# ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI PADA *WEBSITE* PMB PERGURUAN TINGGI XYZ MENGGUNAKAN METODE *OCTAVE ALLEGRO*

**Fairuz KhairaFaza[*1)], Muhamad Nasrullah [2)], Aris Kusumawati[3)]**
[1)]Sistem Informasi, Fakultas Teknologi dan Bisnis, Institut Teknologi Telkom Surabaya, Jl. Ketintang No.156, Ketintang, Kota Surabaya, 60231 , Indonesia
fairuzkhaira@student.ittelkom-sby.ac.id

***Abstrak***

*Teknologi informasi yang terus berkembang seiring dengan kebutuhan pada layanan dibidang akademik yang semakin tinggi. Perguruan Tinggi XYZ mengembangkan sistem yang membantu pelayanan bagi calon mahasiswa baru yakni website PMB. Website PMB merupakan salah satu layanan informasi yang paling penting bagi organisasi dalam hal proses pendaftaran mahasiswa baru, oleh karena itu perlu adanya manajemen risiko keamanan sistem informasi untuk dapat meminimalisir dampak dari risiko. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi atas risiko-risiko dalam penggunaan website PMB, dengan menggunakan metode OCTAVE Allegro untuk membantu memberikan penilaian terhadap aset informasi. Berdasarkan hasil penelitian, terdapat 9 risiko IT yang berhasil diidentifikasi. Beberapa risiko memiliki nilai tertinggi yaitu pada Serangan malware 43 dan terjadinya Brute Force nilai risiko 43. Hasil analisis menunjukkan bahwa dari 9 risiko tersebut, 4 risiko akan dilakukan mitigasi (Mitigate) , 4 risiko akan ditangguhkan (Defer), dan 1 diterima (Accept) karena tidak menimbulkan kerusakan yang sangat parah bagi perguruan tinggi XYZ.*

***Kata kunci:*** *Manajemen Risiko IT, Keamanan Sistem informasi, OCTAVE Allegro, Website PMB.*

## 1. Pendahuluan (Introduction)

Penerapan teknologi informasi terutama internet yang semakin pesat membawa perubahan diberbagai aspek kehidupan manusia dalam mencari dan mendapatkan suatu informasi yang tidak terbatas oleh ruang maupun waktu. Berdasarkan Internet world stats, Indonesia menempati urutan ketiga di Asia dengan jumlah pengguna internet yang mencapai 212,35 juta pada bulan Maret 2021 (Amirul dkk., 2022). Perguruan tinggi XYZ telah menerapkan teknologi informasi untuk menunjang dan mendukung aktifitas akademik. Salah satu penerapan teknologi informasi pada lembaga pendidikan tingkat XYZ tersebut adalah penggunaan *website*. *Website* merupakan salah satu layanan informasi yang dapat diakses oleh orang diseluruh dunia yang menyajikan informasi berupa teks, gambar, audio, maupun video (Kholifah dkk., 2021). Penggunaan *website* yang baik dan benar merupakan aspek yang sangat penting agar dapat diakses dengan tanpa adanya gangguan. *Website* akademik memudahkan civitas akademik untuk dapat mengakses informasi mengenai layanan akademik.Tetapi, dengan banyaknya jumlah pengunjung *website* akademik maka semakin banyak risiko ancaman bagi *website* (Guntoro dkk., 2020).

Peran *website* PMB XYZ sangat penting karena menjadi pusat informasi bagi calon mahasiswa seperti pembelian token atau pin pendaftaran, dan input data informasi pribadi calon mahasiswa. Semakin besar aset informasi yang tersimpan maka, semakin besar pula risiko yang akan terjadi. Apabila terdapat suatu risiko maka akan sangat membahayakan perguruan tinggi XYZ dalam keamanan sistem informasi *website* PMB XYZ. Dalam menangani risiko yang ada diperlukan manajemen risiko yang bertujuan sebagai upaya untuk mengantisipasi terjadinya risiko yang akan membahayakan perguruan tinggi XYZ. Akibat apabila risiko terjadi seperti kerugian besar pada organisasi, kehilangan kepercayaan, pencurian data, dan lain sebagainya. Hasil

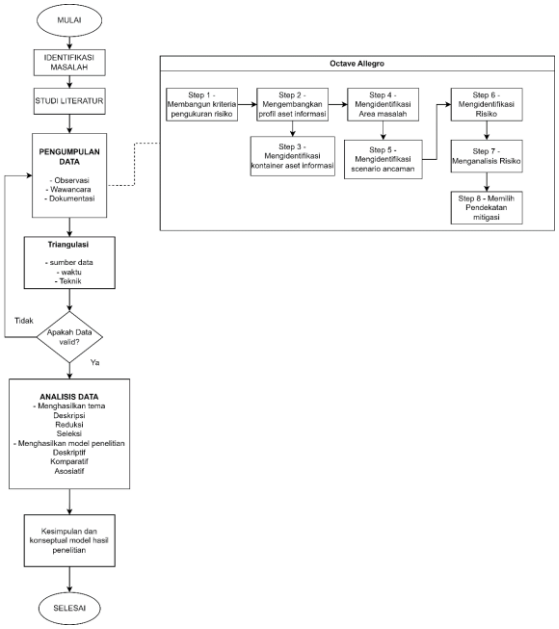
wawancara pendahuluan bersama informan selaku pengelolah website mengatakan bahwa "Pada *Website* PMB belum pernah dilakukannya penilaian risiko dan pernah terjadi *server down* sehingga beberapa menu tidak dapat berjalan dengan normal".

Berdasarkan latar belakang permasalahan tersebut perlu adanya sebuah evaluasi dan penilaian risiko untuk mengetahui risiko apa yang akan mengancam keamanan sistem informasi. Berdasarkan pembahasan sebelumnya, maka peneliti ingin melakukan identifikasi risiko ancaman dan melakukan evaluasi risiko untuk dapat mengetahui risiko yang akan mengancam keamanan sistem informasi. Pada penelitian ini menggunakan metode *OCTAVE Allegro* yang dimana metode ini difokuskan pada aset informasi yang kritis dimana melakukan analisis risiko dengan memperkenalkan konsep container aset informasi, metode ini dirancang untuk melakukan penilaian risiko tanpa melakukan penilaian yang luas (Pradana, 2013). Metode *OCTAVE Allegro* merupakan salah satu metode yang dirancang untuk mefokuskan dan merampingkan proses penilaian risiko keamanan informasi sehingga sebuah organisasi dapat memperoleh hasil yang cukup (St, Adhitya, 2020).

## 2. Metode Penelitian (Methods)

### A. Tahapan Penelitian

Dalam penyusunan penelitian ini menggunakan metode kualitatif studi kasus yang dimana penelitian ini dibatasi oleh waktu dan aktifitas tertentu (John W. Creswell, 2015). Teknik penggumpulan data dengan berdasarkan kerangka kerja *OCTAVE Allegro*, dengan data yang langsung didapatkan dari hasil wawancara langsung kepada informan yang bertujuan untuk dapat melakukan evaluasi risiko keamanan informasi pada *website* PMB perguruan tinggi XYZ. Gambar 1 merupakan tahapan penelitian.




**Gambar 1.** Alur Penelitian

#### 1) Identifikasi Masalah

Identifikasi masalah dilakukan dengan observasi secara langsung pada objek dan melakukan wawancara pendahuluan untuk dapat mengetaui permasalahan yang terjadi pada *website* PMB. Permasalahan yang terjadi pada *website* PMB yaitu belum dilakukannya penilaian atau evaluasi risiko keamanan informasi pada *website* PMB.

**2) Studi Literatur**

Studi literatur dilakukan dengan membaca jurnal, website, buku dan lain sebagainya sebagai penunjang informasi penelitian ini. Yang dimana studi literatur digunakan agar dapat memperkuat teori mengenai *OCTAVE Allegro* dan studi kasus yang berkaitan dengan penelitian.

**3) Pengumpulan Data**

Pengumpulan data dilakukan dengan melakukan Observasi, Wawancara dan Dokumentasi. Pengumpulan data disini dilakukan secara langsung kepada informan yang telah ditetapkan berdasarkan pada struktur organisasi dan Tupoksi masing-masing dari divisi.

**4) Triangulasi**

Setelah mendapatkan dan mengumpulkan data yang dibutuhkan kemudian dilakukan proses keabsahan data atau triangulasi. Tringulasi dilakukan agar dapat membuat data yang telah didapatkan menjadi valid, triangulasi dilakukan dengan teknik yang berbeda-beda. Teknik triangulasi yang digunakan yaitu Triangulasi Teknik, Sumber dan Waktu (Dr. H. Zuchri Abdussamad, S.I.K., 2021).

**5) Analisis Data**

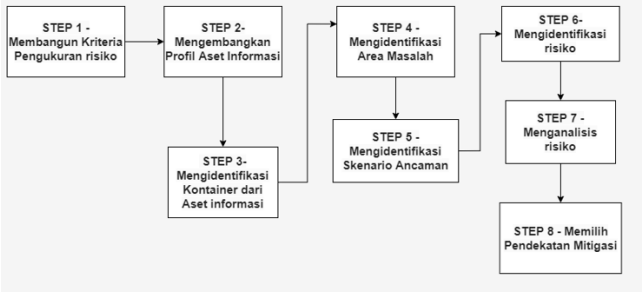
Teknik analisis data merupakan sebuah proses penyusunan data-data yang telah didapatkan dari hasil wawanacara, observasi, dan dokumentasi dengan cara melakukan kategorisasi, sehingga dapat menjadikan tema atau pola yang akan dijadikan kesimpulan penelitian agar dapat memudahdahkan peneliti maupun pembaca memahami (Soegiyono, 2011). Dalam penelitian ini dilakukan analisis hingga titik maksimal atau tidak ada data jenuh yang didapatkan dari hasil wawancara.

6) **Kesimpulan**

Kesimpulan merupakan tahap terakhir yaitu hasil dari penelitian dan jawaban atas rumusan masalah yang sudah ditetapkan pada awal penelitian.

## *B. OCTAVE Allegro*

Metode penelitian penilaian risiko menggunakan *OCTAVE Allegro*. *OCTAVE Allegro* merupakan sebuah kerangka kerja yang didesain untuk melakukan penilaian risiko yang difokuskan pada aset informasi yang bertujuan untuk menghasilkan hasil penilaian yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko (Caralli *dkk.*, 2007). Terdapat 8 tahapan dari *OCTAVE Allegro* yaitu :




**Gambar 1. Tahapan *OCTAVE Allegro***

- **Membangun Kriteria Pengukuran Risiko**

  Pada langkah pertama *OCTAVE Allegro* yaitu penetapan kriteria pengukuran risiko yang dapat digunakan untuk melakukan analisis tisiko terhadap tujuan bisnis dari Perguruan Tinggi XYZ. Pada tahap ini terdapat dua aktifitas, yaitu menentukan area dampak dan melakukan penentuan penilaian prioritas area dampak. Keluaran

dari hasil ini yaitu akan mendapatkan skala prioritas area dampak yang paling pentinng dan yang paling tidak penting. (Keating, 2014).

- **Mengembangkan Profil Aset Informasi**

  Pada tahap ini, mengenai perkembangan aset profil dengan mengidentifikasi aset informasi yang penting pada *website* PMB perguruan tinggi XYZ. Dan pada tahap ini akan menghasilkan profil aset informasi yang kritis atau yang paling diutamakan pada *website* PMB perguruan tinggi XYZ (Mauluddani *et al.*, 2021) .

- **Identifikasi Kontainer aset informasi**

  Pada tahap ini, mengidentifikasi semua kontainer asset informasi, kontainer disini diartikan sebagai tempat atau wadah dimana asset informasi itu disimpan, diproses dan dikirim baik dari sisi internal maupun eksternal. Kategori container berbeda beda yaitu Teknikal, Fisikal, dan Orang (Nelmiawati dkk., 2017).

- **Mengidentifikasi Area yang Diperhatikan**

  Tahap selanjutnya setelah melakukan identifikasi kontainer asset informasi yaitu dengan melakukan identifikasi *area of concern* atau area yang diperhatikan. Area yang diperhatikan yaitu dimana peneliti memberikan pemaparan mengenai risiko atau ancaman yang berdampak pada asset informasi tersebut (Kholifah dkk., 2021).

- **Identifikasi Skenario Ancaman**

  Pada tahap ini, melakukan pendokumentasian untuk dapat mengidentifikasi skenario ancaman yang terjadi. Setelah mendapatkan area yang diperhatikan kemudian pada area yang diperhatikan tersebut diperluas lagi untuk membuat *Threat Properties* agar dapat memperjelas ancaman (Armadyana dkk., 2023).

- **Identifikasi Risiko**

  Pada tahap ini, peneliti menganalisis data yang sudah dikumpulkan dan Hasilnya akan berupa konsekuensi dari skenario ancaman (kondisi) lalu risiko total ancaman kondisi dan konsekuensi tiap risiko yang telah terindentifikasi (Hasibuan, 2019)

- **Analisis Risiko**

  Pada tahap ini, peneliti melakukan perhitungan skor risiko relative untuk setiap risiko asset informasi. *Relative Risk Score* ini ditentukan dengan mempertimbangkan konsekuensi yang akan berdampak pada perguruan tinggi XYZ. *Relative Risk Score* akan dihitung untuk dapat digunakan dalam menganalisis risiko untuk menentukan risiko yang akan dimitigasi (St, Adhitya., 2020). *Relative Risk Score* (rs) didapatkan dari nilai *Impact area* (i) dikalikan dengan nilai dampak (d) (Tinggi, Sedang, Rendah) yang dapat dilihat pada persamaan 1.

$$rs = i * d \quad (1)$$

- **Pendekatan Mitigasi**

  Pada tahap ini, dimana risiko ancaman yang telah diidentifikasi lalu kemudian dilakukan pendekatan mitigasi untuk mengurangi risiko penting hal ini bertujuan agar dapat dengan mudah melakukan pengambilan keputusan status mitigasi (Hendarti, 2020) .

## 3. Hasil dan Pembahasan (Results and Discussions)

Data yang telah didapatkan melalui tahap Wawancara, Observasi dan pengumpulan Dokumentasi kemudian akan dilakukan untuk proses analisis. Analisis tersebut berlandaskan pada 8 tahapan metode *OCTAVE Allegro*.

### a. Membangun Kriteria Pengukuran Risiko

Pada tahap pertama yang dilakukan yaitu membangun kriteria pengukuran risiko pada tahap ini terdiri dari dua aktifitas yaitu aktifitas pertama yaitu penentuan Impact Area. Bertujuan untuk dapat mengevaluasi dampak risiko berdasarkan tujuan bisnis Perguruan Tinggi XYZ. Kriteria pengukuran risiko ditentukan pada area yang memungkinkan terkenda dampak.

**Tabel 1.** Kriteria Pengukuran Risiko – Reputasi dan Kepercayaan Pengguna

| **Lembar kerja Allegro 1** | **Kriteria Penilaian Risiko – Reputasi dan Kepercayaan Pengguna** | | |
|---|---|---|---|
| **Area Terdampak** | **Rendah** | **Sedang** | **Tinggi** |
| **Penurunan Reputasi *Website* PMB** | Reputasi *website* PMB akan sedikit terpengaruh dan sedikit usaha penanganan perbaikan sistem. | Reputasi *website* PMB akan berpengaruh sedang dan dengan usaha perbaikan yang membutuhkan waktu dan biaya yang tidak sedikit. | Reputasi *website* PMB rusak dan usaha perbaikan dilakukan lebih lama dan membutuhkan biaya yang tinggi. |
| **Penurunan Reputasi Perguruan Tinggi XYZ** | Tidak ada dampak dan dapat dilakukan perbaikan secara internal pada saat terjadinya ancaman | Memberikan dampak negatif citra kepada publik | Reputasi perguruan tinggi rusak karena terjadi ancaman pada *website* PMB |
| **Kepercayaan Calon Mahasiswa Baru** | Kepercayaan calon mahasiswa baru tidak berpengaruh jika terjadi kerusakan atau ancaman terhadap *website* PMB. | Kepercayaan calon mahasiswa baru berpengaruh sedang jika terjadi kerusakan atau ancaman terhadap *website* PMB. | Hilangnya seluruh kepercayaan calon mahasiswa baru jika terjadi kerusakan pada data di *website* PMB. |

Pada aktivitas selanjutnya dilakukan penetuan skala prioritas. Area dampak yang lebih penting atau area dampak yang paling berdampak pada proses bisnis organisasi memiliki nilai prioritas tertinggi dan area yang paling tidak berpengaruh memiliki prioritas terendah. Berdasarkan wawancara dengan informan maka skala prioritas area dampak yang paling tinggi yaitu pada area produktifitas dan area yang paling tidak penting berada pada area denda dan pinalti.

**Tabel 2** Prioritas Area Dampak

| **Lembar kerja *OCTAVE Allegro* 7** | **Lembar Kerja Prioritas Area Dampak** |
|---|---|
| **Prioritas** | **Area Dampak** |
| 5 | Produktifitas |
| 4 | Reputasi dan Kepercayaan Calon Mahasiswa Baru |
| 3 | Keamanan |
| 2 | Keuangan |
| 1 | Denda dan Penalty |

**b. Mengembangkan Profil Aset Informasi**

Pada tahap kedua dilakukan dokumentasi profil aset informasi yang kritis. Profil aset informasi kritis didokumentasikan melalui *Critical Information Asset Profile Worksheet*.

**Tabel 3.** Profil Aset Informasi

| Allegro Worksheet 8 | Profil Aset Kritis | |
|---|---|---|
| (1)Aset Kritis<br>Aset informasi apa yang kritis? | (2) Alasan untuk seleksi<br>Mengapa asset informasi ini penting? | (3) Deskripsi<br>Deskripsi asset informasi ini? |
| Data calon mahasiswa baru | Karena berisikan data atau informasi penting mengenai identitas pribadi calon mahasiswa baru yang dapat mendukung aktivitas dalam pendaftaran masuk perguruan tinggi XYZ. | Data pribadi calon mahasiswa baru yang berisikan No telepon, alamat, Foto dan nomor KTP, nama orang tua, nomor telepon orang tua. |
| (4) Pemilik<br>Siapa yang memiliki aset informasi ini? | | |
| Pusat Teknologi dan Informasi<br>Admisi dan Marketing | | |
| (5) Persyaratan Keamanan<br>Apa persyaratan keamanan untuk asset informasi ini? | | |
| Kerahasiaan | Memastikan bahwa hanya orang yang berwenang dapat mengontrol dan mengakses asset informasi | Data hanya dapat diakses oleh staff pusat teknologi informasi, staff admisi dan Marketing serta calon mahasiswa baru |
| Integritas | Memastikan hanya orang tertentu yang mengubah asset informasi ini | Informasi hanya dapat diubah oleh pihak Pusat Teknologi informasi bagian urusan aplikasi, Staff Admisi dan marketing dan calon mahasiswa baru. |
| Ketersediaan | Memastikan bahwa informasi ini harus tersedia dan dapat terus diakses 24 jam. | Data atau informasi ini harus selalu tersedia selama 24 jam setiap hari oleh pihak yang memiliki kewenangan. |
| (6) Persyaratan keamanan yang paling penting?<br>Apa persyaratan keamanan terpenting untuk asset informasi ini? | | |
| [v] kerahasiaan | [v] Integritas | Ketersediaan |

**c. Mengidentifikasi Kontainer Aset Informasi**

Pada langkah ketiga yaitu dengan melakukan identifikasi kontainer aset informasi ini, yang dimana kontainer disini merupakan wadah dimana aset informasi disimpan, dibagikan dan diolah baik internal atau eksternal. Terdapat tiga jenis pada identifikasi container aset informasi yaitu Teknikal, Fisikal dan Orang.

**Tabel 4.** Teknikal

| **Lembar Kerja Allegro 9a** | **Peta Lingkungan Risiko Aset Informasi (Teknikal)** |
|---|---|
| | **Internal** |
| **Wadah** | **Pemilik** |
| Database | Pusat Teknologi Dan Informasi |
| *Website* | Pusat Teknologi Dan Informasi<br>Admisi dan Marketing |
| Perangkat keras: Komputer | Admisi dan Marketing |
| | **Eksternal** |
| Server | *Cloud AWS* |

**Tabel 5.** Fisikal

| Lembar Kerja Allegro 9a | Peta Lingkungan Risiko Aset Informasi (Fisikal) |
|---|---|
| | **Internal** |
| **Wadah** | **Pemilik** |
| Backup database calon mahasiswa baru pertahun ajaran baru | Pusat Teknologi Informasi |
| Backup data calon mahasiswa baru harian | Admisi dan Marketing |

**Tabel 6.** Orang

| Lembar Kerja Allegro 9a | Peta Lingkungan Risiko Aset Informasi (Orang) |
|---|---|
| | **Internal** |
| **Nama / tanggung jawab** | **Pemilik** |
| Staff Admisi dan Marketing | Admisi dan Marketing |
| Kepala bagian Pusat Teknologi Informasi | Pusat Teknologi dan Informasi |
| Kepala Urusan Aplikasi | Pusat Teknologi dan Informasi |
| | **Eksternal** |
| Calon Mahasiswa Baru | Calon Mahasiswa Baru |

**d. Mengidentifikasi Area yang diperhatikan**

Tahapan keempat yaitu setelah mengidentifikasi container dari aset informasi selanjutnya melakukan identifikasi area yang diperhatikan. Area yang diperhatikan yaitu penjelasan mengenai risiko yang berdampak pada aset informasi.

**Tabel 7.** Area yang diperhatikan

| No. | Area yang diperhatikan – Data calon mahasiswa baru |
|---|---|
| 1. | Terjadinya *server down* menyebabkan beberapa layanan tidak dapat diakses |
| 2. | Terjadi serangan *Malware* pada server cloud |
| 3. | Kesalahan dalam melakukan input data calon mahasiswa baru (*human eror*) |
| 4. | Informasi mengenai jurusan kelulusan tidak valid dengan pilihan calon mahasiswa baru (*Human Error*) |
| 5. | *Website* PMB mengalami *error* (*Network flailure*) |
| 6. | Kebocoran data calon mahasiswa baru |
| 7. | Pencurian data calon mahasiswa baru |
| 8. | Terjadinya serangan *Brute Force* pada login super admin |
| 9. | Adanya Bug pada sistem saat PUTI melakukan pengembangan dan pemeliharaan *(software failure)* |

**e. Mengidentifikasi Skenario Ancaman**

Tahap ini area yang diperhatikan akan diperluas menjadi skenario ancaman yang lebih detail lagi mengenai threat properties. Terdapat *threat properties* yang digunakan untuk melakukan identifikasi skenario ancaman yaitu *Actor, Means, Motive, Output, Security Requirement, Probability.*

**Tabel 8.** Skenario Ancaman

| No. | Area yang diperhatikan | Skenario Ancaman | |
|---|---|---|---|
| 1 | Terjadinya *Brute Force* pada login Super admin Admisi | *Actor* | Hacker |
| | | *Means* | Menebak- nebak kata sandi dengan melakukan login terus menerus password |

| No. | Area yang diperhatikan | Skenario Ancaman | |
|---|---|---|---|
| | | | dan username yang telah disesuaikan pada organisasi |
| | | *Motive* | Sengaja |
| | | *Outcome* | *Disclosure*<br><br>*Modification*<br><br>*Interruption* |
| | | *Security Requirement* | Diberikan pengaman berupa captcha pada halaman login super admin, diberikan batasan login |
| | | *Probability* | Sedang |

**f. Mengidentifikasi Risiko**

Pada tahap ini dilakukan identifikasi risiko dengan melakukan penjabaran penjelasan segala bentuk konsekuensi yang akan terjadi atau yang akan terjadi jika scenario ancaman yang telah diidentifikasi sebelumnya terjadi, bagaimana konsekuensi bagi perguruan tinggi XYZ.

**Tabel 9.** Identifikasi Risiko Ancaman

| Risiko | Konsekuensi |
|---|---|
| Terjadinya *Server Down* pada *website* PMB | - Terhambatnya proses calon mahasiswa baru melakukan pendaftaran dan terhambatnya proses pengelolaan data calon mahasiswa baru.<br>- *Website* tidak dapat diakses<br>- Turunnya reputasi dan kepercayaan calon mahasiswa baru<br>- Kehilangan kesempatan untuk memperoleh calon mahasiswa baru<br>- Meningkatnya keluhan dari calon mahasiswa baru |
| Terjadi serangan *Malware* pada server cloud | - Sistem tidak bisa diakses<br>- Proses pengelolaan data penerimaan calon mahasiswa baru terhambat<br>- Pencurian data dan informasi calon mahasiswa baru<br>- Kerusakan data calon mahasiswa baru |
| Kesalahan dalam melakukan input data calon mahasiswa baru (*human error*) | - Menghambat produktifitas pekerjaan Divisi Pusat Teknologi Informasi dan Admisi Marketing<br>- Meningkatnya keluhan calon mahasiswa baru |
| Informasi mengenai jurusan kelulusan tidak valid dengan pilihan calon mahasiswa baru (*Human Error*) | - Menurunnya kepercayaan calon mahasiswa baru<br>- Ketidakvalidan data kelulusan calon mahasiswa baru<br>- Meningkatnya keluhan dari calon mahasiswa baru |

**g. Menganalisis Risiko**

Analisis data dilakukan bertujuan untuk dapat menentukan *Threat Scenario* yang memberikan dampak bagi perguruan tinggi XYZ dan menentukan Probabilitasnya apakah Tinggi, Sedang dan Rendah. Kemudian *Relative Risk Score* dihitung untuk melakukan analisis risiko yang akan digunakan untuk membantu perguruan tinggi XYZ untuk menentukan strategi mitigasi risiko yang tepat. *Relative Risk Score* didapatkan dari persamaan 1 dengan mempertimbangkan tabel 10.

**Tabel 10**. Nilai Impact Area

| Area Dampak | Prioritas | Rendah (1) | Sedang (2) | Tinggi (3) |
|---|---|---|---|---|
| Produktifitas | 5 | **5** | **10** | **15** |
| Reputasi dan Kepercayaan calon mahasiswa baru | 4 | **4** | **8** | **12** |
| Keamanan | 3 | **3** | **6** | **9** |
| Keuangan | 2 | **2** | **4** | **6** |
| Denda dan Penalty | 1 | **1** | **2** | **3** |

**Tabel 11.** Analisis Risiko

| Area Of Concern | Information Asset Risk Worksheet | | | |
|---|---|---|---|---|
| Terjadi serangan *Malware* pada server cloud | Aset Informasi | Data Calon mahasiswa baru | | |
| | Konsekuensi | - Sistem tidak bisa diakses<br>- Proses pengelolaan data penerimaan calon mahasiswa baru terhambat<br>- Pencurian data dan informasi calon mahasiswa baru<br>- Kerusakan data calon mahasiswa baru | | |
| | Severity | **Area Terdampak** | **Nilai** | **Score** |
| | | Produktifitas | Tinggi | 15 |
| | | Reputasi dan Kepercayaan calon mahasiswa baru | Tinggi | 12 |
| | | Keamanan | Tinggi | 9 |
| | | Keuangan | Tinggi | 6 |
| | | Denda dan Hukum | Rendah | 1 |
| | | **Relative Risk Score** | | **43** |

**h. Memilih Pendekatan Mitigasi**

Pada tahap ini merupakan langkah terakhir dari tahapan *OCTAVE Allegro* dimana setiap risiko yang telah teridentifikasi dan memprioritaskan risiko lalu setelah itu dilakukan pendekatan mitigasi untuk dapat mengurangi risiko kritis. Dalam *OCTAVE Allegro* pendekatan mitigasi mempunyai tiga pilihan *Mitigate, Defer, Accept*. Aktifitas pertama yaitu penempatan POOL pada setiap area yang diperhatikan yang telah dianalisis dan memiliki skor risiko relative. Penempatan POOL menjadi sebuah acuan risiko yang dimitigasi (Zulfia dkk.,2021).

**Tabel 12.** Relative Risk Matrix

| *Relative Risk Matrix* | | | |
|---|---|---|---|
| Probabilitas | *Relative Risk Score (Impact)* | | |
| | 30 To 45 | 16 to 29 | 0 to 15 |
| Tinggi | POOL 1 | POOL 2 | POOL 2 |
| Sedang | POOL 2 | POOL 2 | POOL 3 |
| Rendah | POOL 3 | POOL 3 | POOL 4 |

Aktifitas kedua yaitu menetapkan pendekatan mitigasi berdasarkan dengan pemilihan POOL. Tabel 13 merupakan pendekatan mitigasi pada metode *OCTAVE Allegro* (Wini dkk., 2023).

**Tabel 13.** Pendekatan Mitigasi

| POOL | Pendekatan Mitigasi |
|---|---|
| Pool 1 | *Mitigate* |
| Pool 2 | *Mitigate or defer* |
| Pool 3 | *Defer or Accept* |
| Pool 4 | *Accept* |

Aktifitas terakhir yaitu memilih pendekatan mitigasi. Tabel 14 merupakan pemilihan pendekatan mitigasi yang dipilih pada setiap risiko yang telah diidentifikasi.

**Tabel 14.** Pemilihan Mitigasi

| Area yang diperhatikan | Probabilitas | *Relative Risk Score* | POOL | Pendekatan Mitigasi |
|---|---|---|---|---|
| Terjadinya *server down* menyebabkan beberapa layanan tidak dapat diakses | **Rendah** | **37** | **POOL 3** | ***DEFER*** |
| Terjadi serangan *Malware* pada server cloud | **Sedang** | **43** | **POOL 2** | ***MITIGATE*** |
| Kesalahan dalam melakukan input data calon mahasiswa baru (*human eror*) | **Tinggi** | **31** | **POOL 1** | ***MITIGATE*** |
| Informasi mengenai jurusan kelulusan tidak valid dengan pilihan calon mahasiswa baru (*Human Error*) | **Rendah** | **40** | **POOL 3** | ***ACCEPT*** |
| *Website* PMB mengalami error (*Network failure*) | **Rendah** | **35** | **POOL 3** | ***DEFER*** |
| Pencurian data calon mahasiswa baru | **Rendah** | **36** | **POOL 3** | ***DEFER*** |
| Kebocoran data calon mahasiswa baru | **Rendah** | **36** | **POOL 3** | ***DEFER*** |
| Adanya Bug baru pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan *(software failure)* | **Tinggi** | **41** | **POOL 2** | ***MITIGATE*** |
| Adanya serangan *Brute Force* pada halaman login super admin | **Sedang** | **43** | **POOL 2** | ***MITIGATE*** |

**i. Rekomendasi Mitigasi Risiko**

Dari proses penilaian keseluruhan, maka hasil temuan risiko yang telah didapatkan akan diberikan rekomendasi untuk dilakukan perbaikan untuk kedepannya agar dapat mengelolah, mengurasi dampak risiko yang akan ditimbulkan. Berikut rekomendasi yang diberikan rekomendasi perbaikan yang memiliki pendekatan Mitigate atau yang harus segera dilakukan penanganan.

**Tabel 15.** Rekomendasi Mitigasi Risiko

| Area yang diperhatikan | Probabilitas | Pendekatan Mitigasi | Rekomendasi Perbaikan |
|---|---|---|---|
| Terjadi serangan *Malware* pada server cloud | **Sedang** | ***MITIGATE*** | - Melakukan Scanning setiap 6 bulan sekali<br>- Melakukan backup data setiap tahun ajaran baru agar jika terjadi serangan malware data yang telah dibackup tidak hilang atau tidak rusak<br>- Menggunakan *Firewall Fortinet, Firewall Fortinet* adalah salah satu firewall terdepan yang digunakan oleh banyak organisasi besar dan mempunyai keunggulan Keamanan yang terintegritas, Skalabilitas, Manajemen jaringan yang mudah, Proteksi multi-layer yaitu memberikan proteksi lapisan *cloud* yang aman. |
| Kesalahan dalam melakukan input data calon mahasiswa baru (*human error*) | **Tinggi** | ***MITIGATE*** | - Melakukan validasi kembali terhadap data yang telah diinputkan<br>- Adanya pelatihan kepada staff Admisi terkait aplikasi yang diberikan oleh Pusat Teknologi informasi agar dapat mengubah data yang salah |
| Adanya serangan *Brute Force* pada halaman login super admin admisi | **Sedang** | ***MITIGATE*** | - Memberikan pengaman berupa *Captcha* pada laman login super admin untuk memastikan bahwa yang melakukan login merupakan pengguna yang berwenang dan bukan oleh computer yang telah dirancang oleh hacker untuk membobol sistem<br>- Menggunakan *Two Factor Authentication* (2FA), diperlukan outentifikasi dua kali agar dapat melakukan login pada akun yaitu dengan penggunaan password dan kode khusus<br>- Mengatur limit login, yaitu dengan membatasi seberapa banyak percobaan login yang dapat dilakukan<br>- Pengelolaan password terhadap sistem harus dikelola dengan baik. |
| Adanya Bug baru pada sistem saat pihak IT melakukan pengembangan dan pemeliharaan *(software failure)* | **Tinggi** | ***MITIGATE*** | - Melakukan *User Acceptance Testing* (UAT) bersama dengan Admisi untuk melakukan testing bersama agar dapat mendeteksi bug atau error yang terjadi dan dapat dilakukan perbaikan kembali<br>- Perubahan pada proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan. |

### 3.2. Kesimpulan (Conclusion)

Dari hasil analisis teridentifikasi risiko pada Website PMB Perguruan Tinggi XYZ sebanyak 9 risiko IT yaitu, *Server Down*, Terjadi serangan *Malware* pada *server cloud*, Kesalahan dalam melakukan input data calon mahasiswa baru (*human error*), Informasi mengenai jurusan kelulusan tidak valid dengan pilihan calon mahasiswa baru, *Website* PMB mengalami *error (Network flailure*), Terjadinya serangan *Brute Force* pada halaman login super admin , Pencurian data calon mahasiswa baru secara sengaja, Kebocoran data calon mahasiswa baru, Adanya *Bug* pada sistem saat PUTI melakukan pengembangan dan pemeliharaan (*software failure*). Hasil dari analisis dari skor risiko relatif terdapat 4 Risiko yang akan dilakukan mitigasi *(Mitigate)* dan 4 risiko yang ditangguhkan *(Defer*) risiko yang ditangguhkan akan dilakukan analisis dan evaluasi kembali mengenai risiko tersebut. 1 risiko yang diterima (*Accept*) karena tidak berpengaruh ke kriteria risiko perguruan tinggi.

Didapatkan 4 rekomendasi perbaikan dan upaya mitigasi untuk mengatasi risiko. Risiko yang diberikan rekomendasi adalah 4 risiko yang memiliki pendekatan mitigasi Mitigate sehingga dapat dijadikan rekomendasi untuk dilakukan penanganan yang lebih utama.

**Ucapan Terima Kasih (Acknowledgement)**

Terima kasih kepada seluruh pihak yang telah membantu penelitian ini berjalan dengan lancar yaitu kepada Perguruan Tinggi XYZ yang telah memberikan izin menjadikan *Website* PMB perguruan tinggi XYZ sebagai objek penelitian. Dan terima kasih kepada informan yang telah membantu dalam proses wawancara pada penelitian ini yaitu kepada Kepala bagian Pusat Teknologi Informasi, kepala Urusan layanan Pusat Teknologi Informasi dan Kepala bagian Admisi dan Marketing yang telah bersedia menjadi informan pada penelitian ini.

**Daftar Pustaka**

Amirul, M., Fadlil, A. and Riadi, I. (2022) ‘Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework’, *Jurnal Media Informatika Budidarma*, 6, pp. 1468–1475. Available at: https://doi.org/10.30865/mib.v6i3.4099.

Armadyana, R., Yasirandi, R. and Makky, M. Al (2023) ‘Analisis dan Penilaian Risiko Keamanan Informasi Menggunakan OCTAVE Allegro ( Studi Kasus : PT . XYZ )’, 10(3), pp. 3690–3703.

Caralli, R. a R. a. C. *et al.* (2007) ‘Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process’, *Young*, (May), pp. 1–113.

Dr. H. Zuchri Abdussamad, S.I.K., M.S. (2021) *Metode Penelitian Kualitatif*. Edited by M.S. Dr. Patta Rapanna, SE. CV. syakir Media Press.

Guntoro, G., Costaner, L. and Musfawati, M. (2020) ‘Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)’, *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 5(1), p. 45. Available at: https://doi.org/10.29100/jipi.v5i1.1565.

Hasibuan, S.I. (2019) ‘analisis risiko keamanan informasi dengan metode OCTAVE Allegro pada PT. Tirta investama’, *e-Proceeding of Engineering*, 6(2), pp. 7899–7907.

Hendarti, H. (2020) ‘Pengukuran Manajemen Risiko teknologi informasi dengan menggunakan

metode Octave Allegro', *e-Proceeding of Engineering*, 2(9), pp. 917–924.

John W. Creswell (2015) *Research Design Pendekatan Kualitatif , Kuantitatif dan Mixed*. edisi keti. Edited by Saifuddin Zuhri Qudsy. Yayasan Mitra Netra.

Keating, C.G. (2014) *Validating the Octave Allegro Information Systems Risk Assessment Methodology: A Case Study*. Nova Southeastern University.

Kholifah, K., Putra, R.A. and Nopriani, F. (2021) 'Analisis Penilaian Risiko Terhadap Penggunaan Sistem Informasi Akademik Pada Universitas Muhammadiyah Palembang Menggunakan Metode Octave Allegro', *Journal of Computer and Information Systems Ampera*, 2(1), pp. 28–42. Available at: https://doi.org/10.51519/journalcisa.v2i1.58.

Mauluddani, D.N. *et al.* (2021) 'Manajemen Rumah Sakit Modul Aset Menggunakan Metode Octave Allegro ( Studi Kasus : Rumah Sakit Khusus Ibu Dan Anak Bandung ) Risk Analysis and Information Security Control Design in Hospital Management Information System Asset Module Using Octave Allegro', *e-Proceeding of Engineering*, 8(2), pp. 2695–2708.

Nelmiawati, N., Destrianto, F.R. and Sitorus, M.A.R. (2017) 'Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE', *e-Proceeding of Engineering*, 9(1), p. 35. Available at: https://doi.org/10.30871/ji.v9i1.284.

Pradana, R.F.W. (2013) 'Penjualan PT Matahari department store cabang jogja city mall menggunakan metode OCTAVE Allegro', *e-Proceeding of Engineering*, 3(6).

Soegiyono (2011) *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Edited by Sutopo. ALFABETA.

St, R.F., Adhitya, R. and St, N. (2020) 'Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Pada Dinas Komunikasi Dan Informatika', *e-Proceeding of Engineering*, 7(2), pp. 7003–7008.

Wini Astuti, R., Putra, R.A. and Putra, I.S. (2023) 'Penilaian Risiko Penggunaan Sistem Informasi Akademik Pada STIQ Al-Lathifiyyah Palembang Dengan Metode Octave Allegro', *Journal of Computer and Information Systems Ampera*, 4(1), pp. 44–54. Available at: https://doi.org/10.51519/journalcisa.v4i1.337.

Zulfia, A., Ruskan, E.L. and Putra, P. (2021) 'Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya', *JOINS (Journal of Information System)*, 6(1), pp. 40–47. Available at: https://doi.org/10.33633/joins.v6i1.4088.