave Allegro". Expert- Jurnal Manajemen Sistem Informasi Dan Teknologi, 5(1), 1-7.

[2] Wicaksono, S.R., Rizka, C.L.D., & Immanuel, G.A.2019. *Risk Assessment* Menggunakan Pendekatan OCTAVE Allegro (Studi kasus: Schoology.com). *Information Communication & technology*, 18(2), 123-129.

[3] Keating,C.G.2014.*Validating the OCTAVE Allegro Information System Risk Assessment Methodology: A Case Study. NSUWorks*. Nova Southeastern University.

[4] Haeruddin. 2019. Pemetaan Information Asset Profile Dalam Penerapan Manajemen . *JITE (Journal of Informatics and Telecommunication Engineering)*, 3(1),67-75.

[5] Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. Introducing OCTAVE Allegro : *Improving the Information Security Risk Assessment Process. Young*.

[6] Bima Wahyu Pratama,2018. Analisis Manajemen Risiko Keamanan Sistem Informasi Kinerja Pegawai Nasional Menggunakan Metode OCTAVE Allegro(Studi Kasus: PT.PLN Sektor Pekanbaru). Skripsi, Riau: Universitas Islam Negeri Sultan Syarif Kasim Riau.

[7] Handoko., Sylvia, Chatrine., Angela., & Chaterine. 2019. Analisis Manajemen Risiko Sistem Pembelajaran Berbasis Elektronik Pada Perguruan Tinggi XYZ. Dalam: Seminar Nasional Teknologi Informasi dan Komunikasi(pp. 9-18).

[8] Anita Wulansari,2013. Analisis Penilaian Risiko Keamanan Untuk Aset Informasi pada Usaha Kecil dan Menengah Bidang Finansial B2B: Studi Kasus NGATURDUIT.com. Skripsi, Sistem Informasi, Universitas Indonesia,Depok.

[9] Hasibuan, S.I., Kusumawari T.F., & Fauzi Rokhman. 2019. Analisis Risiko Keamanan Informasi dengan Metode OCTAVE Allegro pada PT. Tirta Investama. *Proceeding of Engineering*, 6(2), 7899–7906.

[10] Matondang, N., Isnainiyah, I. N., & Muliawati, A. 2018. Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Rekayasa Sistem Dan Teknologi Informasi*, 2(1), 282–287.

UNESA
Universitas Negeri Surabaya