ANALISIS RISIKO *WEBSITE* UJIAN *ONLINE* DENGAN METODE OCTAVE ALLEGRO PADA PT.XYZ

Muhamad Aufadhiya Elhaq[1], Sri Lestari[2]

[1,2]Institut Informatika dan Bisnis Darmajaya

aufadhiya.2121211008@mail.darmajaya.ac.id[1], srilestari@darmajaya.ac.id[2]

ABSTRACT

PT. XYZ is an integrated ISP and digital infrastructure company in Indonesia. The company focuses on service quality, PT. XYZ requires human resources who have skills and are able to provide good service to customers. Therefore PT. XYZ always conducts training and certification every year for almost all of its employees. In addition to maintaining and improving the quality of existing human resources, the results of this training and certification are also a major consideration for companies whether to continue the employee's employment contract or not. in the era of Covid 19 PT. XYZ implements an Online system for training and certification, then tests are carried out using Online exam Website media and using 3rd party supporting software, namely the Safe Exam Browser, so there is no cheating, the trainer team monitors via CCTV or via the cellphone camera of the examinees who are members of the Online group meeting. An examination of the hazards is done in an effort to reduce them. Risk analyses were performed using the OCTAVE-Allegro approach by the researchers. With instructions, worksheets, and questionnaires included, this system contains four phases and eight stages. The vital information assets controlled by PT. XYZ are the most significant area of influence that can be determined by this analysis. The study's findings revealed five areas of concern, which were then assigned a mitigation strategy in accordance with the relative risk score, yielding a 3 mitigate, 1 defer, and 1 accept.

Keywords—Online Exam, Risk Management, Risk Mitigation, OCTAVE-Allegro.

ABSTRAK

PT. XYZ merupakan salah satu ISP terintegrasi dan perusahaan infrastruktur digital di Indonesia. Perusahaan berfokus pada kualitas layanan, PT. XYZ mengutamakan sumber daya manusia yang mempunyai keterampilan dan mampu memberikan pelayanan dengan baik kepada pelanggan. Oleh karena itu PT. XYZ selalu mengadakan pelatihan dan sertifikasi setiap tahunnya kepada hampir seluruh karyawannya. Selain untuk menjaga dan meningkatkan kualitas SDM yang ada, hasil pelatihan dan sertifikasi ini juga menjadi pertimbangan besar bagi perusahaan untuk melanjutkan kontrak kerja karyawan tersebut atau tidak. Di era Covid 19 PT. XYZ menerapkan sistem Online untuk pelatihan dan sertifikasi, kemudian dilakukan ujian dengan menggunakan media Website ujian Online dan menggunakan software pendukung pihak ke-3 yaitu Safe Exam Browser. Ditambah lagi agar tidak ada kecurangan, divisi trainer memantau melalui CCTV atau melalui kamera ponsel peserta ujian yang tergabung dalam pertemuan kelompok daring. Sebagai upaya untuk meminimalkan risiko kecurangan, dilakukan analisis risiko. Penelitian ini

menggunakan metode OCTAVE-Allegro sebagai panduan dalam menilai risiko. Metode ini terdiri dari 4 fase dengan 8 langkah serta dilengkapi dengan lembar kerja, petunjuk dan kuisioner. Dalam penelitian ini terlihat bahwa area yang paling penting adalah aset informasi krusial yang dimiliki oleh PT. XYZ. Hasil penelitian ini mengidentifikasi 5 masalah yang diidentifikasi kemudian diterapkan pendekatan mitigasi sesuai dengan skor relative risk diperoleh hasil mitigate 3, defer 1 dan accept 1.

Kata Kunci—*Ujian Online, Manajemen Risiko, Mitigasi Risiko, OCTAVE-Allegro.*

I. PENDAHULUAN

PT.XYZ merupakan salah satu perusahaan penyedia layanan internet dan infrastruktur digital yang terintegrasi di Indonesia. Perusahaan ini berfokus pada layanan yang berkualitas sehingga *concern* saat ini adalah menjaga seluruh sektor layanan kepada pelanggan agar berlangsung dengan baik, maka dari itu PT. XYZ membutuhkan sumber daya manusia yang mempunyai kemampuan yang baik dalam hal *skill* sesuai *jobdesc* pekerjaan dan mampu menyampaikan layanan dengan baik kepada pelanggan. Oleh karena itu PT. XYZ selalu melakukan *training* dan sertifikasi setiap tahunnya kepada hampir seluruh karyawannya. Selain untuk menjaga dan meningkatkan kualitas SDM yang ada, hasil dari *training* dan sertifikasi ini juga menjadi pertimbangan besar bagi perusahaan untuk melanjutkan kontrak kerja terhadap karyawan tersebut atau tidak.

Pandemi covid 19 membuat proses bisnis di masa pandemi telah berubah dan salah satunya adalah adanya *social distancing* dan PSBB yang memaksa organisasi untuk melakukan perubahan pada cara kerja untuk mendukung protokol Kesehatan [1], sebelum pandemi *Covid* 19 *training* dan sertifikasi ini dilakukan dengan cara luring dan ujiannya dilaksanakan secara tertulis, namun pada saat pandemi, PT.XYZ dan Divisi Trainernya memberlakukan sistem daring untuk *training* dan sertifikasi kemudian ujiannya dilakukan dengan media *Website* ujian *Online* dan menggunakan *software 3rd party* pendukung yaitu Safe Exam Browser. Ditambah pada saat ujian dilakukan agar tidak terjadi kecurangan divisi *trainer* melakukan pantauan melalui *cctv* atau melalui kamera *handphone* peserta yang tergabung dalam *group meeting Online.*

Dalam pelaksanaan ujian dan *training* ini pernah timbul permasalahan, terjadi kebocoran *key exam* / tertukar yang menyebabkan proses ujian tidak berlangsung sebagai mana mestinya, *Website* ujian dapat diakses melalui

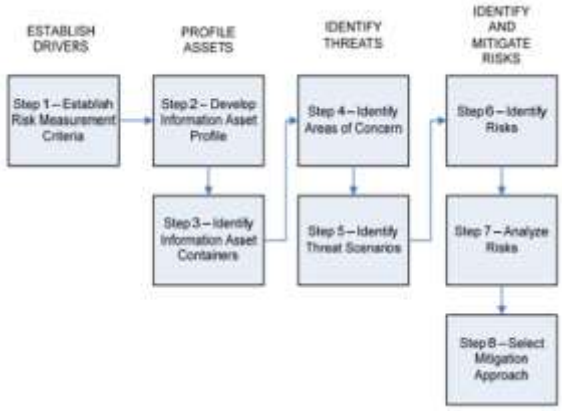
browser biasa tanpa melalui *software 3rd party* Safe Exam Browser, dan yang paling sering terjadi, yaitu gangguan pada jaringan klien sehingga menyebabkan terputusnya koneksi dari *server*. Manajemen risiko diperlukan untuk masalah tersebut untuk mengelola aset dan memitigasi risiko dengan melakukan penilaian risiko menggunakan metode OCTAVE Allegro, menggunakan metode ini diharapkan dapat memberikan hasil berupa perangkingan risiko yang lebih cepat, akurat, dan dapat diaplikasikan sesuai dengan kondisi [2].

Peneliti sebelumnya telah melakukan penelitian terkait metode ini, diantaranya Raihan Ramadhintia A (2021), hasil penelitian mengidentifikasi area pengaruh utama, kumpulan data krusial yang dimiliki oleh organisasi, risiko dalam penerapan *system*, konsekuensi dari manifestasi risiko untuk memitigasi masing-masing risiko. Hasil dari penelitian mengidentifikasi 7 masalah yang diidentifikasi dan diterapkan pendekatan mitigasi menurut penilaian risiko relatif, menghasilkan 4 mitigasi, 1 penundaan dan 2 penerimaan [3]. B. Naibaho mengemukakan pada penelitiannya ditemukan 8 *areas of concern* yang 6 diantaranya dapat menimbukan kerugian yang besar, maka dari itu hasil analisis yang OCTAVE Allegro tidak hanya membantu mengidentifikasi dan memitigasi resiko yang ada, namun juga dapat di jadikan acuan sebagai referensi untuk mengembangkan profil resiko perusahaan [4]. Hasil analisis OCTAVE Allegro juga dapat di gabungkan dengan standar *ISO* untuk memberikan rekomendasi untuk perbaikan atau manajemen risiko, seperti pada penelitian D. Irawan yang menggunakan standard ISO 27001 untuk memberikan 8 rekomendasi penanganan risiko yang telah di identifikasi [5].

II. METODE PENELITIAN

Penelitian dilakukan di PT.XYZ wilayah regional Sumbagsel pada bulan November 2022. Pengumpulan data dilakukan melalui wawancara dan observasi. Wawancara dilakukan terhadap *user* yang sudah pernah melakukan *training* dan ujian, divisi Trainer, dan admin IT yang bertugas langsung dengan mengembangkan, melakukan *maintenance* dan menjaga operasional sistem informasi. Observasi dilakukan dengan mengamati tindakan pengguna terkait penggunaan sistem informasi dalam prosesnya. Langkah pengamatan ini juga merupakan sarana untuk mengumpulkan dokumen otorisasi sistem informasi, kebijakan, dan prosedur kerja yang menunjukkan kondisi dan komponen yang terkait risiko sistem

informasi yang dikembangkan. Informasi yang dihasilkan berupa informasi yang berkualitas menciptakan pendekatan PT XYZ dalam memitigasi risiko sistem informasi. Selain itu, data yang diperoleh diolah dengan menggunakan metode OCTAVE Allegro. Metode ini terdiri dari delapan langkah yang dibagi menjadi empat langkah dan dalam 4 fase tersebut ada 8 langkah [6] yang ditunjukkan pada gambar 1.



Gambar 1. Tahapan Metode OCTAVE-Allegro

III. HASIL DAN PEMBAHASAN

3. 1. Menetapkan Driver

Pada fase pertama ini meliputi langkah pertama yaitu Menetapkan *Risk Measurement Criteria*. Langkah ini dilakukan 2 aktivitas yaitu menetapkan *Risk Measurment Criteria* dan menetapkan *Impact Area Priority*. *Risk Measurement criteria* adalah seperangkat ukuran kualitatif yang digunakan untuk menilai dampak setiap risiko terhadap misi organisasi dan tujuan bisnis [4].

Tahap ini dilakukan wawancara kepada Divisi Trainer dan admin *Website*(Divisi IT Ops) untuk menentukan kriteria pengukuran risiko. *Worksheet* 1-4 dari OCTAVE-Allegro diisi mengacu pada *guideance* yang ada, kemudian disesuaikan dengan hasil wawancara dan kondisi pada PT. XYZ. Area yang terkena dampak pada metode OCTAVE Allegro dikelompokkan dengan tingkatan kategori *low*, *medium*, dan *high*. Tabel 1, tabel 2 berikut ini merupakan hasil pengukuran kriteria risiko yang diperoleh:

Tabel 1. Risk Measurement Criteria - Reputation

Allegro Worksheet 1	***RISK MEASUREMENT CRITERIA - Reputation***		
Impact Areas	***Low***	***Medium***	***High***
Reputasi Divisi Trainer dan Perusahaan	Kepercayaan Divisi Trainer dan Perusahaan terhadap *Website* Ujian *Online* Sedikit Sekali atau tidak terpengaruh, Dibutuhkan usaha kecil atau tidak ada usaha untuk perbaikan	Kepercayaan Divisi Trainer dan Perusahaan terhadap *Website* Ujian *Online* Terpengaruh, Dibutuhkan usaha dan waktu yang lebih Panjang untuk memperbaiki	Kepercayaan Divisi Trainer dan Perusahaan terhadap *Website* Ujian *Online* sangat terpengaruh Dibutuhkan usaha dan waktu yang lebih Panjang untuk memperbaiki
Kerugian Peserta Training	Kerugian yang di rasakan *user* namun tidak berdampak atas ujian	Kerugian *user* proses ujian membutuhkan waktu yang lebih lama.	Kerugian *user* harus mengulangi proses ujian

Tabel 2. Risk Measurement Criteria - Productivity

Allegro Worksheet 3	***RISK MEASUREMENT CRITERIA – Productivity***		
Impact Areas	***Low***	***Medium***	***High***
Jam Kerja	Jam kerja staf meningkat kurang dari 10%	Jam Kerja meningkat antara 20% dan 40% dalam lebih dari 2 hari sampai 4 hari	Jam kerja staf meningkat lebih dari 50% dalam lebih dari 4 hari

Dan didapatkan hasil pada tabel 3 prioritas impact area yaitu merupakan area yang terkena dampak dan diurutkan berdasarkan prioritas yang ditentukan oleh *management* perusahaan PT. XYZ.

Tabel 3. Impact Area Priority

Impact Area	*Priority*
Safety and Health	1
Finance	2
Productivity	3
Trust and Reputation	4

3.2. Profile Assets

Di fase ini berfokus pada identifikasi aset yang akan dinilai risikonya serta ditentukan kebutuhan keamanannya [4] Pada fase ini memuat 2 langkah yaitu

3. 2. 1. Menguraikan profil asset informasi

Langkah pertama yaitu mengenali aset informasi penting dalam organisasi, kemudian didokumentasikan hasil profil aset dan alasan pentingnya *asset* tersebut kemudian siapa yang memiliki aset tersebut serta memiliki persyaratan keamanannya untuk melindungi aset tersebut. Dengan mengidentifikasi kerahasiaan, integritas, dan ketersediaan serta menetapkan syarat keamanan utama dari aset informasi penting ini. Hasil identifikasi terdapat pada tabel 4.

Tabel 4. Daftar Aset Penting

Allegro Worksheet 8	***CRITICAL INFORMATION ASSET PROFILE***	
Aset	***Aset Kriitis***	***Persyaratan Kemanan Yang Penting***
Informasi Karyawan	Data Karyawan	*Integrity*
Informasi Soal dan Jawaban	Data Soal dan Jawaban	*Integrity*
Sistem	*Website* Ujian *Website*	*Availibility*
Hardware	*Server-Router, dll*	*Availibility*

Dalam profil aset dapat diambil contoh pada data Karyawan, data ini merupakan aset krusial karena karyawan merupakan pengguna utama dalam *Website* ujian *Website*, data tersebut berisi informasi mengenai NIK, nama, *Email, password* akun, dan lain lain. Pada aset ini hanya admin IT dan Divisi Trainer yang memiliki hak akses untuk modifikasi data, Setelah mengidentifikasi persyaratan keamanan utama, ada integritas karena data karyawan harus cocok, jika terjadi kegagalan, dapat memengaruhi proses ujian. Selain itu, sumber daya *server* adalah aset penting sebagai pusat dari semua informasi yang berisi *database*. Orang yang berwenang dalam mengakses *server* hanyalah admin IT. Diketahui bahwa persyaratan keamanan telah

disampaikan pada tabel 4, ketersediaan telah diidentifikasi sebagai contoh persyaratan yang penting server harus selalu bisa diakses pada saat ujian dilaksanakan.

3. 2. 2. Identifikasi Container Aset Informasi

Di tahap ini identifikasi dilakukan pada container aset informasi sesuai dengan lembar kerja OCTAVE-Allegro, Tabel 5 dan 6 menunjukkan container *Technical* dan *People*.

Tabel 5. Information Asset Risk Environment Map (Technical)

Allegro Worksheet 9a	***INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)***
INTERNAL	
Container Description	*Owner*
Server	PT. XYZ
PC	PT. XYZ
Database(Data Karyawan, data soal)	PT. XYZ
EXTERNAL	
Container Description	*Owner*
Laptop Pribadi	Peserta *Training*

Tabel 6. Informastion Asset Risk Environment Map (People)

Allegro Worksheet 9c	***INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)***
INTERNAL	
Container Description	*Owner*
Operator *Website*	*IT Operation*
Trainer	*Team Trainer*
Peserta Ujian	Karyawan
EXTERNAL	
Container Description	*Owner*
Peserta Ujian	Calon Karyawan

3. 3. Identify Threats

Dalam *container* yang telah dibentuk pada tabel 5 dan 6 dilakukan identifikasi dan dokumentasi ancaman terhadap asset tersebut [3]. Di fase ini 2 langkah yang dikerjakan yaitu:

3. 3.1. Identify Areas of Concern

Pada langkah ini membahas bagian dari ancaman dengan memperhatikan adanya kemungkinan situasi atau kondisi yang dapat membahayakan aset informasi [7].

Tabel 7. Areas of Concern

No	***Areas Of Concern***	***Asset***
1	Penyalahgunaan hak akses oleh peserta *training*	Aplikasi
2	Penyalahgunaan *key exam*	Informasi
3	Gangguan Jaringan internet	Jaringan
4	Kesalahan input data ujian	Aplikasi
5	*Server Down*	*Server*

Tabel 7 berisi *Areas of concern* yaitu deskripsi dari pernyataan yang menggambarkan skenario atau kondisi yang dapat mempengaruhi isi informasi *Website* ini. Area yang menjadi *concern* diidentifikasi berdasarkan peta lingkungan risiko sumber daya data dari langkah sebelumnya sesuai tabel 4 jika ada situasi di mana penyalahgunaan hak akses dapat memengaruhi sumber daya data aplikasi.

3.3.2 Identify Threat Scenarios

Langkah ini memperluas *Areas of Concern* menjadi skenario yang

mengancam. Skenario ancaman adalah situasi di mana sumber daya informasi dapat dikompromikan. Mengidentifikasi skenario ancaman memiliki dua fungsi, dimulai dengan mengidentifikasi lebih banyak skenario ancaman menggunakan kuesioner skenario ancaman yang disediakan dengan metode OCTAVE-Allegro [8]. Berikut adalah hasil observasi skenario ancaman, yang hasilnya kemudian digunakan untuk mengisi setiap skenario ancaman yang teridentifikasi. Tabel risiko aset informasi yang terkait dengan ancaman dan dampak yang terkait dengan risiko tersebut dicatat, *relative risk score* dihitung, dan rencana mitigasi dicatat [4]. Tabel 8 dan 9 adalah *information asset risk worksheet* yang didapat:

Tabel 8. ***Information Asset Risk Worksheet 10***

Allegro Worksheet 10	*INFORMATION ASSET RISK WORKSHEET*
Information Asset	*Website* ujian *Website*
Areas of Concern	Penyalahgunaan hak akses oleh peserta ujian
Actor	Peserta ujian
Means / How?	Peserta dengan sengaja atau tidak sengaja menyebarkan nama pengguna dan kata sandi yang digunakan untuk *login Website* untuk tujuan tertentu
Motive?	Peserta dengan sengaja atau tidak sengaja
Outcome ? Security	Pengungkapan Modifikasi Gangguan
Security Requirements	Hanya divisi trainer, peserta yang terjadwal yang dapat mengakses *Website* ujian dan harus dipantau dengan baik melalui camera CCTV.
Probability	Medium – kemungkinan penyalahgunaan hak akses menengah karena walaupun pelaksaan Ujian dipantau *cctv*, namun peserta yang tidak terpantau *cctv* hanya menggunakan kamera HP Peserta yang bergabung ke *meeting Website* sebagai alat pantau.

Tabel 8 menjelaskan tempat di mana hak akses disalahgunakan, pelaku ancaman ini dikenal sebagai peserta ujian yang secara sengaja atau tidak sengaja membagikan nama pengguna serta kata sandi. Pengaruh ancaman aset bersifat *disclosure* karena pengungkapan informasi ini merupakan pelanggaran persyaratan keamanan (*confidentally*). Kemungkinan terjadi ancaman ini ialah Medium karena pelaksanaan ujian dipantau *cctv*, namun peserta yang tidak terpantau cctv hanya menggunakan kamera HP Peserta yang bergabung ke *meeting Website* sebagai alat pantau.

Tabel 9. ***Information Asset Risk Worksheet 2***

Allegro Worksheet 10	*INFORMATION ASSET RISK WORKSHEET*
Information Asset	Data Soal
Areas of Concern	Penyalahgunaan *key exam*
Actor	Peserta Ujian
Means / How?	Peserta menyebarkan *key exam* / menyalahgunakan.
Motive	Peserta dengan Sengaja menyebarkan, dengan alasan untuk menginformasikan soal yang sudah dikerjakan kepada peserta lain.
Outcome? Security	Pengungkapan Modifikasi
Security Requirements	Hanya divisi trainer, peserta yang terjadwal yang mengetahui *key exam*, dan *key exam* otomatis berubah setelah selesai ujian.
Probability	Medium – kemungkinan

	penyalahgunaan *key exam* Medium karena pelaksanan Ujian karena *key exam* tidak otomatis diganti saat ujian berakhir.

Pada *areas of concern* penyalahgunaan *key exam*, karena *key exam* tidak dinamis dan otomatis berubah dapat memberikan dampak *disclosure* karena proses ujian tidak lagi adil dan jujur. Pelanggaran persyaratan keamanan termasuk dalam ketersediaan dan kemungkinan terjadinya sedang karena kebocoran masalah telah terjadi.

4.1. Identify and Mitigate Risks

4.1.1 Identify Risks

Pada langkah keenam ini, identifikasi risiko dengan mencari konsekuensi ketika kekhawatiran muncul, seperti yang ditunjukkan pada Tabel 10.

Tabel 10. Identify Risk

No	***Threat Scenarios***	***Konsekuensi***
1	Penyalahgunaan hak akses oleh peserta *training*	Kepercayaan divisi trainer kepada peserta *training* menurun, karena terjadi kecurangan
2	Penyalahgunaan *key exam*	Terjadi kebocoran data soal
3	Gangguan Jaringan internet	Penggunaan *Website* ujian terganggu karena gangguan jaringan
4	Kesalahan input data ujian	Dibutuhkan waktu tambahan untuk memverifikasi dan mengubah data ujian peserta yang salah
5	*Server Down*	Pelaksanaan ujian terhambat karena *server down*

4.1.2 Analyze Risk

Ada dua kegiatan dalam langkah ini, yang pertama adalah melihat kriteria pengukuran risiko dengan mengukur efek yang ditimbulkan oleh ancaman. Di sini peneliti menggunakan kriteria penilaian risiko pada fase 1 langkah pertama sebagai panduan. Selanjutnya ditambahkan *impact score* yang hasilnya dapat dilihat pada Tabel 11.

Tabel 11. Impact Score

Areas Of Concern	*Priority*	*Impact Score*		
		Low (1)	*Med (2)*	*High (3)*
Safety and Health	1	1	2	3
Finance	2	2	4	6
Productivity	3	3	6	9
Trust and Reputation	4	4	8	12

Nilai prioritas dihasilkan dari prioritas area pengaruh pada langkah 1 fase pertama, dimana area yang dianggap paling penting mendapat nilai tertinggi. Untuk mendapatkan skor dampak, nilai prioritas dikalikan dengan nilai masing-masing kategori yaitu rendah-1, sedang-2 dan tinggi-3 [9]. Pada tabel 12, 13 dan 14 berikut adalah Hasil analisis risiko dari masing masing a*reas of concern*.

Tabel 12. Analyze Risk 1

Areas Of Concern	**Resiko**		
Penyalahgunaan hak askes oleh peserta	*Impact Area*	*Impact Value*	*Score*
	Safety and Health	*Low*	1
	Finance	*Low*	2
	Productivity	*Low*	3
	Trust and Reputation	*Med*	8
	Relative Risk Score		14

Saat menetapkan *impact value*, penting untuk mengamati kriteria pengukuran risiko dahulu dan mempertimbangkan bagaimana konsekuensi ini terkait dengan domain dampak [10].

Tabel 13. Analyze Risk 2

Areas Of Concern	Resiko		
Penyalahgunaan *key exam*	*Impact Area*	*Impact Value*	*Score*
	Safety and Health	*Low*	1
	Finance	*Low*	2
	Productivity	*Med*	6
	Trust and Reputation	*Med*	8
	Relative Risk Score		17

Dan berikut adalah *relative risk score* dari setiap *areas of concern* lainnya:

Tabel 14. Analyze Risk 3

No	***Areas of concern***	***Relative Risk Score***
3	Gangguan Jaringan internet	21
4	Kesalahan input data ujian	17
5	*Server Down*	26

4. 1.3 Select Mitigation Approach

Pada Langkah ini hanya risiko dengan prioritas tinggi yang dipilih untuk mitigasi. Dalam penelitian ini, metode klasifikasi risiko sederhana digunakan dengan mengurutkan risiko dari yang tertinggi ke terendah hingga terendah [11]. *Relative Risk Matrix* digunakan untuk mengklasifikasi risiko. *Relative risk score* merupakan nilai yang diperoleh dengan mempertimbangkan deskripsi kualitatif probabilitas risiko yang dikombinasikan dengan peringkat efek risiko organisasi dalam kaitannya dengan kriteria pengukuran risiko organisasi. Setiap area yang terkena dampak memiliki probabilitas untuk menetapkan skor risiko relatif, termasuk dalam *pool-pool 1(Mitigate), 2(Mitigate or Defer), 3(Defer or Accept), 4(Accept).*

Tabel 15 adalah areas of concern dari penyalahgunaan hak akses dan menghasilkan pendekatan mitigasi sebagai berikut:

Tabel 15. Mitigation Approach

No	*Areas Of Concern*	*Relative Risk Score*	*Probability*	*Pool*	*Mitigation Approach*
1	Penyalahgunaan hak akses oleh	14	*Low*	4	*Accept*

	peserta *training*				
2	Penyalahgunaan *key exam*	17	*Med*	2	*Mitigate*
3	Gangguan Jaringan internet	21	*Med*	2	*Mitigate*
4	Kesalahan input data ujian	17	*Med*	2	*Mitigate*
5	*Server Down*	26	*Low*	3	*Defer*

Dari tabel 15 telah teridentifikasi metode mitigasi menurut matriks *relative risk*. Saat menentukan metode mitigasi, pertama-tama perlu dipertimbangkan kemungkinan bahwa setiap *areas of concern* di Lembar Kerja *information asset risk* sebelumnya akan menghasilkan kategori Risiko Rendah, Sedang, atau Tinggi, dan relative *risk score* pada langkah analisis risiko. Hasil skor r*elative risk* disesuaikan dengan kelas probabilitas dan matriks *relative risk* untuk menentukan pendekatan mitigasi yang tepat [12].

Misalnya, penyalahgunaan hak akses pelanggan memiliki kategori probabilitas rendah dengan nilai risiko relatif 14, di mana nilai tersebut masuk ke dalam kategori *pool* 4, artinya risiko *defer* atau risiko tersebut dapat diterima. Berikut pada tabel 16, 17, dan 18 adalah hasil dari *areas of concern* yang telah di identifikasi dan membutuhkan pendekatan mitigasi.

Tabel 16. Mitigasi Risiko 1

Risk Mitigation	
Areas of Concern	Penyalahgunaan *key exam*
Action	*Mitigate*
Container	Kontrol
Team IT Ops	Membuat *key exam* selalu *unique* Membatasi akses *exam* hanya menggunakan *browser* spesifik *safe exam browser*

Tabel 17 Mitigasi Risiko 2

Risk Mitigation	
Areas of Concern	Gangguan Jaringan internet
Action	*Mitigate*
Container	Kontrol
Divisi Trainer	Memastikan Seluruh peserta t*raining* untuk menggunakan jaringan kantor saat melakukan ujian
IT Ops	Memberikan *Website* aturan pengecualian jika ada yang terkendala jaringan agar waktu ujian dapat di sesuaikan

Tabel 18 Mitigasi Risiko 3

Risk Mitigation	
Areas of Concern	Kesalahan input data ujian
Action	*Mitigate*
Container	*Control*
Divisi Training	Melakukan verifikasi data Ujian

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa area yang paling terdampak adalah *Trust and Reputation*, *Productivity, Finance*, serta *Safety and Health*. Selain itu, ditemukan aset TI berupa teknis yaitu komputer, *server* dan *database*, aset berupa manusia yaitu admin IT, peserta ujian dan divisi trainer sebagai pihak internal dan peserta ujian yang merupakan calon karyawan sebagai pihak eksternal.

Analisis sumber daya IT pada PT. XYZ ditemukan 5 *areas of concern* seperti penyalahgunaan hak akses, penyalahgunaan *key exam*, gangguan

jaringan internet, kesalahan input data ujian, dan *server down*. Dari seluruh *areas of concern* yang ditemukan, *relative risk score* yang tertinggi adalah 26 yaitu terjadi saat *server down*, dan penyalahgunaan hak akses oleh peserta ujian mempunyai hasil terendah yaitu bernilai 14.

Langkah selanjutnya mendiskusikan dengan pihak organisasi untuk menentukan pendekatan mitigasi yang dapat diterapkan dari setiap *areas of concern*. Hasil dialog yang telah dilakukan diperoleh skenario mitigasi dari 5 *Areas of concern*, 3 area diantaranya perlu adanya mitigasi berupa *mitigate*, 1 area yang perlu adanya mitigasi berupa *defer*, dan 1 area yang perlu adanya mitigasi berupa *accept*. Untuk pendekatan *mitigate* akan diberikan rekomendasi skenario seperti pada penyalahgunaan *key exam*, admin IT dapat merancang agar *key* exam selalu *unique* atau pada gangguan jaringan internet perlu diberlakukan aturan seluruh peserta *training* wajib menggunakan jaringan kantor saat melakukan ujian.

Saran yang ingin disampaikan oleh penulis untuk penelitian selanjutnya adalah diharapkan dapat dilakukan evaluasi secara berkala pada *asset* informasi terhadap *resiko* yang ada agar dapat diketahui kebutuhan atau kelemahan TI yang digunakan.

DAFTAR PUSTAKA

[1] D. F. Tanjung, O. A, and A. P. Widodo, "Analisis Manajemen Risiko Startup Pada Masa Pandemi Covid-19 Startup Risk Management Analysis During Covid-19 Pandemic Using," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 3, pp. 635–642, 2021, doi: 10.25126/jtiik.202184914.

[2] A. D. P. and K. Ramli, "A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods," *34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, 2019.

[3] R. Ramadhintia and R. Bisma, "Jurnal Sistem dan Teknologi Informasi Analisis Manajemen Risiko Aplikasi Ujian Online dengan Metode OCTAVE Allegro pada lembaga pendidikan," vol. 6, no. 2, 2021.

[4] B. S. G. Naibaho and D. Tjahjadi, "Kajian Manajemen Risiko Sistem Informasi Menggunakan Metode Octave Allegro," *Jutisi : Jurnal Ilmiah Teknik Informatika dan*

Sistem Informasi, vol. 11, no. 1, p. 131, 2022, doi: 10.35889/jutisi.v11i1.758.

[5] D. Irawan and M. R. Arief, "EXPLORE – Volume 11 No 2 Tahun 2021 Terakreditasi Sinta 5 SK No : 23 / E / KPT / 2019 Rekomendasi Penjual Bahan Makanan Dengan Metode Filtering Berbasis Konten dan Lokasi Pada Aplikasi Resep Masakan EXPLORE – Volume 11 No 2 Tahun 2021 Terakreditasi Sinta," *Jurnal Explore*, vol. 11, no. 2, pp. 29–34, 2021.

[6] R. a R. a. C. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," *Young*, no. May, pp. 1–113, 2007.

[7] H. Ikhsan and N. Jarti, "Analisis Risiko Keamanan Teknologi Informasi," *Jurnal Responsive*, vol. 2, no. 1, pp. 31–41, 2018.

[8] J. Sanjaya, "Analisis Risk Assessment Terhadap Perusahaan IT di Bidang Finansial Menggunakan OCTAVE Allegro Framework," *Inspiration: Jurnal Teknologi Informasi dan Komunikasi*, vol. 10, no. 1, 2020, doi: 10.35585/inspir.v10i1.2528.

[9] R. Ichsan, A. Falach, L. Abdurrahman, I. Santoso, and S. Si, "Analisis Risiko Dan Perancangan Kontrol Keamanan Informasi Pada Sistem Informasi Manajemen Rumah Sakit Modul Billing Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Khusus Ibu Dan Anak Bandung)," vol. 8, no. 2, pp. 2709–2722, 2021.

[10] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, no. 27, p. 12, 2022, doi: 10.34010/jati.v12i2.

[11] R. F. Hamzah, I. D. Jaya, and U. M. Putri, "Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X," *Jusifo*, vol. 6, no. 1, pp. 55–65, 2020, doi: 10.19109/jusifo.v6i1.5880.

[12] S. Alfarisi and N. Surantha, "Risk assessment in fleet management system using OCTAVE allegro," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 530–540, 2022, doi: 10.11591/eei.v11i1.3241.