Analisis dan Penilaian Risiko Keamanan Informasi Menggunakan OCTAVE Allegro (Studi Kasus : PT. XYZ)

1st Raihan Armadyana
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
raihanarmadyana@student.telkomuniversity.ac.id

2nd Rahmat Yasirandi
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
Rahmat.yasirandi@telkomuniversity.ac.id

3rd Muhammad Al Makky
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
malmakky@telkomuniversity.ac.id

Abstrak—PT. XYZ ialah salah satu anak perusahaan dari PT. Telekomunikasi Indonesia yang berfokus pada layanan Business Process Outsourcing. Penggunaan aset Teknologi Informasi sudah dilakukan oleh PT. XYZ untuk menunjang proses bisnis perusahaan. Perencanaan keamanan informasi dilakukan dengan pendekatan OCTAVE Allegro dalam penilaian risiko. Metode OCTAVE Allegro dipilih karena metode tersebut sudah mencakup tiga aspek keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan. Penilaian risiko ini akan menjadi acuan untuk membuat langkah mitigasi risiko berdasarkan standar ISO 27001. Penyusunan langkah mitigasi risiko diharapkan dapat meningkatkan tingkat keefektifan dalam penggunaan aset Teknologi Informasi pada PT. XYZ. Hasil penelitian menunjukan bahwa terdapat 15 risiko yang teridentifikasi dan terdapat 14 poin mitigasi risiko

Kata kunci —keamanan informasi, penilaian risiko, OCTAVE Allegro, ISO 27001.

Abstract—PT. XYZ is a company that focuses on Business Process Outsourcing services. The use of Information Technologyassets has been carried out by PT. XYZ to support the company's business processes. Information security risk assessment is carried out using the OCTAVE Allegro method. The OCTAVE Allegro method was chosen because it covers three aspects of information security: confidentiality, integrity, and availability. This risk assessment will be a reference for making risk mitigation measures based on the international standard ISO 27001. Preparing risk mitigation measures is expected to increase the effectiveness of using Information Technology assets at PT. XYZ.The results showed that there were 15 identified risks and 14 risk mitigation points..

Keywords—information security, risk assessment, OCTAVE Allegro, ISO 27001.

I. PENDAHULUAN

A. Latar Belakang

Perkembangan ilmu pengetahuan dan teknologi informasi pada era ini terlihat sangat pesat, seiringnya waktu segala aktivitas dalam berbagai bidang akan mengandalkan penggunaan teknologi informasi karena dapat memudahkan dalam menjalankan proses bisnis yang ada khususnya dalam perusahaan-perusahaan besar. Teknologi Informasi (TI) selain memudahkan bagi suatu organisasi/perusahaan juga memberikan dampak risiko- risiko yang beragam, contohnya kehilangan data baik disengaja maupun tidak disengaja. Apalagi data-data perusahaan yang sifatnya sensitif. Maka hal yang perlu diperhatikan bagi beberapa perusahaan besar ialah penting nya menjaga keamanan aset informasi mereka dari beberapa ancaman-ancaman yang ada. PT. XYZ adalah perusahaan berfokus pada layanan Business Process Outsourcing. Perusahaan ini umumnya mengelola informasi baik informasi secara internal ataupun eksternal yang kemudian akan disimpan atau dibagikan. Dengan menyimpan sejumlah data dan informasi milik perusahaan maupun klien maka perlu diperhatikan penerapan keamanan informasi yang dilakukan perusahaan. Bahaya kehilangan data, kerusakan, atau terekspos data ke pihak luar yang tidak berwenang meningkat karena lebih banyak informasi perusahaan disimpan, dikelola, dan dibagikan. Mengambil teori dari Sarno & Iffano, Keamanan informasi adalah metode untuk melindungi aset informasi dari potensi bahaya. Keamanan merupakan isu penting bagi sebuah organisasi.

Seperti pada kasus nya pada PT. XYZ yang menjalani proses bisnis mereka dengan bantuan penggunaan aset TI mereka yang tentunya dapat menyebabkan berbagai risiko dari penggunanya. Untuk membantu hal tersebut perlu dilakukan penilaian risiko pada aset TI yang dimiliki perusahaan. Yang hasilnya nanti akan dijadikan acuan untuk menyusun langkah-langkah mitigasi pada risiko yang OCTAVE Allegro adalah salah satu metode penilaian risiko yang mengoptimalkan proses penilaian risiko keamanan informasi dengan meminimalkan waktu, sumberdaya manusia dan sumberdaya lainnya. Pendekatan OCTAVE Allegro berfokus pada aset informasi yang akan digunakan, disimpan, dibagikan dan bagaimanan informasi tersebut terdapat ancaman-ancaman yang tidak diduga dan gangguan lainnya. Hasil dari penilaian risiko dengan melakukan pendekatan OCTAVE Allegro

akan dijadikan acuan dalam menyusun langkah mitigasi risiko dengan standard control ISO 27001.

B. Topik dan Batasannya

Topik pada peneltian ini berupa penilaian risiko dengan metode OCTAVE Allegro. Adapun dua rumusan masalah pada peneltian ini. Yang pertama, bagaimana hasil penilaian risiko dengan metode OCTAVE Allegro pada PT. XYZ dan yang kedua bagaimana langkah mitigasi pada risiko yang ada pada PT. XYZ berdasarkan ISO27001.

Batasan pada penelitian ini ialah penilaian risiko dilakukan pada proses bisnis recruitment pada PT. XYZ dengan metode OCTAVE Allegro dan langkah mitigasi dibuat berdasarkan standar internasional ISO 27001.

II. KAJIAN TEORI

A. Keamanan Informasi

Keamanan informasi memiliki tiga aspek penting yaitu [1] :

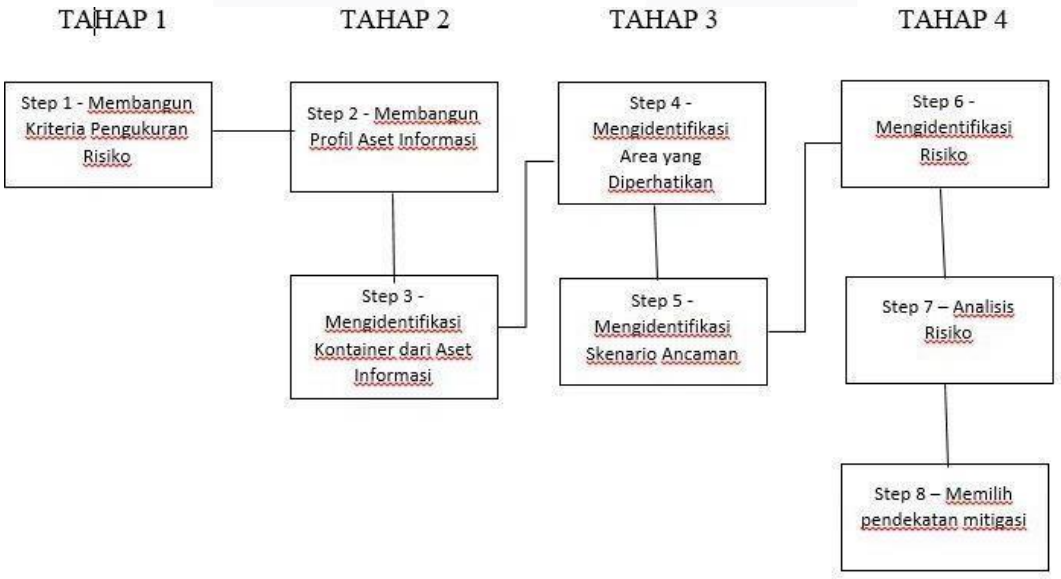
1. *Confidentiality* (Kerahasiaan) → Aspek ini menjamin keamanan data dan informasi.
   Confidentiality memiliki dua pilar dalam penerapannya yaitu *Authentication* dan *Authorization*.
2. *Integrity* (Integritas) → Aspek ini menjamin tingkat akurasi dan kelengkapan data dan informasi. Memastikan bahwa data tidak dirubah atau dimodifikasi tanpa ada izin pihak yang berwenang.
3. *Availability* (Ketersediaan) → Aspek ini menjamin bahwa data dan informasi yang akan diminta oleh pihak berwenang tersedia dan mudah untuk diakses. Selain data dan informasi, mekanisme authentication, saluran akses dan sistem operasi nya harus berfungsi dengan baik agar data terlindungi dan memastikan data tersedia saat dibutuhkan.

B. ISO 27001

ISO (*International Organization for Standardization*) adalah sistem khusus untuk standardisasi diseluruh dunia [2]. ISO 27001 merupakan standar internasional untuk untuk melakukan pendekatan manajemen risiko, memastikan otoritas terkait bahwa risiko telah dikelola dengan baik, untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi. [2].

C. **OCTAVE Allegro**

OCTAVE Allegro adalah metode penilaian risiko yang mengoptimalkan proses penilaian risiko keamanan informasi dengan meminimalkan waktu, sumberdaya manusia dan sumberdaya lainnya [3]. Fokus dari OCTAVE Allegro ialah pada aset informasi dalam konteks bagaimana mereka digunakan, disimpan, diproses dan bagaimana informasi tersebut terdapat ancaman-ancaman yang tidak diduga dan gangguan lainnya [3]. OCTAVE Allegro memiliki delapan langkah dalam empattahap, yaitu :



D. Manajemen Risiko

Dalam proses manajemen risiko keamanan informasi hal yang harus diperhatikan ialah bagaimana strategi manajemen risiko perusahaan/instansi harus diantisipasi secara akurat [6].

Manajemen memiliki definisi yaitu aktivitas manusia umum dalam skala domestik, lingkungan sosial dan politik, dan dalam organisasi. Risiko merupakan sebuah probabilitas yang berdampak pada kerusakan atau

kerugian [7]. Jika definisi dari manajemen dan risiko disatukan maka dapat dideskripsikan bahwa manajemen risiko ialah sebuah aktivitas manusia dalam menganalisis kemungkinan dampak kerusakan atau kerugian dalam sebuah organisasi.

III. PT. XYZ.

Pada bab ini menjelaskan tentang profil studi kasus penelitian. Bagaimana visi & misi dari PT. XYZ.

A. Profil Perusahaan

PT. XYZ adalah perusahaan berfokus pada layanan Business Process Outsourcing. PT. XYZ berlokasi di daerah Jakarta Selatan kawasan Jalan Fatmawati. PT. XYZ bergerak mulai dari tahun 1970an, PT. XYZ merupakan salah satu perusahaan pertama yang beroperasi dibidang penyedia layanan informasi telepon di Indonesia. Layanan Business Process Outsourcing ialah layanan Outsourcing yang meliputi bidang Human Resource Services, Contact Center Services, IT Services, dan Back Office Services. Produk yang dihasilkan PT. XYZ merupakan komitmen yang dilakukan PT. XYZ dalam memberikan layanan informasi yang terbaik dan komunikasi yang terbaik untuk customer dan masyarakat Indonesia.

B. Aplikasi Recruitment SSO

Aplikasi Recruitment SSO ialah merupakan salah satu aplikasi yang dikelola oleh DIvisi IT BPM. Aplikasi Recruitment SSO mendukung dan memfasilitasi segala proses bisnis recruitment PT. XYZ. Mulai dari input CV hingga proses diterima atau tidaknya.

IV. HASIL DAN PEMBAHASAN

Pada bagian analisis data, data yang sudah dikumpulkan akan diolah dan dianalisis dengan metode OCTAVE Allegro. Berikut tahapan dari proses analisis data menggunakan OCTAVE Allegro.

A. Membangun Kriteria Pengukuran Risiko

Hal yang pertama dilakukan dalam OCTAVE Allegro ialah membangun kriteria pengukuran risiko. Kriteria pengukuran risiko akan didokumentasikan dengan *Risk Measurement Criteria Worksheet.* Berikut tabel kriteria pengukuran risiko.

TABEL 1
KRITERIA PENGUKURAN RISIKO

Allegro Worksheet 3	**KRITERIA PENGUKURAN RISIKO – PRODUKTIVITAS**		
Impact Area	**Low**	**Medium**	**High**
Jam Kerja	Jam kerja staff meningkat kurang dari 4 jam dalam per bulan.	Jam kerja staff meningkat mulai dari 4 jam sampai 10 jam dalam per bulan.	Jam kerja staff meningkat lebih dari 10 jam dalam perbulan.

B. Membangun Profil Aset Informasi

Tahapan selanjutnya setelah dilakukan tahap pertama ialah membangun profil aset informasi. Profil aset informasi yang akan dibangun ialah aset informasi yang sudah ditentukan sebagai aset informasi kritikal yang nantinya akan didokumentasikan lewat *Critical Information Asset Profile Worksheet*.

TABEL 2
PROFIL ASET INFORMASI KRITIS

Allegro Worksheet 8A	**PROFIL ASET INFORMASI KRITIS**	
Aset Kritis (Nama aset informasikritis?)	**Alasan Pemilihan** (Mengapa aset informasi ini penting?)	**Deskripsi** (Apa deskripsi dari aset informasi ini?)
Data SSO Operation	Untuk memastikan SSO Operation memiliki	Untuk user SSO Operation berisi tentang nama karyawan,

	kewenangan untuk mengakses Recruitment SSO.	NIP, keterangan jabatan, username, dan password.
Owner		
SSO Operation		
Security Requirements		
Confidentiality	Pihak yang berwenang yang dapat melihat aset informasi ini	SSO Operation, IT SSO.
Integrity	Pihak yang berwenang yang dapat memodifikasi asetinformasi ini	SSO Operation, IT SSO.
Availability	Aset ini harus tersedia untuk pihak ini agar dapat melakukantugasnya	SSO Operation
	Aset ini harus tersedia dalam 24 jam, 7 hari dalam seminggu	
Most Important Security Requirements		
[] Confidentiality	[V] Integrity	[] Availability

C. Identifikasi Kontainer dari Aset Informasi

Langkah ketiga pada OCTAVE Allegro ialah mengidentifikasi kontainer dari aset informasi. Kontainer ialah wadah yang mana aset disimpan, dibagikan, dan diolah. Semua kontainer pada langkah ini yang menyimpan, mengirim, dan memproses baik internal maupun eksternal diidentifikasi. Kontainer diidentifikasi dengan Worksheet 9 yaitu *Information Asset Risk Environment Map* yang terbagi tiga jenis yaitu *technical, physical, people.*

TABEL 3
TECHNICAL

Allegro Worksheet 9a – Data SSO Operation	**PETA LINGKUNGAN RISIKO ASET INFORMASI (TECHNICAL)**
INTERNAL	
DESKRIPSI KONTAINER	**OWNER(S)**
1. *Personal Computer & Notebook* Peralatan fisik yang digunakan untuk mengakses aplikasi Recruitment SSO.	SSO Operation
2. Database Server Tempat data dari Recruitment SSO disimpan.	IT SSO
3. Aplikasi Recruitment SSO Data diakses menggunakan aplikasi Recruitment SSO	SSO Operation dan IT SSO.
EXTERNAL	
DESKRIPSI KONTAINER	**OWNER(S)**
Jaringan Internet	Internet Service Provider

TABEL 4
PHYSICAL

Allegro Worksheet 9b – Data SSO Operation	PETA LINGKUNGAN RISIKO ASET INFORMASI (PHYSICAL)
EXTERNAL	
DESKRIPSI KONTAINER	OWNER(S)
Database Server	PT. XYZ
Jaringan Internet	Internet Service Provider

TABEL 5
PEOPLE

Allegro Worksheet 9c – Data SSO Operation	PETA LINGKUNGAN RISIKO ASET INFORMASI (PEOPLE)
INTERNAL	
NAMA ATAU PERAN TANGGUNG JAWAB	DEPARTEMEN ATAU UNIT
IT SSO	IT Business Process Management
SSO Operation	IT Business Process Management

D. Mengindetifikasi Area yang Diperhatikan

Tahapan selanjutnya setelah mengidentifikasi kontainer dari aset informasi ialah mengidentifikasi a*rea of concern* atau area yang diperhatikan. *Area of Concern* adalah penjelasan deskriptif tentang masalah yang berdampak pada aset informasi. Berikut dokumentasi *area of concern* yang bisa dilihat pada tabel dibawah ini.

TABEL 6
AOC *DATA SSO OPERATION*

No.	Area of Concern – Data SSO Operation
1.	Pihak yang tidak memiliki kewenangan dapat masuk ke sistem.
2.	Terdapat kesalahan saat input data.
3.	Penyebaran hak akses pada data SSO Operation.
4.	Kehilangan data pada data SSO Operation.

E. Mengidentifikasi Skenario Ancaman

Tahapan selanjutnya yaitu mengidentifikasi scenario ancaman. Setelah mengidentifikasi area yangdiperhatikan. Pada step 5 area yang diperhatikan akan diperluas menjadi scenario ancaman atau *threat scenario* yang menggambarkan karakteristik ancaman secara lebih dalam dengan cara melengkapi *Information Asset Risk Worksheet.*

TABEL 7
DATA SSO OPERATION

Allegro Worksheet 10		RISIKO ASET INFORMASI - WORKSHEET
1	Information Asset	Data SSO Operation
	Area of Concern	Pihak yang tidak memiliki kewenangan dapat masuk ke sistem.
	(1) Actor	Tidak diketahui
	(2) Means	Mengeksploitasi kelemahan atau titik celah keamanan dalam sistem dengan sengaja.
	(3) Motives	*Malicious*

	(4) Outcome	[V] Disclosure [V] Modification [V] Destruction [V] Interruption
	(5) Security Requirement	Dilakukan peninjauan pada keamanan sistem secara berkala dan meningkatkan keamanan untuk software, hardware,dan jaringan.
	(6) Probability	[] High [] Medium [] Low

F. Mengidentifikasi Risiko

Setelah itu yang harus dilakukan setelah identifikasi skenario ancamanialah mengidentifikasi risiko. Tujuan dari langkah ini ialah mengetahui konsekuensi pada setiap *threat scenario* dokumentasikan dalam setiap *Information Asset Risk Worksheet.* Berikut konsekuensi dari skenario ancaman pada data SSO Operation, data Lowongan, data Pelamar, dan data Lamaran.

TABEL 8
KONSEKUENSI DATA SSO OPERATION

No.	Area of Concern	(7) Consequence
1.	Pihak yang tidak memiliki kewenangan dapat masuk ke sistem.	Data SSO Operation terancam dan dapat disebarluaskan secara bebas.

TABEL 9
KONSEKUENSI DATA LOWONGAN

No.	Area of Concern	(7) Consequence
1.	Terdapat kesalahan saat input datalowongan.	User harus menginputkan ulang data yang akan diperbaharui dan harus mengkonfirmasi apakah data sudah benar.

TABEL 10
KONSEKUENSI DATA PELAMAR

No.	Area of Concern	(7) Consequence
1.	Pemalsuan pada data pelamar.	Reputasi pelamar menjadi buruk dan akan mendapatkan blacklist dari perusahaan.

TABEL 11
KONSEKUENSI DATA LAMARAN

No.	Area of Concern	(7) Consequence
3.	Terjadi kerusakan data pada datalamaran.	Harus dilakukan backup data yang akanmemakan waktu di database yang berbeda.

G. Analisis Risiko

Langkah ketujuh dari OCTAVE Allegro ialah analisis risiko. Pada langkah ini, dengan menetapkan skorrisiko untuk setiap ancaman pada aset informasi dapat dinilai dampak ancaman terhadap organisasi secara kualitatif. Tahapan ini terdapat dua aktivitas yaitu membuat tabel *impact area* dengan cara melakukan *review* pada kriteria pengukuran risiko yang dilakukan pada langkah 1 OCTAVE Allegro. Aktivitas ini berfokus pada dampak *high, medium, low.* Aktivitas kedua ialah skor risiko relatif akan dihitung, skor risiko relatif akan digunakan untuk organisasi dalam menganalisis risiko dan memilih strategi dalam menghadapi risiko.

TABEL 12
IMPACT AREA

Priority	Impact Areas	Low (1)	Medium (2)	High (3)

3	Reputasi dan Kepercayaan Pelanggan	3	6	9
2	Finansial	2	4	6
5	Produktivitas	5	10	15
4	Keselamatan dan Kesehatan	4	8	12
1	Denda dan Pinalti	1	2	3

TABEL 13
RISIKO ASET INFORMASI (DATA SSO OPERATION)

<table>
<tr><td colspan="3">Data SSO Operation</td><td colspan="3">RISIKO ASET INFORMASI - WORKSHEET</td></tr>
<tr><td rowspan="11">Information Asset Risk</td><td rowspan="10">Threat</td><td>Information Asset</td><td colspan="3">Data SSO Operation</td></tr>
<tr><td>Area of Concern</td><td colspan="3">Pihak yang tidak memiliki kewenangan dapat masuk ke sistem.</td></tr>
<tr><td>1 – Actor</td><td colspan="3">Tidak diketahui</td></tr>
<tr><td>2 – Means</td><td colspan="3">Mengeksploitasi kelemahan atau titik celah keamanandalam sistem dengan sengaja.</td></tr>
<tr><td>3 – Motives</td><td colspan="3">Malicious</td></tr>
<tr><td>4 - Outcome</td><td colspan="3">[V] Disclosure
[V] Modification
[V] Destruction
[V] Interruption</td></tr>
<tr><td>5 – Security Requirement</td><td colspan="3">Dilakukan peninjauan pada keamanan sistem secara berkala dan meningkatkan keamanan untuk software,
hardware, dan jaringan.</td></tr>
<tr><td>6 - Probability</td><td colspan="3">[] High
[V] Medium[]
Low</td></tr>
<tr><td colspan="2">7 - Consequences</td><td colspan="3">8 - Severity</td></tr>
<tr><td colspan="2" rowspan="2">Data SSO Operation terancam dan dapat disebar luaskan secara bebas.</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputasi dan Kepercayaan Pelanggan</td><td>Medium</td><td>6</td></tr>
</table>

		Finansial	Medium	4
		Produktivitas	High	15
		Keselamatan & Kesehatan	Low	4
		Denda & Pinalti	Low	1
Relative Risk Score				30

H. Memilih Pendekatan Mitigasi

Langkah terakhir dari OCTAVE Allegro ialah memilih pendekatan mitigasi. Dalam OCTAVE Allegro terkait dengan pendekatan mitigasi, organisasi mempunyai tiga pilihan saat menghadapi risiko yaitu *accept, defer, mitigate.* Aktivitas pertama dalam langkah ini ialah melakukan penempatan pool pada setiap *area of concern* yang telah diidentifikasi dan analisis hingga memiliki skor risiko relatif kedalam *Relative Risk Matrix*. Penempatan pool akan menjadi acuan apakah risiko perlu dimitigasi atau tidak atau harus ditangguhkan. Berikut *Relative Risk Matrix*pada OCTAVE Allegro.

RELATIVE RISK MATRIX			
Probability	**Risk Score**		
	30-45	**16-29**	**0-15**
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

GAMBAR 1
RELATIVE RISK MATRIX

Aktivitas kedua adalah menetapkan pendekatan mitigasi berdasarkan penempatan pool. Berikut pendekatan mitigasi pada OCTAVE Allegro.

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

GAMBAR 2
PENEMPATAN POOL

Aktivitas ketiga ialah membuat rencana mitigasi berdasarkan pendekatan mitigasi. Tabel dibawah ini menjelaskan tentang langkah pendekatan mitigasi apa yang akan diambil pada masing-masing area of concern.

TABEL 14
PENDEKATAN MITIGASI

Area of Concern	**Risk Code**	**Probability**	**Risk Score**	**Pool**	**Mitigation Approach**
Pihak yang tidak memiliki kewenangan dapat masuk ke sistem. – Data SSO Operation	SSO1	Medium	30	Pool 2	Mitigate
Terdapat kesalahan saat input data.	SSO2	Low	20	Pool 3	Accept

Penyebaran hak akses pada data SSO	SSO3	Low	25	Pool 3	Defer
Kehilangan data padadata SSO Operation.	SSO4	Medium	30	Pool 2	Mitigate
Pihak yang tidak memiliki kewenangan dapat masuk ke sistem. – Data Lowongan	LWG1	Medium	30	Pool 2	Mitigate
Terdapat kesalahan saat input datalowongan	LWG2	Low	20	Pool 3	Accept
Terjadi kerusakan data pada data lowongan.	LWG3	Medium	30	Pool 2	Mitigate
Pemalsuan pada data lowongan	LWG4	Low	28	Pool 3	Defer
Pihak yang tidak memiliki kewenangan dapat masuk ke sistem. – Data Pelamar	PEL1	Medium	30	Pool 2	Mitigate
Terdapat kesalahan saat input data pelamar.	PEL2	Low	20	Pool 3	Accept
Terjadi kerusakan data pada data pelamar.	PEL3	Medium	30	Pool 2	Mitigate
Pemalsuan pada data pelamar	PEL4	Low	28	Pool 3	Defer
Pihak yang tidak memiliki kewenangan dapat masuk ke sistem. – Data Lamaran	LMR1	Medium	30	Pool 2	Mitigate
Terdapat kesalahansaat mengapply lamaran.	LMR2	Low	20	Pool 3	Accept
Terjadi kerusakan datapada data lamaran	LMR3	Medium	30	Pool 2	Mitigate

V. REKOMENDASI PERENCANAAN KONTROL

Pada bab ini akan dijelaskan tentang pemilihan kontrol untuk risiko yang telah diidentifikasi. Dalam OCTAVE Allegro tidak ada rekomendasi kontrol risiko sehingga dalam penelitian ini untuk menentukan rekomendasi kontrol risiko digunakan standar ISO 27001.

A. Rekomendasi KontrolKontrol risiko ialah tindakan mengelola potensi risiko sehingga kemungkinan risiko terjadi lagi akan berkurang di masa depan. Standar internasional yang disebut ISO 27001 adalah standar internasional yang dibuat untuk menentukan persyaratan untuk membuat, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi. Berikut tabel rekomendasi kontrol pada setiap risiko yang telah diidentifikasi.

TABEL 15
REKOMENDASI KONTROL

No.	Area of Concern	Risk Code	Klausul ISO 27001	Kontrol
1.	Pihak yang tidak memiliki kewenangan dapat masukke sistem. – Data SSO Operation	SSO1	A.10.1.1 Kebijakan penggunaan kontrol kryptografi	- Pembuatan dan penerapan kebijakan kontrol kryptografiuntuk menjagainformasi harusditerapkan. (A.10.1.1)
2.	Pihak yang tidak memiliki kewenangan dapat masukke sistem. – Data Lowongan	LWG1	A.16.1.3 Melaporkan kelemahan keamanan informasi	- Pegawai dan staff yang memakai sistem atau layananinformasi organisasidiwajibkan untuk memiliki list dan memberi laporan ketika kelemahan keamanan informasiada yang dirasa janggal. (A.16.1.3)
3.	Pihak yang tidak memiliki kewenangan dapat masukke sistem. – Data Pelamar	PEL1		
4.	Pihak yang tidak memiliki kewenangan dapat masuk ke sistem. – Data Lamaran	LMR1		
5.	Kehilangan data pada data SSO	SSO4	A.11.1.4 Melindungi dari ancaman eksternal& lingkungan A.12.3.1 Cadangan Informasi	- Harus dirancang dan ditnerapkan perlindungan fisik terhadap kecelakaan, serangan jahat, dan bencana alam. (A.11.1.4)
6.	Terjadi kerusakan data pada data lowongan.	LWG3		
7.	Terjadi kerusakan datapada data pelamar.	PEL3		
8.	Terjadi kerusakan datapada data lamaran.	LMR3		

				- Menurut kebijakan pencadangan yang ditetapkan, data *backup*, peragkat lunak, dan gambar sistem harus dibuat dan ditinjau secara berkala. (A.12.3.1)
9.	Pemalsuan pada data lowongan.	LWG4	A.18.1.4 Perlindungan informasi identitas pribadi & privasi	- Informasi pribadi harus dilindungi dan dijaga kerahasiaannya sesuai dengan setiap hukum dan aturan yang relevan.
10.	Pemalsuan pada data pelamar.	PEL4		
11.	Penyebaran hak akses pada data SSO.	SSO3	A.9.2.2 Penyediaan akses pengguna A.9.2.5 Tinjauan hak akses pengguna A.9.3.1 Penggunaan data otentikasi rahasia	- Harus ada proses terdokumentasi untuk memberikan atau mencabut hak akses untuk semua jenis pengguna ke semua sistem dan layanan. (A.9.2.2) - Pemilik aset harus secara berkala memeriksa hak akses pengguna. (A.9.2.5) - Pengguna harus mematuhi prosedur organisasi saat menggunakan data otentikasi rahasia. (A.9.3.1)

B. Perancangan Rekomendasi Mitigasi

Pada bagian ini akan dijelaskan bagaimana perancangan rekomendasi mitigasi yang bertujuan sebagai langkah mitigasi dalam menangani risiko yang sudah dianalisis menggunakan OCTAVE Allegro. Berikut penjelasan tentang rekomendasi mitigasi ISO 27001 dari risiko yang ada pada PT. XYZ.

TABEL 16
KONTROL 1 (PIHAK YANG TIDAK MEMILIKI KEWENANGAN DAPAT MASUK KE SISTEM)

- **Klausul A.10 *Cryptographic Controls***

Tujuan: Untuk memastikan bahwa kriptografi digunakan dengan benar dan berhasil untuk menjaga kerahasiaan, keaslian, dan integritas informasi

- **Sub Kontrol A.10.1.1 Kebijakan penggunaan kontrol kryptografi**

Kontrol: Pembuatan dan penerapan kebijakan kontrol kriptografi untuk perlindungan informasi harus diterapkan.

TABEL 17
KONTROL 2 (PIHAK YANG TIDAK MEMILIKI KEWENANGAN DAPAT MASUK KE SISTEM)

- **Klausul A.16.1 Manajemen insiden dan peningkatan keamanan informasi**

Tujuan: Untuk menyediakan strategi manajemen yang terorganisir dan efisien untuk masalah keamanan informasi, termasuk komunikasi tentang insiden dan kelemahan keamanan.

- **Sub Kontrol A.16.1.3 Melaporkan kelemahan keamanan informasi**

Kontrol: Pegawai dan staff yang memakai sistem atau layanan informasi organisasi diwajibkan untuk memiliki list dan memberi laporan ketika kelemahan keamanan informasi ada yang dirasa janggal.

1. Rekomendasi Mitigasi
   a. Pihak PT. XYZ menerapkan standar algoritma kriptografi yang sesuai dengan kebutuhan organisasi untuk memaksimalkan keamanan informasi yang sudah ada.
   b. Setiap pegawai harus peduli dan wajib mencatat jika ada cacat sistem, atau kelemahan pada sistem informas agar diambil langkah yang tepat dalam penanganannya

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil peneltitian pada aplikasi Recruitment SSO PT. XYZ dapat disimpulkan bahwa:

1. Pada aplikasi Recruitment SSO memiliki empat aset informasi kritis yaitu Data SSO Operation, Data Lowongan, Data Pelamar, dan Data Lamaran.
2. Dengan menggunakan OCTAVE Allegro didapatkan lima impact area yang menjadi indikator dalam melakukan penilaian risiko yaitu reputasi dan kepercayaan pelanggan, finansial, produktivitas, kesehatandan keselamatan, dan denda dan pinalti.
3. Dari empat aset informasi kritis, didapatkan risiko yang teridentifikasi sebanyak 15 risiko. Berdasarkan hasil analisis terdapat 8 risiko yang dimitigasi, 3 risiko yang ditangguhkan, dan 4 risiko yang diterima.
4. Rekomendasi kontrol pada penelitian ini mengacu pada standar internasional ISO 27001. Terdapat 8 subkontrol ISO 27001 yang menjadi acuan untuk langkah mitigasi.
5. Perancangan rekomendasi mitigasi dibuat berdasarkan hasil analisis risiko dan kontrol ISO 27001 yang digunakan. Terdapat 14 poin mitigasi yang diberikan pada penelitian ini.

B. Saran

Berikut saran yang diberikan oleh penulis dari penelitian yang sudah dilakukan:

1. Menerapkan rekomendasi kontrol dan mitigasi agar risiko dan segala ancaman dapat diminimalisir.
2. Untuk penelitian selanjutnya, hasil analisis dan penilaian risiko ini dapat menjadi acuan dimasa yangakan datang.
3. Untuk penelitian selanjutnya, dapat menambah metode lain yang berkaitan dengan analisis risiko untuk didapati hasil yang lebih komprehensif.

REFERENSI

[1] Bambang Supradono (2009), MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION), Media Elektrika, Vol. 2, No. 1, 2009 : 4 – 8.

[2] *International Standard* (2013), *Information technology — Security techniques — Information security management systems — Requirements*, ISO/IEC 27001:2013.

[3] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson (2007), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. SOFTWARE ENGINEERING INSTITUTE.*

[4] Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody (2005), *OCTAVE-S Implementation Guide, Version* 1.0, CMU/SEI-2003-HB-003 Volume 1.

[5] Firzah A Basyarahil, Hanim Maria Astuti, dan Bekti Cahyo Hidayanto (2017), Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya, JURNAL TEKNIK ITS Vol. 6, No. 1, (2017).

[6] Amir Samimi (2020), Risk Management in Information Technology, Progress in Chemical and Biochemical Research 2020, 3(2), page 130-134.

[7] Boris Kaehler & Jens Grundei (2018), HR Governance A Theoretical Introduction, Springer 2019.