Manajemen Risiko Keamanan Aset Informasi pada MAN 1 Pasuruan dengan Menggunakan Metode *OCTAVE Allegro*

Zuyinatul Munadhiroh[1], Anang Kunaefi[2], Faris Muslihul Amin[3]

[1,2,3] Program Studi Sistem Informasi, Universitas Islam Negeri Sunan Ampel Surabaya
[1]zuyinatul05@gmail.com
[2]akunaefi@uinsby.ac.id
[3]faris@uinsby.ac.id

***Abstrak*— Aset merupakan hal yang paling penting dan paling berharga bagi setiap lembaga maupun organisasi, dimana harus dijaga agar tidak terjadi risiko yang tidak diinginkan bagi lembaga atau organisasi tersebut. Dengan tujuan agar keberlangsungan bisnis yang ada didalamnya bisa dipertahankan dan dilindungi. MAN 1 Pasuruan memiliki aset informasi seperti *E-learning* yang harus dilindungi keamanannya. Namun, pihak MAN 1 Pasuruan belum menerapkan manajemen risiko untuk menilai risiko-risiko yang kemungkinan bisa terjadi dan belum memiliki prosedur atau dokumen secara formal dan tertulis mengenai penanganan atau mitigasi risiko. Sehingga pihak MAN 1 Pasuruan belum mengetahui tindakan tetap dan pasti untuk menangani dan mengurangi risiko yang kemungkinan terjadi. Untuk membantu MAN 1 Pasuruan mengidentifikasi, menganalisis dan memilih pendekatan mitigasi digunakan metode *OCTAVE Allegro* serta memilih kontrol yang tepat sesuai dengan ancaman yang terjadi digunakan standar internasional ISO 27001 sebagai pedoman. Pada hasil analisis manajemen risiko *E-learning* MAN 1 Pasuruan didapatkan 7 risiko dengan 5 area dampak yang memiliki risiko.**

***Kata Kunci*— Manajemen risiko, keamanan aset informasi, *OCTAVE Allegro*, ISO 27001, *E-learning*.**

I. PENDAHULUAN

Penerapan teknologi pada era kompetisi saat ini semakin meningkat di berbagai kalangan lembaga, organisasi maupun disegala lini. Tercatat pada tahun 2021 penggunaan teknologi informasi di Indonesia mencapai 202,6 juta dari 274,9 juta atau 73,7% dari total keseluruhan populasi masyarakat Indonesia yang menggunakan internet dalam mencari informasi [1]. Setiap lembaga maupun organisasi memiliki tuntutan yang besar untuk bisa menerapkan dan mengembangkan teknologi informasi maupun sistem informasi secara efektif, efisien dan aman guna terlaksananya kegiatan operasional. Dalam sistem informasi data merupakan peranan yang sangat penting karena data termasuk salah satu dari komponen sistem informasi selain *hardware*, *software*, *procedure*, *network* dan *peoples*. Dengan adanya pendapat yang telah disebutkan tersebut menunjukkan pada setiap lembaga maupun organisasi mempunyai aset yang harus diperhatikan serta dijaga keamanan dan risikonya [2]. Salah satu lembaga yang tengah bergerak maju dalam menerapkan sistem informasi dan teknologi informasi yaitu MAN 1 Pasuruan. MAN 1 Pasuruan adalah salah satu lembaga pendidikan Islam pada jenjang SMA yang ada di kota Bangil. Dalam pelaksanaan proses pembelajarannya, MAN 1 Pasuruan sangat memerlukan perhatian lebih pada keamanan aset informasi demi keberhasilan tujuan yang akan dicapai.

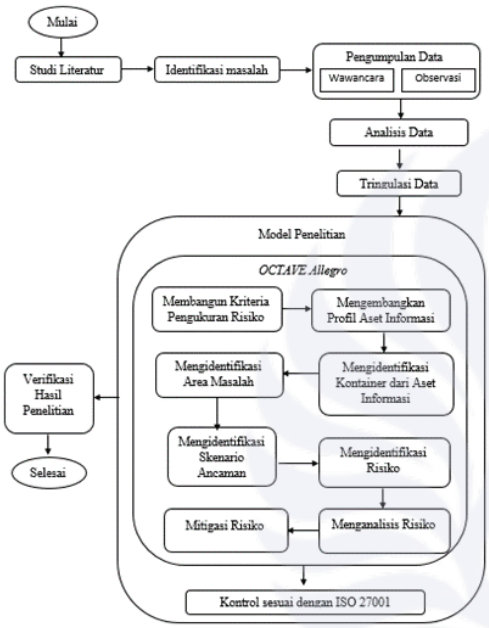
Penelitian yang memiliki kesamaan atau relevan dengan penelitian ini diantaranya peneliian yang dilakukan oleh Aulia Zulfia dkk (2021) yang berjudul "Penilaian Risiko Aset Informasi dengan Metode *OCTAVE Allegro*: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya", hasil dari penelitian tersebut adalah diperoleh pada penelitian ini adalah informasi dari 5 aset informasi yang dianggap kritikal ditemukan 73 risiko keamanan. Dalam kategori ditunda atau mitigasi didapatkan juga sebanyak 61 risiko. Kemudian pada kategori 3 ditemukan 9 risiko yaitu ditunda atau diterima. Kemudian sisanya pada kategori 4 terdapat 3 risiko yaitu diterima [3]. Adapun penelitian lain yang dilakukan oleh Soetam Rizky Wicaksono (2019) yang berjudul "*Risk Assessment* Menggunakan Pendekatan *OCTAVE Allegro* (Studi Kasus: Schoology.com)", hasil penelitian yang diperoleh adalah impact area yang menjadi prioritas pada *website Schoology* adalah Reputasi dan Kepercayaan *Customer*, karena pada situs ini terdapat kegiatan belajar mengajar menggunakan *E-learning*. Berdasarkan dari penelitian yang dilakukan, hasil lain yang didapatkan adalah tingkatan pada *website Schoology* memiliki tingkatan medium, karena data yang tersimpan dapat dibilang tidak terlalu penting sehingga kemungkinan untuk disalahgunakan oleh orang asing sangat kecil [4].

Dalam penelitian terdahulu yang pernah dilakukan di MAN 1 Pasuruan belum ada penelitian yang membahas tentang manajemen risiko, bagaimana analisis atau penilaian pada aset informasinya. Maka dari itu, dibutuhkan manajemen risiko untuk mengelola aset sistem informasi dengan dilakkan penilaian risiko dengan menggunakan *OCTAVE Allegro*. Metode *OCTAVE Allegro* hanya memfokuskan pada aset informasi dengan memiliki kriteria yang lebih jelas dan memiliki cakupan yang luas dibandingkan dengan metode lainnya yang berhubungan dengan aset informasi. Dengan menggunakan metode *OCTAVE Allegro* bisa membantu tetap ruang lingkup dengan latar belakan bisnis yang relevan dan bisa menghemat waktu [5]. Metode *OCTAVE Allegro* merupakan varian bentuk yang kritis, ancaman, aset, efisien dari ancaman operasional dan evaluasi kerentanan. Metode ini memiliki fokus pada aset informasi, maksudnya adalah bagaimana menggunakannya, dimana menyimpannya, dimana dimuatnya, bagaimana di prosesnya dan bagaimana keadaan

jika terjadi ancaman, sensibilitas dan gangguan yang akan ditimbulkan [6]. Sesuai dengan permasalahan diatas, maka dilakukan penelitian yang berjudul, "**Manajemen Risiko Keamanan Aset Informasi pada MAN 1 Pasuruan dengan Menggunakan Metode *OCTAVE Allegro***".

II. METODOLOGI

Pada penelitian ini difokuskan untuk menganalisis risiko aset sistem informasi. Untuk mendapatkan hasil penelitian yang diinginkan, pada penelituan ini dilakukan beberapa tahapan atau alur yang dilakukan pada penelitian seperti pada gambar dibawah ini



Gbr. 1 Metode Penelitian

Penerapan metode *OCTAVE Allegro* memiliki beberapa langkah yang harus dilakukan untuk menilai dan mengukur setiap risikonya, yaitu: [7]

1) Membangun Kriteria Pengukuran Risiko

Untuk melakukan langkah ini ada 2 tahapan yang dilakukan, yaitu pertama melakukan evaluasi terhadap dampak risiko pada organisasi untuk mengetahui *impact area* dengan cara membangun penggerak organisasi. Hal ini dilakukan dengan mendefinisikan ukuran kualitatifnya yang akan didokumentasikan pada *worksheets* kriteria pengukuran risiko.

2) Mengembangkan Profil Aset Informasi

Terdapat 8 (delapan) tahapan yang harus dilakukan pada langkah ini, yaitu (1) mengidentifikasi aset informasi, (2) melakukan penilaian pada akses yang dianggap kritis, (3) melakukan pengumpulan aset yang masuk dalam kategori penting, (4) mendokumentasikan alasan kenapa memilih aset tersebut, mendeskripsikan aset informasi yang kritis, (5) mengidentifikasikan kepemilikan aset informasi yang kritis, (6) mengisi kebutuhan akan keamanan untuk menjaga kerahasiaan, (7) integritas dan ketersedian dan (8) mengidentifikasi kebutuhan keamanan dalam kategori paling penting untuk aset informasi.

3) Mengidentifikasi Kontainer dari Aset Informasi

4) Mengidentifikasi Area Masalah

Pada tahapan ini dilakukan pengembangan terhadap profil dari risiko aset informasinya dengan cara mencari komponen yang jadi ancaman dari kondisi yang memiliki kemungkinan akan mengancam aset informasi.

5) Mengidentifikasi Skenario Ancaman

Pada langkah ini ada satu tahapan yang dilakukan yaitu, melakukan identifikasi pada skenario ancaman bisa dengan menggunakan *Appendix C-Threat Scenarios Questionnaires*.

6) Mengidentifikasi Risiko

Pada langkah ini dilakukan penentuan *threat scenario* yang sudah diidentifikasikan di *worksheet* yang bisa berdampak bagi organisasi.

7) Menganalisis Risiko

Pada tahapan ini yang harus dilakukan adalah me*review* kriteria pengukuran risiko yang selanjutnya dilakukan dengan menghitung nilai risiko yang relatif agar bisa dilakukan analisis risikonya dan agar bisa menyimpulkan strategi apa yang harus dilakukan.

8) Memilih Pendekatan Mitigasi

Pada langkah ini semua risiko yang telah teridentifikasi diurutkan berdasarkan dengan nilai risikonya

1. ISO 27001. Dalam penelitian ini, untuk menentukan kontrol keamanan risikonya didasarkan pada standar ISO 27001 dengan memetakkan klausul berdasarkan risiko yang ditemukan. Langkah-langkah yang dilakukan untuk menentukan kontrol berdasarkan ISO 27001 adalah sebagai berikut, (1) mengidentifikasi risiko aset (dari metode *OCTAVE Allegro*), (2) mitigasi risiko aset (dari metode *OCTAVE Allegro*), (3) pemilihan klausul yang sesuai dengan risiko aset.
2. Verifikasi Hasil Penelitian. Dilakukan kepada narasumber dengan cara mengkaji kembali semua tahapan mulai dari awal hingga akhir dari analisis risiko dengan menggunakan metode *OCTAVE Allegro*. Dibacakan kembali setiap tahapan proses analisis risiko kepada narasumber. Serta menunjukkan hasil analisis risiko aset informasi kepada narasumber.

III. HASIL DAN PEMBAHASAN

A. Membangun Kriteria Pengukuran Risiko

1) Langkah 1 Kegiatan 1

Pada langkah 1 kegiatan 1 yang harus dilakukan adalah mengidentifikasi area dampak yang kemungkinan memiliki risiko. Berdasarkan dengan hasil observasi dan wawancara yang dilakukan kepada pihak MAN 1 Pasuruan didapatkan 5 area dampak, yaitu (1) reputasi dan keberhasilan pengguna, dimana didapatkan 2 area dampak yaitu reputasi sistem dan kehilangan pengguna. (2) keuangan, didapatkan 1 area dampak yaitu biaya operasional. (3) produktivitas, didapatkan 1 area dampak yaitu jam kerja. (4) keamanan dan kesehatan, didapatkan

3 area dapak yaitu keamanan, kesehatan dan kehidupan. (5) *IT Risk*, didapatkan 3 area dampak yaitu *software*, *hardware* dan SDM.

2) Langkah 2 Kegiatan 2

TABEL 1
SKALA PRIORITAS AREA DAMPAK

Lembar Kerja *OCTAVE Allegro 6*	**PRIORITAS AREA DAMPAK**
Prioritas	**Area Dampak**
3	Reputasi dan Keberhasilan Pengguna
2	Keuangan
1	Produktivitas
4	Keamanan dan Kesehatan
5	*IT Risk*

Pada area dampak skala prioritas yang berada diurutan atas atau yang paling penting memiliki prioritas 5 dan yang tidak dianggap terlalu penting memiliki skala prioritas 1.

B. Membangun Profil Aset Informasi

TABEL II
PROFIL ASET INFORMASI

Lembar Kerja *OCTAVE Allegro* 7	**Profil Aset Informasi yang dianggap Kritis**	
(1) Aset Kritis Aset informasi apa yang paling dianggap krisis?	(2) Kenapa dianggap kritis Mengapa aset informasi ini dianggap krisis?	(3) Deskripsi Apa uraian tentang aset informasi?
Aset otomasi *E-learning*	Karena aset ini digunakan untuk proses pembelajaran secara *online* dan semua data setiap proses pembelajaran *online* ada di aset ini. Jika otomasi *E-learning* tidak dilakukan maka tidak akan bisa melakukan pengelolaan data	Aset informasi ini berisikan data siswa, data guru, data kelas, data tugas dan data-data lainnya yang berhubungan dengan proses pembelajaran *online* ada di *E-learning*
(4) Pemilik		
Siapa pemilik dari *E-learning* ini?		
Pemilik dari *E-learning* ini adalah prodistik MAN 1 Pasuruan		
(5) Persyaratan Keamanan Persyaratan keamanan apa saja yang harus diterapkan pada *E-learning* ini?		
Kerahasiaan	Dipastikan jika hanya orang-orang yang diberikan kewenangan yang dapat mengakses *E-learning*	Pegawai yang mempunyai tanggung jawab dan bagian tersendiri atas sistem yang di *handle*
Integrasi	Memastikan bahwa aset informasi tetap dalam kondisi baik dan bisa mencapai tujuan yang sudah ditentukan pihak prodistik MAN 1 Pasuruan (pemilik)	Hanya pegawai yang memiliki wewenang atau yang diberikan tanggung jawab untuk melakukan pembaruan, *input*, mengubah, memodifikasi aset informasi
Ketersediaan	Memastikan jika aset informasi dapat diakses oleh pengguna	*E-learning* harus tersedia bagi user untuk mengolah data yang ada (melakukan *input* data)
(6) Persyaratan Keamanan yang paling Penting Apa persyaratan keamanan yang paling penting untuk *E-learning*?		
• Kerahasiaan	✓ Integritas	• Ketersediaan

Pada tabel diatas dijelaskan bahwa aset informasi yang paling penting adalah *E-learning* karena jika *E-learning* tidak bisa digunakan maka proses pembelajaran secara online tidak dapat berjalan dan berdampak pada aktivitas pembelajaran yang menjadi terkendala. Persyaratan keamanan yang diprioritaskan adalah integritas karena yang dapat melakukan pembaruan hanyalah pegawai memiliki wewenang dan tanggung jawab saja yang, *input*, mengubah, memodifikasi data pada aset informasi.

C. Mengidentifikasi Kontainer Aset Informasi

TABEL III
PETA LINGKUNGAN ASET INFORMASI TEKNIKAL

Lembar Kerja *OCTAVE Allegro* 9A	**Peta Lingkungan Aset Informasi (Teknikal)**
Dalam	
Wadah Deskripsi	**Pemilik**
Server *E-learning*	Dikelola oleh prodistik MAN 1 Pasuruan
Sebagian besar informasi disimpan di server	Dikelola oleh prodistik MAN 1 Pasuruan
Jaringan Internal, terdapat kurang lebih 30 wifi yang tersebar	Dikelola oleh prodistik MAN 1 Pasuruan
Workstation	Dikelola oleh prodistik MAN 1 Pasuruan
Luar	
Source code sistem	KEMENAG RI
Internet 10mbps	Indihome

Pada tabel diatas menjelaskan tentang peta lingkungan aset informasi secara teknikal yang memiliki keterkaitan dengan proses yang dilakukan secara teknik yang dijalankan untuk

melakukan pengelolaan data yang ada di *E-learning* oleh pegawai IT MAN 1 Pasuruan.

TABEL IV
PETA LINGKUP ASET INFORMASI FISIK

Lembar Kerja *OCTAVE Allegro* 9B	**Peta Lingkungan Aset Informasi (Fisik)**
Dalam	
Wadah Deskripsi	**Pemilik**
Laporan, salinan dan ringkasan dokumen, serta laporan cetak disimpan oleh TU MAN 1 Pasuruan secara berkala	Pegawai TU

Pada tabel diatas menjelaskan tentang peta lingkungan aset informasi secara fisik yang berhubungan dengan laporan informasi yang berada di bagian IT MAN 1 Pasuruan.

TABEL V
PETA LINGKUP ASET INFORMASI *PEOPLE*

Lembar Kerja *OCTAVE Allegro* 9C	**PETA LINGKUNGAN RISIKO ASET INFORMASI (PEOPLE)**
Dalam	
Nama atau Peran/Responsibilitas	**Departemen atau Unit**
Automasi jaringan dan komputer	Layanan IT dan jaringan
Pegawai IT	Layanan Pengolah IT dan jaringan
Luar	
Kontraktor, Vendor, dll	**Organisasi**
Hosting	Tidak diketahui

Pada tabel diatas dijelaskan tentang peta lingkungan aset informasi secara people yang berhubungan dengan peranan siapa saja pihak terkait yang melakukan pengelolaan dan pertanggungjawaban pada *E-learning* MAN 1 Pasuruan.

D. Mengidentifikasi Area Masalah

TABEL VI
AREA MASALAH

No	**Area Dampak**	**ID *Risk***	**Area Masalah Yang Menjadi Perhatian**
1.	Reputasi dan keberhasilan pengguna	R1	*E-learning* mengalami *crash* karena kelebihan *user* akibat dari penyalahgunaan hak akses sehingga bisa menyebabkan kendala pada pembelajaran *online*
2.	Reputasi dan keberhasilan pengguna	R2	Tidak bisa login ke sistem sehingga tidak dapat mengakses *E-learning*
3.	Reputasi dan keberhasilan pengguna	R3	Jaringan internet yang mengalami kendala sehingga membuat *E-learning* tidak berjalan
4.	Keuangan	R4	Bencana alam seperti petir, puting beliung dan lain-lainnya yang dapat menyebabkan listrik padam serta kerusakan pada aset informasi sehingga *E-learning* tidak bisa diakses
5.	Produktivitas	R5	Terjadinya *human error* sehingga proses input data, pengolahan data pada *E-learning* menjadi tidak beraturan
6.	Keamanan dan kesehatan	R6	Hak akses ke ruang server diakses oleh orang yang tidak memiliki tanggung jawab atau tidak memiliki wewenang mengambil, menyebarkan dan menghapus data
7.	*IT RISK*	R7	Terjadi kerusakan pada *hardware* seperti pada komputer, prosesor dan harddisk yang bisa mengancam data yang tersimpan dan juga menghambat kinerja pegawai

Pada tabel diatas, dijelaskan tantang area masalah yang harus diperhatikan untuk mencegah dan meminimalisir risiko yang kemungkinan akan terjadi.

E. Mengidentifikasi Skenario Ancaman

TABEL VII
PROPERTI SKENARIO ANCAMAN

No	**ID Risk**	**Properti Ancaman**	
1.	R1	1. *People / Actor*	Siswa MAN 1 Pasuruan
		2. *Means*	Siswa yang dengan sengaja atau tidak menyebarkan username dan password untuk melakukan login lebih dari satu akun
		3. *Motive*	Ingin melakukan login lebih dari satu akun
		4. *Outcome*	Penyikapan Modifikasi
		5. *Security Requirement*	Security Requirement
2.	R2	1. *People / Actor*	Guru dan siswa MAN 1 Pasuruan
		2. *Means*	Tidak bisa login ke sistem akibat dari lupa username dan password
		3. *Motive*	Secara tidak sengaja lupa username dan

			password sehingga tidak bisa login ke sistem
		4. Outcome	Penyikapan Modifikasi
		5. Security Requirement	Menyimpan aktivitas login di akun google masing-masing
3.	R3	*1. People / Actor*	Pegawai IT MAN 1 Pasuruan
		2. Means	Dengan sengaja ataupun tidak sengaja melakukan kesalahan dalam mengatur konfigurasi jaringan
		3. Motive	Secara sengaja maupun tidak sengaja melakukan kesalahan saat mengatur konfigurasi jaringan
		4. Outcome	Interupsi Penyikapan
		5. Security Requirement	Melakukan evaluasi pada jaringan internet
4.	R4	*1. People / Actor*	Eksternal
		2. Means	Melakukan perusakan pada sistem dan semua aset yang dimiliki
		3. Motive	Secara tidak sengaja merusak sistem dan semua aset serta menghilangkan data-data penting
		4. Outcome	Modifikasi Rugi
		5. Security Requirement	Melakukan backup secara rutin
5.	R5	*1. People / Actor*	Guru dan siswa MAN 1 Pasuruan
		2. Means	Secara sengaja ataupun tidak sengaja melakukan kesalahan saat menginputkan data
		3. Motive	Secara sengaja maupun tidak sengaja melakukan kesalahan saat menginputkan data
		4. Outcome	Interupsi Penyikapan
		5. Security Requirement	Melakukan pelatihan atau simulasi dalam penggunaan sistem
6.	R6	*1. People / Actor*	Internal dan eksternal
		2. Means	Melakukan pengambilan, penyebaran dan penghapusan data
		3. Motive	Ingin mengambil, menyebarkan dan menghapus data
		4. Outcome	Penyikapan Modifikasi
		5. Security Requirement	Melakukan evaluasi pada keamanan hak akses masuk ruang server
7.	R7	*1. People / Actor*	Pegawai IT, guru atau pihak internal lainnya yang ada di MAN 1 Pasuruan
		2. Means	Ingin merusak hardware
		3. Motive	Ingin mengambil, menyebarkan dan menghapus data
		4. Outcome	Modifikasi Interupsi
		5. Security Requirement	Melakukan pengecekan secara berkala pada setiap hardware

Pada tabel diatas menjelaskan tentang identifikasi dari skenario ancaman secara terperinci mengenai *people/actor, means, motive, outcome dan security requirement*.

F. Mengidentifikasi Risiko

TABEL VIII
IDENTIFIKASI RISIKO

No	ID *Risk*	Konsekuensi
1.	R1	Terganggunya proses pembelajaran online sehingga dapat berakibat buruk pada seluruh proses pembelajaran yang ada
2.	R2	Siswa tidak bisa mengikuti pembelajaran melalui E-learning yang akan menyebabkan tertinggalnya materi pembelajaran, bahkan saat ujian siswa tidak akan bisa mengikuti ujian
3.	R3	E-learning tidak bisa diakses karena gangguan internet yang menyebabkan pembelajaran menjadi terhambat
4.	R4	Menyebabkan kerusakan sistem atau aset informasi lainnya bahkan kerusakan bisa bersifat permanen
5.	R5	Terjadinya kesalahan pada input atau pemrosesan data, sehingga data yang ada di E-learning menjadi tidak beraturan atau rancu
6.	R6	Keamanan data pada server menjadi terancam untuk dimanipulasi, disebar dan dihapus atau dihilangkan oleh orang yang tidak bertanggung jawab
7.	R7	Membahayakan data yang tersimpan bisa berakibat hilangnya data dan menghambat kinerja pegawai

Pada Tabel diatas dijelaskan tentang keterkaitan antara bagaimana skenario ancamannya dengan apa konsekuensi yang akan dihadapi oleh seluruh warga MAN 1 Pasuruan.

G. Menganalisis Risiko

1) Langkah 7 Aktivitas 1, dilakukan analisis risiko seperti pada Tabel VIII
2) Langkah 7 Aktivitas

Pada langkah langkah 1 aktivitas 2 dilakukan bertujuan untuk mengetahui area dampak yang dianggap paling penting. Dengan dilakukan tahapan 1 maka bisa didapatkan area dampak yang memiliki nilai dampak tinggi, sedang dan rendah. Cara untuk menentukan nilai dampak adalah dengan melihat efek samping yang ditimbulkan pada sistem atau aplikasi.

TABEL IX
SKOR KESELURUHAN AREA DAMPAK

Area Dampak	Peringkat	Rendah/ R (1)	Sedang/ S (2)	Tinggi/ T (3)
Reputasi dan Keberhasilan Pengguna	3	3	6	9
Keuangan	2	2	4	6
Produktivitas	1	1	2	3
Keamanan dan Kesehatan	4	4	8	12
IT RISK	5	5	10	15

Pada tabel diatas, didapatkan nilai pada masing-masing area dampak adalah mengalikan peringkat pada nilai dampak dengan level masing-masing dimana tinggi bernilai 3, sedang bernilai 2 dan rendah bernilai 1.

3) Langkah 7 Aktivitas 3

TABEL X
MENGHITUNG TOTAL SKOR AREA DAMPAK

R1	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	T (3)	9
	Keuangan	2	S (2)	4
	Produktivitas	1	R (1)	1
	Keamanan dan Kesehatan	4	R (1)	4
	IT RISK	5	T (3)	15
	Skor Total			**33**
R2	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	T (3)	9
	Keuangan	2	R (1)	2
	Produktivitas	1	R (1)	1
	Keamanan dan Kesehatan	4	R (1)	4
	IT RISK	5	R (1)	5
	Skor Total			**21**
R3	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	T (3)	9
	Keuangan	2	R (1)	2
	Produktivitas	1	R (1)	1
	Keamanan dan Kesehatan	4	R (1)	4
	IT RISK	5	S (2)	10
	Skor Total			**26**
R4	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	R (1)	3
	Keuangan	2	T (3)	6
	Produktivitas	1	R (1)	1
	Keamanan dan Kesehatan	4	T (3)	12
	IT RISK	5	T (3)	15
	Skor Total			**37**
R5	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	R (1)	3
	Keuangan	2	T (3)	6
	Produktivitas	1	T (3)	3
	Keamanan dan Kesehatan	4	R (1)	4
	IT RISK	5	R (1)	5
	Skor Total			**21**
R6	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	R (1)	3
	Keuangan	2	R (1)	2
	Produktivitas	1	R (1)	1
	Keamanan dan Kesehatan	4	T (3)	12
	IT RISK	5	T (3)	15
	Skor Total			**33**
R7	**Area Dampak**	**Peringkat**	**Nilai Dampak**	**Nilai**
	Reputasi dan Keberhasilan Pengguna	3	R (1)	3
	Keuangan	2	T (3)	6
	Produktivitas	1	R (1)	1

	Keamanan dan Kesehatan	4	R (1)	4
	IT RISK	5	T (3)	15
	Skor Total			**29**

Pada Tabel diatas menghitung skor area dampak, nilai dampak tinggi memiliki nilai 3, sedang memiliki nilai 2 dan rendah memiliki nilai 1. Sedangkan nilai didapatkan dengan cara mengalikan peringkat dengan nilai dampak.

H. Memilih Pendekatan Mitigasi

1) Langkah 8 Aktivitas 1

TABEL XI
RELATIVE RISK MATRIX

Relative Risk Matrix			
Risk Skore			
Kemungkinan	30 - 40	16 - 29	0 -5
T	POOL 1	POOL 2	POOL 2
S	POOL 2	POOL 2	POOL 3
R	POOL 3	POOL 3	POOL 4

2) Langkah 8 Aktivitas 2, pendekatan mitigasi. Dimana pada pool 1 pendekatannya adalah mengurangi, pool 2 menunda atau mengurangi, pool 3 menerima atau mengurangi dan pool 4 menerima
3) Langkah 8 Aktivitas 3

TABEL XII
MITIGASI RISIKO

ID Risk	**Tindakan**	**Wadah**
R1	Mengurangi	Kontrol teknik dan *people*
R2	Menunda atau Mengurangi	Kontrol teknik dan *people*
R3	Menunda atau Mengurangi	Kontrol teknik
R4	Mengurangi	Kontrol teknik, fisik dan *people*
R5	Menerima atau Mengurangi	Kontrol *people*
R6	Mengurangi	Kontrol teknik, fisik dan people
R7	Menunda atau Mengurangi	Kontrol teknik

1. Kontrol ISO 27001 pada R1

Didapatkan R1 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu, *E-learning* mengalami *crash* karena kelebihan *user* akibat dari penyalahgunaan hak akses sehingga bisa menyebabkan kendala pada pembelajaran *online*. Mitigasi risiko yang didapatkan berdasarkan hasil diskusi dengan pegawai IT MAN 1 Pasuruan yang tepat sesuai dengan standar ISO 27001 pada klausul A.7: A.7.1.2; A.7.2.1; A.7.2.2 dan A.7.2.3.

2. Kontrol ISO 27001 pada R2

Didapatkan mitigasi R2 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu pada klausul A.9: A.9.2.2.

3. Kontrol ISO 27001 pada R3

Didapatkan mitigasi R3 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu pada klausul A.13: A.13.1.1 dan A.13.1.2.

4. Kontrol ISO 27001 pada R4

Didapatkan mitigasi R4 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu pada klausul A.11: A.11.1.1; A.11.1.4 dan A.11.1.5.

5. Kontrol ISO 27001 pada R5

Didapatkan mitigasi R5 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu pada klausul A.7: A.7.2.2.

6. Kontrol ISO 27001 pada R6

Didapatkan mitigasi R6 yang ditemukan pada *E-learning* MAN 1 Pasuruan yaitu pada klausul A.6: A.6.1.1 dan A.6.1.2, A.9: A.9.1.1; A.9.1.2; A.9.4.1; A.9.4.3; A.9.4.4 dan A.9.4.5, A.11: A.11.1.1; A.11.1.2; A.11.1.3 dan A.11.1.4, A.18: A.18.2.1 dan A.18.2.2.

7. Kontrol ISO 27001 pada R7

Didapatkan mitigasi R6 yang ditemukan pada E-learning MAN 1 Pasuruan yaitu pada klausul A.11: A.11.2.1; A.11.2.2; A.11.2.3 dan A.11.2.4, A.12: A.12.2.1 dan A.12.3.1.

Berdasarkan dengan hasil penilaian yang telah dilakukan menggunakan metode *OCTAVE Allegro* ditemukan 5 area dampak yang memiliki risiko pada *E-learning* MAN 1 Pasuruan. Sedangkan untuk risikonya terdapat 7 risiko yang kemungkinan terjadi pada *E-learning* MAN 1 Pasuruan. Dari hasil penilaian tersebut, maka pihak IT MAN 1 Pasuruan dapat membuat perencanaan pada strategi untuk pengelolaan manajemen risiko demi menjaga keamanan sistem yang digunakan. Berikut ini adalah risk register risiko-risiko yang telah diidentifikasi.

IV. KESIMPULAN

Berdasarkan hasil penilaian dan analisis risiko dengan menggunakan metode *OCTAVE Allegro* pada penelitian ini, dapat ditarik kesimpulan setelah dilakukan seluruh proses penilaian manajemen risiko sesuai dengan metode, maka diperoleh hasil tingkatan risiko pada *E-learning* MAN 1 Pasuruan adalah:

1. Terdapat 5 area dampak yang memiliki risiko pada *E-learning* MAN 1 Pasuruan. Hasil penilaian risiko yang didapatkan sesuai dengan metode *OCTAVE Allegro* yaitu reputasi dan keberhasilan pengguna berada pada prioritas ke-3, keuangan berada pada prioritas ke-2, produktivitas berada pada prioritas ke-1, keamanan dan kesehatan berada pada prioritas ke-4 dan IT Risk berada pada prioritas ke-5.
2. Berdasarkan hasil analisis sesuai dengan metode *OCTAVE Allegro* didapatkan 7 risiko yang terjadi pada *E-learning* MAN 1 Pasuruan, yaitu yang *pertama E-learning* mengalami crash karena kelebihan *user* akibat dari penyalahgunaan hak akses sehingga bisa menyebabkan

kendala pada pembelajaran *online* dengan pendekatan mitigasi pool 1 yaitu mengurangi. *Kedua* terjadi kerusakan pada *hardware* seperti pada komputer, prosesor dan *harddisk* yang bisa mengancam data yang tersimpan dan juga menghambat kinerja pegawai dengan pendekatan mitigasi pool 2 yaitu menunda atau mengurangi. *Ketiga* hak akses ke ruang server diakses oleh orang yang tidak bertanggung jawab atau tidak berwenang yang dapat mengambil, menyebarkan dan menghapus data dengan pendekatan mitigasi pool 2 yaitu menunda atau mengurangi. *Keempat* jaringan internet yang mengalami kendala sehingga membuat *E-learning* tidak berjalan dengan pendekatan mitigasi pool 2 yaitu menunda atau mengurangi. *Kelima* terjadinya *human error* sehingga proses *input* data, pengolahan data pada *E-learning* menjadi tidak dengan pendekatan mitigasi pool 3 yaitu menerima atau mengurangi. *Keenam* Bencana alam seperti petir, puting beliung dan lain-lainnya yang dapat menyebabkan listrik padam sehingga *E-learning* tidak bisa diakses dengan pendekatan mitigasi pool 1 yaitu mengurangi. Terakhir, yang *ketujuh* adalah tidak bisa *login* ke sistem sehingga tidak dapat mengakses *E-learning* dengan pendekatan mitigasi pool 3 yaitu menerima atau mengurangi.

3. Berdasarkan hasil analisis manajemen risiko didapatkan kontrol sesuai dengan ISO 27001 adalah risiko pertama pada klausul A.7. Risiko kedua pada klausul A.11 dan A.12. Risiko ketiga pada klausul A.6, A.9, dan A.18, risiko keempat pada klausul A.13, risiko kelima pada klausul A.17, risiko keenam pada klausul A.11, dan risiko ketujuh pada klausul A.9.

REFERENSI

[1] Afrianto, Y., Ginting, N. B., Suratun, S., & Nelawati, Y. (2020). Sistem Informasi Inventory POS (Point of Sales) Berbasis Web Pada Counter Cellular. JURTEKSI (Jurnal Teknologi dan Sistem Informasi), 6(2), 125-134.

[2] Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.Young, May, 1-154.

[3] Rachmaniah, M., & Mustafa, B. (2015). Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode OCTAVE Allegro. Jurnal Pustakawan Indonesia, 14(1).

[4] [4] Tobing, J. J. L., & Puspa, A. K. (2015). Analisis Manajemen Resiko untuk Evaluasi Aset Menggunakan Metode OCTAVE Allegro. EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi, 5(1).

[5] UKEssays. (November 2018). OCTAVE Allegro Risk Assessment Method. Retrieved from https://www.ukessays.com/essays/business/octave-allegro-risk-assessment-method-2338.php?vref=1.

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

[7] Zulfia, A., Ruskan, E. L., & Putra, P. (2021). Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya.