JUSTINDO
Jurnal Sistem dan Teknologi Informasi
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO
E-ISSN: 25541-5735, P-ISSN: 2502-5724
Volume 6, No. 2, Agustus 2021

Analisis Manajemen Risiko Aplikasi Ujian Online dengan Metode OCTAVE Allegro pada lembaga pendidikan

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

Universitas Negeri Surabaya
Email: raihanramadhintia@gmail.com

(Naskah Masuk: 1 April 2021, diterima: 31 Mei 2021, diterbitkan:31 Agustus 2021)

ABSTRAK

Penerapan teknologi informasi dalam menunjang bidang pendidikan telah diterapkan oleh SMA Semen Gresik dengan menggunakan aplikasi ujian online. Penggunaan aplikasi ujian online dilakukan pada saat ujian tengah semester dan ujian akhir semester dengan berbagai sesi sesuai jadwal ujian. Dalam penerapan teknologi informasi dapat menimbulkan sebuah risiko seperti gangguan pada jaringan *client* sehingga terputus dengan server,software terjadi *error* disebabkan oleh virus. Sebagai upaya untuk meminimalisir risiko tersebut dilakukan analisis risiko yang berkaitan dengan penggunaan aplikasi ujian online pada SMA Semen Gresik. Peneliti menggunakan metode OCTAVE Allegro dalam melakukan penilaian risiko. Metode ini terdiri dari empat fase dengan delapan tahapan dan telah dilengkapi dengan *guidance, worksheet* dan kuesioner. Dalam penelitian ini dapat diketahui area dampak yang terpenting, aset informasi kritis yang dimiliki oleh sekolah, risiko - risiko dalam penerapan aplikasi tersebut, konsekuensi jika risiko tersebut terjadi hingga pendekatan mitigasi dari setiap risiko yang telah diidentifikasi. Hasil dari penelitian ini ditemukan 7 area perhatian yang telah diidentifikasi dan diberikan pendekatan mitigasi sesuai dengan *relative risk score* menghasilkan *mitigate* berjumlah 4, *defer* berjumlah 1 dan *accept* berjumlah 2.

Kata kunci: Analisis risiko, Manajemen risiko, OCTAVE Allegro.

ABSTRACT

The application of information technology to support the education sector has been implemented by SMA Semen Gresik by using an online exam application. The use of the online exam application is carried out during midterm and final semester exams with various sessions according to the exam schedule. In the application of information technology, it can be pose a risk such as disruption to the client network so that it is disconnected from the server, software errors are caused by viruses. In an effort to minimize this risk, a risk analysis was carried out related to the use of the online exam application at SMA Semen Gresik. Researchers used the OCTAVE Allegro method in conducting risk assessments. This method consists of four phases with eight stages and equipped with guidance, worksheets and questionnaires. In this study, it can be seen that the most important impact areas, critical information assets owned by the school, the risks in implementing the application, the consequences if these risks occur and the mitigation approach of each identified risk. The results of this study found 7 areas of concern that have been identified and given a mitigation approach according to the relative risk score resulting in 4 mitigate, 1 defer and 2 accept.

Keywords: *Risk analysis, Risk management, OCTAVE Allegro.*

1. **PENDAHULUAN**

Dalam penggunaan sistem dan teknologi informasi risiko adalah hal yang harus diantisipasi. Risiko dapat timbul dari berbagai hal seperti keamanan informasi, terjadinya kebakaran, kerusakan *hardware,*dsb yang dapat mengganggu proses bisnis organisasi. Dengan kemungkinan munculnya risiko pada penggunaan sistem dan teknologi informasi dibutuhkan manajemen risiko untuk memudahkan identifikasi kemungkinan terjadinya risiko tersebut. Menurut Gibson (2011), manajemen risiko merupakan sebuah praktik mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko.

SMA Semen Gresik sebagai organisasi yang bergerak dalam bidang pendidikan. SMA Semen Gresik telah menerapkan teknologi informasi aplikasi ujian online. Aplikasi ujian online tersebut digunakan untuk pelaksanaan Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS). Dalam pelaksanaan ujian dibagi beberapa sesi waktu berdasarkan kelas. Tentu dalam penerapan teknologi informasi tersebut menimbulkan suatu permasalahan. Permasalahan yang pernah terjadi yaitu gangguan pada jaringan *client* sehingga terputus dengan *server*,*software* terjadi *error* disebabkan oleh virus yang dapat mempengaruhi penggunaan aplikasi ujian. Perbaikan dilaksanakan berdasarkan kejadian saat itu terjadi oleh operator IT belum dilakukan pengecekan secara berkala. Dari permasalahan tersebut dibutuhkan manajemen risiko untuk mengelola aset sekolah dan meminimalisir risiko dengan dilakukan penilaian risiko dengan metode OCTAVE Allegro.

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) Allegro dikembangkan oleh tim *CERT® Survivable Enterprise Management* dengan tujuan utama untuk membantu organisasi memastikan bahwa kegiatan keamanan informasi mereka selaras dengan tujuan organisasi (Caralli, Stevens, Young, & Wilson, 2007). 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 (Appari & Johnson, 2010; Caralli et al., 2007).

Penelitian yang berkaitan dengan metode ini telah dilakukan oleh peneliti sebelumnya, diantaranya penelitian yang dilakukan oleh Haeruddin (2019) dengan judul "Pemetaan Information Asset Profile dalam Penerapan Manajemen Risiko Sistem Informasi Menggunakan Metode Octave Allegro" dan hasil dari penelitian adalah dampak area prioritas yang tertinggi terdapat pada reputasi dan kepercayaan pelanggan dan memiliki 12 aset informasi dengan 8 aset informasi kritikal. Aset informasi kritis yang sangat berpengaruh pada reputasi dan kepercayaan pelanggan adalah profil mahasiswa dan ditemukan yang menyebabkan seringnya terjadi kesalahan adalah people yang kurang teliti.

Adapun penelitian lainnya dilakukan oleh Sulaimanda Isra H.,Tien F.K, Rokhman Fauzi (2019) dengan judul "Analisis Risiko Keamanan Informasi Dengan Metode Octave Allegro pada PT. Tirta Investama", hasil dari penelitian tersebut ditemukan area dampak tertinggi adalah produktivitas, reputasi dan kepercayaan karyawan,dsb. Analisis risiko yang menjadi *areas of concern* yang memiliki nilai *relative risk score* tinggi adalah perubahan data master dengan nilai 32 dan data transaksi setelah back-up data dan network failure dengan nilai 34. Dari nilai risiko tersebut perlu dilakukan mitigasi dengan memberikan rekomendasi berdasarkan ISO 27001:2013 yaitu dengan menerapkan kontrol A.9 kendali akses dan kontrol 9.1 pemantauan, pengukuran, analisis dan evaluasi.

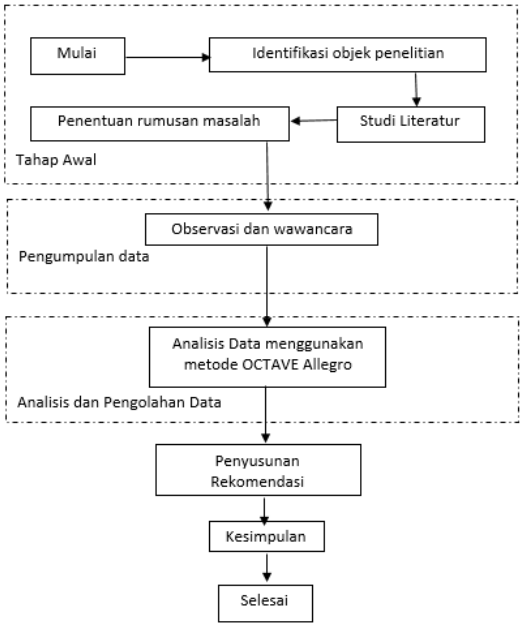
p-ISSN : 2502-5724; e-ISSN : 2541-5735

Penelitian menggunakan OCTAVE Allegro berfokus pada aset informasi misalnya infrastruktur jaringan dan perangkat keras dianggap sebagai aset kontainer, yang memfasilitasi penyimpanan dan aliran aset. Pada metode ini fokus utamanya pada estimasi dampak dan tidak mengusulkan aktivitas untuk mengatasi probabilitas selain penyebutan singkat di lembar kerja serta dalam penerapannya telah dilengkapi dengan *guidance,worksheet* dan kuesioner.

Dari permasalahan diatas dibutuhkan manajemen risiko dengan melakukan penilaian risiko menggunakan metode OCTAVE Allegro. Hasil dari penelitian ini adalah dapat memberikan suatu rekomendasi dari risiko dengan mengidentifikasi aset teknologi informasi dan analisis risiko yang muncul.

2. METODOLOGI PENELITIAN

Metode penelitian merupakan gambaraan tahapan penelitian untuk memperoleh dan mengumpulkan data yang dibutuhkan pada penelitian tersebut. Berikut merupakan metode penelitian yang digunakan.



Gambar 1 Metode Penelitian

Berdasarkan pada gambar 1, berikut penjelasan mengenai tahapan – tahapan pada metode penelitian:

1. Tahap Awal

Tahap awal merupakan tahap yang dilakukan sebelum memulai penelitian. Pada tahap awal ini terdapat tahapan sebagai berikut :

- Identifikasi Objek Penelitian

Identifikasi objek penelitian dilakukan untuk mengetahui mengenai objek penelitian yang akan digunakan dalam penelitian sehingga memudahkan peneliti dalam melaksanakan penelitian atau pengambilan data.

- Studi Literatur Sejenis

Studi literatur dilakukan untuk mencari refrensi yang berkaitan dengan objek penelitian yang diambil.

- Penentuan Rumusan Masalah

Penentuan tujuan penelitian dilakukan untuk mengetahui tujuan utama penelitian dan rumusan masalah setelah mengidentifikasi objek penelitian dan melakukan studi literatur.

2. Pengumpulan Data

Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam melakukan penelitian. Pengumpulan data dilakukan dengan observasi dan wawancara.

3. Analisis dan Pengolahan Data

Analisis data dilakukan untuk memperoleh informasi baru dari hasil pengumpulan data yang dapat memenuhi tujuan penelitian. Dalam melakukan analisis dan pengolahan data menggunakan metode OCTAVE Allegro. Pada metode OCTAVE Allegro terdiri dari 8 langkah yang dibagi menjadi 4 fase :

1) Establish Driver

Pada fase pertama memuat langkah pertama pada metode OCTAVE Allegro yaitu *Establish Risk Measurement Criteria* (Membangun Kriteria Pengukuran Risiko) yang merupakan langkah untuk membuat kriteria pengukuran risiko diawali dengan identifikasi kriteria pengukuran risiko dan

memberikan prioritas sesuai tingkat kepentingan menggunakan *impact area ranking worksheet*.

2) Profile Assets

Pada fase kedua memuat langkah kedua dan ketiga.

- *Develop an Information Asset Profile* (Pembutan Profil Aset)

Pembuatan profil untuk setiap aset informasi membentuk dasar identifikasi ancaman dan risiko pada langkah selanjutnya. Informasi profil aset penting untuk memastikan bahwa aset secara jelas dan konsisten dijelaskan, tentang batas-batas aset dan bahwa persayaratan keamanan untuk aset tersebut didefinisakan secara layak.

- *Idenitfy Information Asset Containers* (Mengidentifikasi Kontainer dari Aset Informasi)

Melakukan identifikasi setiap container aset informasi. *Container* biasanya diidentifikasi sebagai beberapa jenis aset teknis (*hardware, software, system*), tetapi *Container* juga dapat menjadi objek fisik seperti selembar kertas atau orang penting bagi organisasi.

3) Identify Threats

Pada fase ketiga memuat langkah keempat dan kelima

- *Identify Areas of Concern* (Mengindentifikasi Area Masalah)

Pada langkah keempat memulai proses pengembangan profil aset informasi. Selain itu, langkah keempat ini mulai membahas komponen ancaman dari risiko dengan memikirkan tentang kemungkinan kondisi atau situasi yang dapat mengancam aset informasi.

- *Identify Threat Scenarios* (Mengidentifikasi Skenario Ancaman)

Pada Langkah kelima diawali dengan mengidentifikasi skenario ancaman tambahan dengan menggunakan *threat scenarios questionnaries.* Aktivitas dua melengkapi *information asset risk worksheets* untuk setiap skenario ancaman yang umum.

4) *Identify and Mitigate Risks*

Pada fase keempat memuat langkah keenam, ketujuh, dan kedelapan.

- *Identify Risks* (Mengidentifikasi Risiko)

Pada langkah ini mengidentifikasi risiko dengan menentukan dampak dari skenario ancaman yang telah didokumentasikan di *Information Asset Risk Worksheets.*

- *Analyze Risks* (Menganalisis Risiko)

Dalam langkah ini akan menghasilkan skor risiko relatif. Skor risiko relatif diperoleh dengan mempertimbangkan sejauh mana konsekuensi risiko mempengaruhi organisasi.

- *Select Mitigation Approach*

Pada langkah delapan melakukan sortir pada setiap risiko berdasarkan skor risiko kemudian mempertimbangkan risiko mana yang perlu mitigasi dan strategi mitigasi.

4. Penyusunan rekomendasi

Penyusunan rekomendasi merupakan hasil dari penelitian ini. Dalam penyusunan rekomendasi ini berdasarkan penilaian risiko yang telah diidentifikasi.

5. Kesimpulan

Kesimpulan merupakan tahapan terakhir yang berisi mengenai hasil dari penelitian.

3. HASIL DAN PEMBAHASAN

Pada penelitian ini dilakukan untuk penilaian risiko aplikasi ujian online pada SMA Semen Gresik dilakukan secara langsung dan bertemu dengan operator IT dan guru untuk menjelaskan tujuan penilaian risiko aplikasi ujian online. Dalam pengumpulan data dilakukan wawancara secara rinci untuk memperoleh informasi mengenai aset informasi penting. Hasil dari pengumpulan data yang sudah mencukupi selanjutnya dilakukan penilaian risiko menggunakan metode OCTAVE Allegro yang terdiri dari delapan langkah yang dibagi menjadi 4 fase :

p-ISSN : 2502-5724; e-ISSN : 2541-5735

1. Establish Driver

Menetapkan arahan organisasi dan mengembangkan kriteria pengukuran risiko yang konsisten. Pada fase pertama ini meliputi langkah 1 *Establish Risk Measurement Criteria* (Membangun Kriteria Pengukuran Risiko). Pada langkah pertama ini terdapat 2 aktivitas yaitu menentukan kriteria pengukuran risiko dan menetapkan prioritas pada area dampak. *Risk Measurement criteria* merupakan seperangkat tindakan kualitatif terhadap dampak setiap risiko pada misi dan tujuan bisnis organisasi dievaluasi (Caralli et al.,2007).

Tahap ini dilakukan wawancara kepada operator IT dan guru untuk menetapkan kriteria pengukuran risiko. Pengisian *Allegro worksheet* 1-4 ini mengacu pada *guidance* OCTAVE Allegro yang telah memberikan contoh demonstrasi pengerjaan *Allegro worksheet* 1-4 kemudian disesuaikan dengan hasil wawancara dan kondisi pada SMA Semen Gresik. Area dampak pada metode OCTAVE Allegro diukur dengan kategori *low, medium,* dan *high*. Berikut ini merupakan kriteria pengukuran risiko:

Tabel 1 *Risk Measurement Criteria 1*

Allegro Worksheet	***RISK MEASUREMENT CRITERIA* –Reputasi dan kepercayaan Pelanggan**		
Impact Area	***Low***	***Medium***	***High***
Reputasi	1.Kepercayaan guru dan siswa terhadap aplikasi ujian online sedikit sekali atau tidak terpengaruh. 2.Dibutuhkan usaha kecil atau tidak ada usaha untuk perbaikan	1.Kepercayaan guru dan siswa terhadap aplikasi ujian online terpengaruh. 2. Dibutuhkan usaha dan waktu yang lebih untuk perbaikan	1.Kepercayaan guru dan siswa terhadap aplikasi ujian online sangat terpengaruh. 2.Dibutuhkan usaha dan waktu yang relatif lama untuk perbaikan
Kehilangan User	Tidak ada dampak kehilangan user karena aplikasi ujian online hanya digunakan untuk internal sekolah.		

Pada aktivitas kedua yaitu membuat prioritas area dampak yang terpenting akan mendapatkan nilai tertinggi dan area dampak yang tidak terlalu penting akan mendapatkan nilai yang rendah. Nilai prioritas area ini disesuaikan dengan apa yang dianggap paling penting oleh organisasi. Dari hasil wawancara dihasilkan area yang paling berdampak pada tabel sebagai berikut:

Tabel 2 *Impact Area Prioritazion*

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

2. Profile Assets

Aset yang menjadi fokus penilaian risiko diidentifikasi persyaratan kemanannya dan *asset container* diidentifikasi (Caralli et al.,2007). Pada fase ini memuat 2 langkah yaitu :

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

Aktivitas pertama yang dilakukan adalah mengidentifikasi aset informasi kritis pada organisasi yang kemudian mendokumentasikan hasil profil aset dilengkapi dengan alasan rasional mengapa aset tersebut dianggap penting dan siapa pemilik aset tersebut serta dilengkapi persayaratan keamanan dalam melindungi aset tersebut dengan mengidentifikasi kerahasiaan (*confidentality*), integritas (*integrity*), ketersediaan (*availability*) dan menentukan

persyaratan keamanan yang paling penting dari aset informasi kritis tersebut.

Tabel 3 Daftar Aset Kritis

No	Aset	Aset Kritis	Persyaratan Keamanan yang penting
1	Infor-masi	Database informasi (Data siswa, data guru, data soal, data nilai)	*Integrity*
2	Sistem	Aplikasi ujian online	*Availability*
3	*Hard-ware*	*Server,switch /hub,PC*	*Availability*

Dalam pembuatan profil aset dapat dijabarkan misalnya pada 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 ini orang yang memiliki hak akses adalah operator IT dan setelah dilakukan identifikasi persyaratan keamanan yang paling penting adalah *integrity* karena data siswa harus sesuai jika terjadi kesalahan dapat mempengaruhi penggunaan aplikasi ujian tersebut. Selain itu, pada aset server merupakan aset kritis sebagai pusat semua data yang dihasilkan dari *database* yang terdapat pada komputer user. Orang yang berwenang dalam mengakses server hanyalah operator IT. Pada persyaratan keamanan yang telah diidentifikasi pada tabel diatas ditemukan *availability* merupakan persyaratan keamanan yang penting karena server harus tersedia.

b) Identify Information Asset Containers

Pada langkah ini mengidentifikasi setiap *container* aset informasi, *container* biasanya diidentifikasi sebagai beberapa jenis aset teknis (*hardware, software, system*) tetapi *container* juga dapat menjadi objek fisik seperti selembar kertas atau orang penting bagi organisasi. *People container* merupakan orang khusus sehubungan dengan pengetahuan mengenai informasi yang rahasia atau sensitif. Berikut tabel *container* yang telah diidentifikasi:

Tabel 4 *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 5 *Information Asset Risk Environment Map (people)*

Information Asset Risk Environment Map(people)	
Internal Personnel	
Name or role	*Unit*
Operator IT	Bagian IT
Guru	Guru
External	
Name or role	*Organization*
Siswa	Siswa
Penyedia jaringan internet	Telkom

3. *Identify Threats*

Ancaman terhadap aset dalam konteks *container* diidentifikasi dan didokumentasikan (Caralli et al.,2007). Pada fase ini meliputi 2 langkah sebagai berikut:

a) *Identify Areas of Concern* (Mengindentifikasi Area Masalah)

Pada langkah keempat ini mulai membahas komponen ancaman dengan memikirkan tentang kemungkinan kondisi

p-ISSN : 2502-5724; e-ISSN : 2541-5735

atau situasi yang dapat mengancam aset informasi.

Tabel 6 *Areas of Concern*

No	*Areas of concern*	Aset terkait
1	Penyalahgunaan hak akses oleh siswa	Aplikasi
2	Gangguan jaringan internet karena salah konfigurasi	Jaringan
3	Kesalahan input data siswa	Aplikasi
4	Terjadi crash sistem karena virus	Aplikasi
5	*Server down*	Server

Areas of concern merupakan pernyataan deskriptif yang menggambarkan suatu kondisi yang dapat mempengaruhi aset informasi aplikasi ujian online. *Areas of concern* diidentifikasi berdasarkan pada *information asset risk evironment map* pada langkah sebelumnya seperti pada tabel diatas apabila terdapat suatu kondisi penyalahgunaan hak akses dapat mempengaruhi aset informasi pada aplikasi.

b) *Identify Threat Scenarios* (Mengidentifikasi Skenario Ancaman)

Pada langkah kelima memperluas *areas of concern* menjadi sebuah *threat scenario*. *Threat scenario* adalah situasi di mana aset informasi dapat dikompromikan. Biasanya terdiri dari seorang aktor, motif, sarana (akses), dan hasil yang tidak diinginkan (Caralli et al.,2007). Dalam mengidentifikasi *threat scenarios* terdapat 2 aktivitas, diawali dengan mengidentifikasi *threat scenario* tambahan dengan menggunakan *threat scenarios questionnaries* yang telah disediakan oleh metode OCTAVE Allegro. Berikut ini hasil dari *threat scenarios qustionnaries* ditemukan:

Tabel 7 *Areas of Concern 2*

No	*Areas of concern*
1	Perubahan fitur dalam pengaksesan aplikasi ujian online
2	Kebakaran

Aktivitas dua yaitu melengkapi *information asset risk worksheets* untuk setiap *threat scenarios* yang telah diidentifikasi. *Information asset risk worksheets* ini ancaman dan dampak yang terkait risiko dicatat, *relative risk score* dihitung dan rencana mitigasi dicatat (Caralli et al.,2007). Berikut ini hasil dari *information asset risk worksheet*:

Tabel 8 *Information Asset Risk Worksheet 1*

Allegro Worksheet	***Information Asset Risk worksheet***
Aset Informasi	Aplikasi ujian online
Areas of concern	Penyelahgunaan hak akses oleh siswa
***Actor* (siapa yang melakukan *area of concern* atau ancaman?)**	Siswa
***Means* (bagaimana cara aktor melakukannya?)**	Siswa dengan sengaja atau tidak sengaja menyebarkan *username dan password* yang digunakan untuk login aplikasi
***Motive* (Apa alasan aktor melakukannya?)**	Siswa dengan sengaja atau tidak sengaja
***Outcome* (apa dampak terhadap aset informasi?)**	✓*Disclosure* *Modification* *Interruption* *Loss*
***Security Requirements* (*Security Requirements* apa yang dilanggar?)**	Hanya guru, siswa, dan operator IT yang dapat mengakses aplikasi ujian sekolah
Probability	*Low* – kemungkinan penyalahgunaan hak akses rendah karena pelaksaan ujian selalu di laboratorium komputer

Pada *areas of concern* penyalahgunaan akses oleh siswa telah diketahui bahwa pelaku dari ancaman tersebut adalah siswa yang secara sengaja atau tidak sengaja menyebarkan *username* dan *password*. Dampak ancaman terhadap aset adalah *disclosure* karena melakukan tindakan pengungkapan informasi kepada pihak lain dan melakukan pelanggaran persyaratan keamanan (*confidentally*). Kemungkinan ancaman tersebut berada pada kategori *low* karena pelaksanaan ujian selalu dilakukan di sekolah dan sesuai dengan jadwal kelas masing-masing.

Tabel 9 *Information Asset Risk Worksheet 2*

Allegro Worksheet	***Information Asset Risk worksheet***
Aset Informasi	Jaringan Internet
Areas of concern	Gangguan jaringan internet karena salah konfigurasi
Actor **(siapa yang melakukan *area of concern* atau ancaman?)**	Operator IT
Means **(bagaimana cara aktor melakukannya?)**	Adanya kesalahan dalam konfigurasi jaringan
Motive **(Apa alasan aktor melakukannya?)**	Sengaja
Outcome **(apa dampak terhadap aset informasi?)**	*Disclosure* *Modification* ✓*Interruption Loss*
Security Requirements **(*Security Requirements* apa yang dilanggar?)**	Aset harus tersedia untuk guru, siswa
Probability	*High* – Karena kesalahan konfigurasi internet pernah terjadi

Pada *areas of concern* gangguan jaringan internet karena kesalahan konfigurasi yang dilakukan oleh operator IT memberikan dampak *interruption* karena layanan terjadi gangguan sehingga tidak dapat diakases. Pelanggaran persyaratan keamanan termasuk dalam *availability* dan kemungkinan terjadinya berada pada kategori *high* karena kesalahan konfigurasi pernah terjadi.

4. *Identify and mitigate risks*

Mengidentifikasi, menganalisis risiko berdasarkan ancaman dan strategi mitigasi dikembangkan untuk mengatasi risiko tersebut (Caralli et al.,2007). Pada fase ini meliputi 3 langkah yaitu:

a) *Identify risks*

Pada langkah keenam ini adalah mengidentifikasi dari *threat scenario* akan ditemukan dampak atau konsekuensi yang mungkin akan timbul ketika ancaman terjadi. Hasil dari identifikasi risiko sebagai berikut:

Tabel 10 *Identify Risks*

No	***Threat Scenarios***	**Konsekuensi**
1	Penyalahgunaan hak akses oleh siswa	Kepercayaan guru menurun terhadap siswa karena bukan siswa yang seharusnya mengerjakan ujian
2	Gangguan jaringan internet karena salah konfigurasi	Penggunaan aplikasi ujian online terganggu karena adanya gangguan jaringan
3	Kesalahan input data siswa	Dibutuhkan waktu tambahan untuk mengganti data siswa yang salah
4	Terjadi crash sistem karena virus	Memberikan dampak gangguan atau terhentinya aplikasi ujian online
5	Server down	Terhambatnya ujian karena server down
6	Perubahan fitur dalam pengaksesan aplikasi ujian online	Dibutuhkan waktu untuk melakukan *back up* data dan perubahan pada prosedur penggunaan aplikasi ujian

p-ISSN : 2502-5724; e-ISSN : 2541-5735

7	Kebakaran	Kerusakan infrastruktur sekolah karena terjadinya kebakaran

Pada langkah keenam mengidentifikasi risiko dengan ditemukannya konsekuensi jika *areas of concern* terjadi. Seperti pada tabel diatas penyalahgunaan hak akses oleh siswa tentu sangat berpengaruh pada kepercayaan guru terhadap siswa karena ujian bertujuan untuk sebuah evaluasi mengenai seberapa jauh pengetahuan siswa. Salah satu *areas of concern* kebakaran juga dapat memberikan dampak pada aset informasi hingga rusaknya infrastruktur sekolah.

b) Analyze risks

Langkah ketujuh terdapat 2 aktivitas, diawali dengan meninjau kriteria pengukuran risiko dengan mengukur dampak yang ditimbulkan dari *threats*. Sebelum melakukan penilaian perlu mengulas kembali *risk assessment criteria* yang terdapat pada langkah 1 aktivitas 1 sebagai panduan, evaluasi konsekuensi terhadap masing-masing area dampak dan catat termasuk pada kategori "*low*","*Medium*",atau "*High*". Nilai dampak diberikan nilai *Low*-1, *Medium*-2, dan *High*-3 (Caralli et al.,2007).

Tabel 11 *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
Produktivi-tas	3	3	6	9
Reputasi dan kepercaya-an siswa	4	4	8	12

Error! Not a valid embedded object.

Nilai *Priority* didapatkan dari *Impact area prioritzation* pada fase 1 langkah perrtama dimana area yang dianggap paling penting diberi nilai tertinggi kemudian untuk mendapatkan *Impact score* nilai prioritas tersebut dikalikan dengan nilai kategori masing-masing yaitu *low*-1, *medium*-2, dan *high*-3. Hasil dari analisis risiko dari *areas of concern* yang telah diidentifikasi sebagai berikut:

Tabel 12 *Analyze Risk 1*

Areas of concern	**Risiko**			
Penyalah gu-naan hak akses oleh siswa	*Se v e r i t y*	*Impact Area*	*Impact Value*	*Sco -re*
		Keamanan dan kesehatan	*Low*	1
		Keuangan	*Low*	2
		Produktivitas	*Low*	3
		Reputasi dan kepercayaan pelanggan	*Med*	8
	Relative Risk Score			14

Dalam menentukan *impact value* dan nilai perlu meninjau kriteria pengukuran risiko dan mempertimbangan sejauh mana konsekuensi tersebut mempengaruhi area dampak Pada *areas of concern* penyalahgunaan hak akses oleh siswa pada area keamanan dan kesehatan, keuangan dan produktivitas berada pada kategori *low* namun pada reputasi dan kepercayaan pelanggan berada pada kategori *medium*.

Tabel 13 *Analyze Risk 2*

Areas of concern	**Risiko**			
Gangguan jaringan internet karena salah konfigurasi	*Se v e r i t y*	*Impact Area*	*Impact Value*	*Sco -re*
		Keamanan dan kesehatan	*Low*	1
		Keuangan	*Med*	4
		Produktivi-tas	*Med*	6
		Reputasi dan kepercayaan pelanggan	*Med*	8
	Relative Risk Score			19

Pada *area of* concern gangguan internet karena salah konfigurasi setelah dilakukan pertimbangan dari konfigurasi ke area dampak memberikan dampak *low* pada keamanan dan kesehatan dan dampak *medium* pada area dampak yang lain. Berikut merupakan *relative risk score* dari setiap *areas of concern*:

Tabel 14 *Analyze Risk 3*

No	*Areas of Concern*	*Relative Risk Score*
3	Kesalahan *input* data siswa	17
4	Terjadi *crash* sistem karena virus	26
5	Server down	21
6	Perubahan fitur dalam pengaksesan aplikasi ujian online	19
7	Kebakaran	21

c) Select Mitigation Approach

Pemilihan risiko yang akan dilakukan mitigasi hanya risiko yang memiliki prioritas tinggi. Pada penelitian ini kategorisasi risiko menggunakan *Straight Forward* dengan memilah risiko dari tertinggi ke terendah. Dalam klasifikasi risiko digunakan *Relative Risk Matrix. Relative risk score* adalah nilai yang diperoleh dari pertimbangan deskripsi kualitatif probabilitas risiko dikombinasikan dengan prioritas dampak organisasi dari risiko dalam hal kriteria pengukuran risiko organisasi(Caralli et al.,2007).

Relative Risk Matrix			
Probability	Risk Score		
	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

Gambar 2 *Relative Risk Matrix*

Pada setiap *areas of concern* terdapat *probability* untuk menentukan *Relative Risk Score* termasuk pada *pool* 1,2,3,4.

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

Gambar 3 *Mitigation Approach*

Aktivitas kedua menentukan pendekatan mitigasi setiap *areas of concern* dari *relative risk score* dan probabilitasnya. Untuk pemilihan pada pendekatan mitigasi perlu didiskusikan dengan pihak organisasi. Dari setiap *areas of concern* telah diidentifikasi menghasilkan pendekatan mitigasi sebagai berikut:

Tabel 15 *Mitigation Approach*

No	*Areas of concern*	*Relative Risk Score*	*Proba-bility*	*Pool*	Pendekatan Mitigasi
1	Penyalah-gunaan hak akses oleh siswa	14	*Low*	*Pool 4*	*Accept*
2	Gangguan jaringan internet karena salah konfigurasi	19	*Med*	*Pool 2*	*Mitigate*
3	Kesalahan *input* data siswa	17	*Med*	*Pool 2*	*Mitigate*
4	Terjadi *crash* sistem karena virus	26	*High*	*Pool 2*	*Mitigate*
5	Server down	21	*Med*	*Pool 2*	*Mitigate*
6	Perubahan fitur dalam pengakses-an aplikasi ujian online	19	*Low*	*Pool 3*	*Accept*
7	Kebakaran	21	*Low*	*Pool 3*	*Defer*

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Dari tabel diatas telah dilakukan identifikasi mengenai pendekatan mitigasi sesuai dengan *relative risk matrix.* Dalam menentukan pendekatan mitigasi langkah pertama adalah melihat probabilitas setiap *areas of* concern pada *information asset risks worksheet* sebelumnya berada pada kategori *low, medium, high* dan *relative risk score* yang dihasilkan dari langkah menganalisis risiko. Hasil *relative risk score* tersebut disesuaikan dengan kategori *probability* dan disesuaikan dengan *relative risk matrix* untuk mengetahui pendekatan mitigasi yang sesuai.

Sebagai contoh pada penyalahgunaan hak akses oleh siswa memiliki kategori *probability low* dengan *relative risk score* 14 dari nilai tersebut termasuk ke dalam *pool 4* yang berarti *accept* atau risiko tersebut dapat diterima dan pada *areas of concern* kebakaran menghasilkan pendekatan mitigasi *defer* yang berarti dapat ditangguhkan kepada pihak lain (pemadam kebakaran). Untuk *areas of concern* yang membutuhkan mitigasi telah diidentifikasi sebagai berikut:

Tabel 16 Mitigasi Risiko 1

Risk Mitigation	
Areas of Concern	Gangguan Jaringan Internet
Action	*Mitigate*
Container	Kontrol
Operator IT	-Pembuatan prosedur untuk menganalisis dan memantau perangkat infrastruktur jaringan -Adanya pelatihan untuk operator IT untuk konfigurasi jaringan yang baik

Tabel 17 Mitigasi Risiko 2

Risk Mitigation	
Areas of Concern	Kesalahan *input* data siswa
Action	*Mitigate*
Container	Kontrol
Database Data Siswa	Dibuat validasi *input* data pada *field* tertentu
Guru	Melakukan verifikasi data siswa yang telah diisi oleh operator IT

Tabel 18 Mitigasi Risiko 3

Risk Mitigation	
Areas of Concern	Terjadi *Crash* sistem karena virus
Action	*Mitigate*
Container	Kontrol
Operator IT	Menata ulang konfigurasi jaringan yang rawan terhadap keamanan
Server	Adanya antivirus pada *hardware* dan dilakukan update antivirus setiap 3 bulan

Tabel 19 Mitigasi Risiko 4

Risk Mitigation	
Areas of Concern	*Server Down*
Action	*Mitigate*
Container	Kontrol
Operator IT	Melakukan konfigurasi pembatasan akses pada server

4. KESIMPULAN

Dari penelitian yang dilakukan ditemukan *impact area* yang paling berpengaruh adalah reputasi dan kepercayaan pelanggan,produktivitas, keuangan, dan keamanan dan kesehatan. Selain itu, ditemukan aset IT berupa *physical* yaitu PC, Server, Switch/Hub dan aset IT berupa *people* yaitu operator IT dan guru sebagai pihak internal dan siswa berserta penyedia jaringan internet sebagai pihak eksternal.

Dari analisis aset IT organisasi tersebut ditemukan 7 *areas of concern* seperti gangguan internet karena kesalahan konfigurasi, kesalahan *input* data siswa, kebakaran,dsb. Setiap *areas of concerns* yang telah diidentifikasi memiliki *relative risk score* masing – masing dan hasil tertinggi bernilai 26 dan 21 yaitu pada *areas of concern* terjadi *crash* system karena virus dan server down, hasil terendah bernilai 14 yaitu penyalahgunaan hak akses oleh siswa. Langkah selanjutnya yaitu menentukan pendekatan mitigasi dari setiap *areas of concern* dengan mendiskusikan dengan pihak organisasi.

Hasil dari diskusi tersebut menghasilkan pendekatan mitigasi dari 7 *Areas of Concern* ditemukan 4 *areas of concern* dengan pendekatan mitigasi berupa *mitigate,* 1 *area of concern* dengan pendekatan mitigasi berupa *defer,* dan 2 *areas of concern* dengan pendekatan mitigasi berupa *accept*. Untuk pendekatan mitigasi *mitigate* perlu diberikan sebuah rekomendasi seperti pada gangguan jaringan internet karena salah konfigurasi dapat dilakukan upaya pembuatan prosedur untuk menganalisis dan memantau infrastruktur jaringan dan memberikan pelatihan untuk operator IT mengenai jaringan.

Saran untuk penelitian selanjutnya dapat melakukan penilaian risiko secara detail pada semua aset informasi perusahaan atau organisasi dan diharapkan menerapkan metode baru dalam penilaian risiko untuk membandingkan efektivitas setiap metode.

DAFTAR PUSTAKA

Aprilia, Via.P., Rachmadi, Aditya., & Perdanakusuma Andi,R.2019. Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*,3(3)*,2829-2836*

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

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

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

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)

Supristiowadi, Eko., G.S,Yudho.2018. Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementrian Keuangan. *Indonesia Treasury Review,*3(1),23-33.

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.

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

Wangen, Gaute., Hallstensen, Christoffer., & Snekkenes, Einar.2018. *A framework for estimating information security risk assessment method completeness*. Norway : Springer.

Yuca Akbar Maulana,2017. “Perencanaan mitigasi risiko pada layanan koordinasi tele-presence menggunakan metode OCTAVE-S di Pemerintah Kabupaten Malang”. Skripsi. Sistem Informasi, Universitas Negeri Jember,Jember.