

**Manajemen Risiko Sistem Informasi Akademik pada Universitas Pembangunan Nasional Veteran Jakarta Menggunakan Metode Octave Allegro**

Diselesaikan Untuk Memenuhi Tugas Mata Kuliah Manajemen Risiko Teknologi Informasi

Oleh

Muhammad Rio Pratama 1810512002

Khusnul Khotimah 1810512031

Ahmad Ghani Fadillah 1810512072

Allvira Arianti Amir Hamzah 1810512078

Dosen Pengampu

Kraugusteeliana, M.Kom., M.M.

**PROGRAM SARJANA SISTEM INFORMASI**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**2021**

# **KATA PENGANTAR**

Segala puji dan syukur kami panjatkan atas kehadirat Allah SWT, karena berkat rahmat dan hidayah-Nya, kami dapat menyelesaikan tugas penilaian risiko pada Mata Kuliah Manajemen Risiko Teknologi Informasi dengan tepat waktu.

Penilaian risiko yang berjudul “Manajemen Risiko Sistem Informasi Akademik pada Universitas Pembangunan Nasional Veteran Jakarta Menggunakan Metode Octave Allegro” dapat diselesaikan karena bantuan dari banyak pihak. Kami berharap penilaian risiko tentang Sistem Informasi Akademik ini dapat menjadi referensi dan menambah wawasan baru bagi para pembaca.

Penulis menyadari bahwa makalah bertema penilaian risiko ini memerlukan penyempurnaan, terutama pada bagian pembahasan. Kami menerima segala bentuk kritik dan saran yang bersifat membangun untuk penyempurnaan makalah dan untuk langkah selanjutya.

Demikian yang dapat kami sampaikan, semoga makalah ini dapat bermanfaat bagi pembaca untuk melakukan penelitian selanjutnya. Terima Kasih.

Jakarta, 5 April 2021

Penulis

# **DAFTAR ISI**

[**KATA PENGANTAR** ii](#_Toc68766189)

[**DAFTAR ISI** iii](#_Toc68766190)

[**BAB I** 1](#_Toc68766191)

[**PENDAHULUAN** 1](#_Toc68766192)

[**1.1 Pendahuluan** 1](#_Toc68766193)

[**1.2 Rumusan Masalah** 2](#_Toc68766194)

[**1.3 Batasan Masalah** 2](#_Toc68766195)

[**1.4 Tujuan Penilaian Risiko** 2](#_Toc68766196)

[**1.5 Manfaat Penilaian Risiko** 3](#_Toc68766197)

[**BAB II** 4](#_Toc68766198)

[**LANDASAN TEORI** 4](#_Toc68766199)

[**2.1 Keamanan Sistem Informasi** 4](#_Toc68766200)

[**2.2. Ancaman Keamanan Sistem Informasi** 4](#_Toc68766201)

[**2.3 Manajemen Risiko dan Penilaian Risiko** 4](#_Toc68766202)

[**2.4 Metode Octave** 5](#_Toc68766203)

[Gambar I. Langkah-langkah Metode Octave Allegro. 6](#_Toc68766204)

[**BAB III** 7](#_Toc68766205)

[**TAHAPAN PENILAIAN RISIKO** 7](#_Toc68766206)

[**BAB IV** 9](#_Toc68766207)

[**PEMBAHASAN** 9](#_Toc68766208)

[Tabel I. *Impact Area* dan Reputasi Kepercayaan Pelanggan. 9](#_Toc68766209)

[Tabel II. Skala Prioritas *Impact Area*. 10](#_Toc68766210)

[Tabel III. Informasi Asset *Profilling* dan Transaksi Nilai Mahasiswa. 10](#_Toc68766211)

[Tabel IV. Informasi Asset *Risk Environtment (Technical)* dan Transaksi Nilai Mahasiswa. 11](#_Toc68766212)

[Tabel V. Area Concern dan Transaksi Nilai Mahasiswa. 12](#_Toc68766213)

[Tabel VI. Properties of Threat dan Transaksi Nilai Mahasiswa. 12](#_Toc68766214)

[Tabel VII. Cara Menghitung *Relative Score.* 14](#_Toc68766215)

[Tabel VIII. Analisis Risiko dan Transaksi Nilai Mahasiswa. 15](#_Toc68766216)

[Tabel IX. Relative Risk Matrix. 15](#_Toc68766217)

[Tabel X. Mitigation Approach. 15](#_Toc68766218)

[Tabel XI. Contoh Mitigasi Risiko Berdasarkan *Area of Concern.* 16](#_Toc68766219)

[**BAB V** 17](#_Toc68766220)

[**PENUTUP** 17](#_Toc68766221)

[**DAFTAR PUSTAKA** 18](#_Toc68766222)

# **BAB I**

# **PENDAHULUAN**

## **1.1 Pendahuluan**

Teknologi informasi memberikan kemudahan kepada pengguna untuk mengakses informasi cepat yang disediakan oleh *website* maupun pustaka digital. Namun, teknologi informasi ini rentan terhadap tindak kejahatan seperti sabotase. Perguruan tinggi banyak memanfaatkan teknologi *web* sebagai sarana untuk melayani mahasiswa dan dosen dalam bidang akademik. Teknologi *web* yang mudah diakses dan digunakan menjadi alasan utama beberapa perguruan tinggi untuk pelayanan akademik.

Tujuan penelitian ini untuk mengamati layanan akademik berbasis *web* pada Universitas Pembangunan Nasional Veteran Jakarta. Penelitian ini memfokuskan pada identifikasi, analisis dan penilaian risiko Sistem Informasi Akademik berbasis *web* pada perguruan tinggi Universitas Pembangunan Nasional Veteran Jakarta dengan menggunakan Metode Octave Allegro.

Saat ini belum banyak perguruan tinggi yang melakukan *risk assessment* pada sistem informasi yang digunakan. Di satu sisi sistem informasi telah menjadi bagian yang sulit dipisahkan pada setiap proses bisnis di perguruan tinggi tersebut. Dengan demikian jika terdapat gangguan pada sistem informasi maka dapat mengganggu keberlangsungan proses bisnis pada perguruan tinggi yang bersangkutan.

Banyak penelitian yang menunjukkan bahwa sistem informasi beserta asetnya rentan terhadap risiko kerusakan fisik dan logika. Risiko kerusahakan fisik berkaitan dengan perangkat keras seperti bencana alam *(natural disaster),* pencurian *(thieft),* kebakaran *(fires),* lonjakan listrik *(power surge),* dan perusakan *(vandalism).* Risiko kerusakan logika mengacu pada akses yang tidak sah, kerusakan secara sengaja maupun tidak sengaja pada sistem informasi dan data untuk itu harus dilakukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi.

Atas dasar tersebut, maka penulis melakukan penilaian risiko yang berjudul “Manajemen Risiko Sistem Informasi Akademik pada Universitas Pembangunan Nasional Veteran Jakarta Menggunakan Metode Octave Allegro”. Dengan adanya penilaian risiko ini, diharapkan dapat menghasilkan temuan dan rekomendasi yang dapat digunakan sebagai referensi untuk meningkatkan pengelolaan dan penilaian risiko teknologi informasi yang ada.

## **1.2 Rumusan Masalah**

Rumusan masalah untuk penilaian risiko sistem informasi akademik pada Universitas Pembangunan Nasional Veteran Jakarta ini adalah sebagai berikut:

1. Pihak manajemen mengalami kesulitan dalam menyampaikan pentingnya untuk menjaga sistem informasi beserta aset-aset dalam rangka menjaga keberlangsungan proses bisnis yang sedang berlangsung.
2. Kurangnya kebijakan mengenai pengelolaan sistem informasi.
3. Masih kurangnya perhatian terhadap penilaian risiko pada sistem informasi yang terdapat pada Universitas Pembangunan Nasional Veteran Jakarta.

## **1.3 Batasan Masalah**

Adapun batasan masalah pada penilaian risiko sistem informasi akademik pada Universitas Pembangunan Nasional Veteran Jakarta ini adalah sebagai berikut:

1. Penilaian risiko ini sangat difokuskan untuk sistem informasi dalam melindungi asset-asset yang penting untuk menjaga informasi dan data perguruan tinggi.
2. Penilaian risiko ini dilakukan oleh bidang teknologi informasi perguruan tinggi yang bertanggungjawab dan mengelola sistem informasi akademik.
3. Metode yang digunakan dalam penilaian risiko ini adalah Octave Allegro.

## **1.4 Tujuan Penilaian Risiko**

Adapun tujuan penelitian dari penilaian manajemen risiko sistem informasi akademik pada Universitas Pembangunan Nasional Veteran Jakarta ini adalah:

1. Mengidentifikasi, menganalisis dan mengelola risiko Sistem Informasi Akademik pada Universitas Pembangunan Nasional Veteran Jakarta dengan menggunakan Metode Octave Allegro.
2. Memperbarui strategi keamanan sistem informasi akademik untuk meningkatkan keamanan sistem informasi.
3. Membuat kebijakan manajemen risiko yang mendukung misi dan prioritas organisasi untuk mengurangi dampak kerugian akibat kerusakan sistem.

## **1.5 Manfaat Penilaian Risiko**

Adapun manfaat yang didapatkan pada penelitian penilaian risiko sistem informasi akademik pada Universitas Pembangunan Nasional Veteran Jakarta ini adalah sebagai berikut:

1. Untuk mengurangi risiko kerusakan yang akan teradi pada sistem informasi akademik beserta aset-asetnya.
2. Untuk meningkatkan keamanan sistem informasi akademik.
3. Mengurangi dampak kerugian akibat kerusakan sistem informasi akademik.
4. Menekankan kepada karyawan mengenai pentingnya strategi keamanan sistem informasi beserta asset-assetnya.
5. Menyadarkan karyawan akan pentingnya menjaga keamanan sistem informasi dari kerusakan yang dapat menyebabkan terganggunya proses bisnis di perguruan tinggi yang bersangkutan.

# **BAB II**

# **LANDASAN TEORI**

## **2.1 Keamanan Sistem Informasi**

Menurut SANS.org, keamanan informasi mengacu pada proses dan metodologi yang dirancang dan dilaksanakan untuk melindungi informasi elektrobik atau bentuk lainnya yang bersifat rahasia, informasi pribadi serta data yang sensitif dari akses yang tidak sah, penyalahgunaan, pengungkapan, perusakan dan modifikasi serta gangguan. Prinsip utama keamanan informasi atau yang disebut CIA terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan).

## **2.2. Ancaman Keamanan Sistem Informasi**

Ancaman *(threats)* merupakan setiap peristiwa yang jika terjadi, dapat menyebabkan kerusakan pada sistem dan membuat hilangnya kerahasiaan, ketersediaan, atau integritas. Ancaman bisa berbahaya seperti modifikasi yang disengaja terhadap informasi sensitif atau tidak disengaja seperti kesalahan dalam perhitungan transaksi atau penghapusan file.Sedangkan kerentanan *(vulnerability)* adalah kelemahan dalam sistem yang dapat dieksploitasi oleh ancaman. Mengurangi aspek kerentanan dari sistem dapat mengurangi risiko ancaman pada sistem.

## **2.3 Manajemen Risiko dan Penilaian Risiko**

Manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja. Manajemen risiko ini memiliki ketersinambungan dengan penilaian risiko.

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara, kerentanan pada organisasi baik dari internal maupun eksternal, bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan, kemungkinan terjadinya bahaya atau kerusakan.

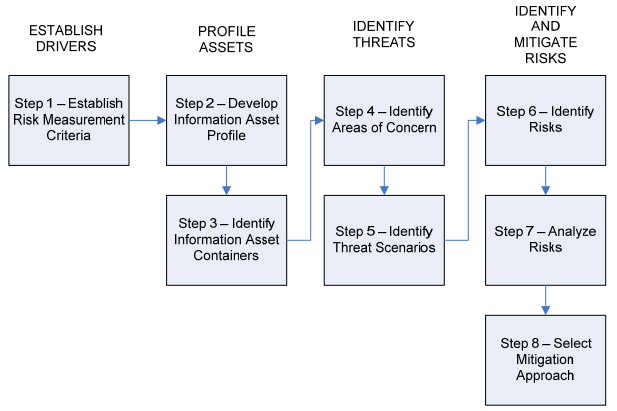
Dalam melakukan analisis risiko terdapat tiga langkah utama, analisis risiko umumnya jauh lebih komprehensif dan dirancang untuk digunakan agar dapat mengukur tingkat kerumitan dalam skenario multi risiko. Adapun langkah-langkah yang dapat ditempuh adalah sebagai berikut:

1. Memperkirakan potensi kerugian pada aset dengan menentukan nilai masing-masing aset.
2. Melakukan analisis potensi ancaman terhadap aset.
3. Menentukan *Annualized Loss Expectancy* (ALE).

## **2.4 Metode Octave**

*Operationally Critical Threat, Asset, and Vulnerability Evaluation* atau akronim dari Octave adalah definisi dari komponen-komponen penting secara komprehensif, dan sistematis dari konteks berbasis *(context-driven)* evaluasi risiko keamanan informasi. Dengan menggunakan metode Octave, organisasi dapat membuat perlindungan terhadap informasi untuk pengambilan keputusan risiko berdasarkan CIA *(Confidentiality, Integrity, Authentication)* untuk asset teknologi informasi kritis.

Metode Octave memiliki tiga varian yaitu Octave, Octave-S dan Octave Allegro. Octave merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. Octave Allegro merupakan metode yang disederhanakan dengan fokus pada asset informasi. Varian ini dapat dilakukan dengan metode *workshop-style* dan kolaboratif. Octave Allegro terdiri dari delapan langkah dibagi dalam empat fase sebagai berikut:



### Gambar I. Langkah-langkah Metode Octave Allegro.

# **BAB III**

# **TAHAPAN PENILAIAN RISIKO**

1. Membangun Kriteria Pengukuran Risiko

Pada tahapan ini terdapat 2 (dua) aktivitas yang dijalankan, yaitu membangun *organizational drivers* yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* dari ruang lingkup penilaian risiko.

1. Mengembangkan Profil Asset Informasi

Pada tahapan ini terdiri dari 8 (delapan) aktivitas yang dijalankan, yaitu identifikasi asset informasi, penilaian risiko terstruktur, mengumpulkan informasi asset, membuat dokumentasi pemilihan asset, aktivitas kelima dan keenam membuat deskripsi asset, mengisi keamanan untuk *confidentiality, integrity,* dan *availability* serta mengidentifikasi kebutuhan keamanan untuk asset informasi.

1. Mengidentifikasi Kontainer dari Aset Informasi

Pada tahapan ini terdiri dari 1 (satu) aktivitas yaitu memperhatikan poin-poin penting dari asset informasi yang akan dijaga.

1. Mengidentifikasi Area Masalah

Pada tahapan ini terdiri dari 1 (satu) aktivitas yaitu pengembangan profil risiko dari asset informasi.

1. Mengidentifikasi Skenario Ancaman

Pada tahapan ini terdiri dari1 (satu) aktivitas yaitu melakukan identifikasi scenario ancaman tambahan.

1. Mengidentifikasi Risiko

Pada tahapan ini terdiri dari1 (satu) aktivitas yaitu risiko atau ancaman yang telah didokumentasikan pada *information asset risk worksheet.*

1. Menganalisis Risiko

Pada tahapan ini terdiri dari 2 (dua) aktivitas yaitu melakukan *review risk measurement criteria* dan menghitung nilai risiko relative yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

1. Memilih Pendekatan Pengurangan

Pada tahapan ini terdiri dari1 (satu) aktivitas yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risiko dan melakukan pendekatan dan mitigasi untuk setiap risiko dengan berpedoman pada kondisi organisasi.

# **BAB IV**

# **PEMBAHASAN**

Hal yang pertama kali kita harus lakukan adalah mendapatkan informasi mengenai asset dan juga informasi mengenai sistem yang mau kita analisis risiko yaitu dengan metode komunikasi dan juga wawancara. Pada metode komunikasi dimulai dengan menghubungi pihak-pihak yang memiliki kepentingan seperti divisi TI, pimpinan divisi, sistem analis, dan programmer. Hal ini dilakukan agar nantinya proses analisis risiko berjalan lancar dan tidak ada yang tertinggal.

1. **Langkah 1**

Setelah membangun *organizational drivers* maka dilakukan penentuan *impact area* dan memberikan nilai skala prioritas pada *impact area*. Dan untuk membuat *impact area* harus memerhatikan misi dan tujuan bisnis dari organisasi tersebut. Prioritas *impact area* yangd dipilih pertama yaitu kepercayaan pelanggan, Finansial, produktivitas, keamanan, dan kesehatan serta denda dan pinalti berikut adalah tabel dari *impact area* dan skala prioritas.

### Tabel I. *Impact Area* dan Reputasi Kepercayaan Pelanggan.

|  |  |  |  |
| --- | --- | --- | --- |
| *Impact Area* | *Low* | *Medium* | *High* |
| *Reputation* | Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan. | Reputasi terkena dampak buruk dan dibutuhkan usaha serta biaya perbaikan. | Reputasi terkena dampak buruk, sangat buruk hingga hampir tidak dapat diperbaiki. |
| *Customer Loss* | Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan. | Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan. | Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan. |

### Tabel II. Skala Prioritas *Impact Area*.

|  |  |
| --- | --- |
| *Priority* | *Impact Area* |
| 5 | Reputasi dan kepercayaan pelanggan |
| 4 | Financial |
| 3 | Produktifitas |
| 2 | Keamanan dan kesehatan |
| 1 | Denda dan penalti |

1. **Langkah 2**

Dalam prosesmengembangkan *information asset profile* harus ditentukan asset informasi kritis berdasarkan *core process,* dimulai dari data mahasiswa hingga laporan nilai akhir. kemudian yang harus dilakukan selanjutnya yaitu menentukan asset informasi kritikal yang dicatat pada *critical asset information worksheet.* Asset informasi yang dipilih harus mempertimbangkan hal-hal berikut:

1. Asset informasi yang penting dan digunakan dalam kegiatan sehari-hari.
2. Asset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi dari sistem informasi akademik yang penting diantaranya yaitu profil mahasiswa, profil dosen, profil mata kuliah dan transaksi nilai mahasiswa. Berikut contoh *information asset profiling* untuk transaksi nilai mahasiswa.

### Tabel III. Informasi Asset *Profilling* dan Transaksi Nilai Mahasiswa.

|  |  |  |
| --- | --- | --- |
| ***Critical Asset*** | | Transaksi nilai mahasiswa. |
| ***Rationale for Selection*** | | Digunakan untuk menentukan IPK dan penentuan mutu mahasiswa. |
| ***Description*** | | Terdiri dari nilai akhir mahasiswa. |
| ***Owner*** | | Kepala Program Studi. |
| ***Security Requirements*** | ***Confidentiality*** | Informasi nilai sangat penting bagi mahasiswa, dosen, dan jurusan. Bagian administrasi mahasiswa menggunakan informasi untuk mencetak transkrip nilai |
| ***Integrity*** | Informasi harus benar dan akurat, dapat berubah dan diganti oleh dosen, hanya operator di bagian administrasi kemahasiswaan yang dapat memasukan atau memodifikasi nilai mahasiswa |
| ***Availability*** | Informasi harus selalu tersedia bagi mahasiswa, dosen dan bagian administrasi kemahasiswaan |
| ***Most Important Security Requirement*** | | *Integrity*  Alasan: Nilai merupakan informasi penting bagi mahasiswa, jika terdapat kesalahan akan merugikan mahasiswa |

1. **Langkah 3**

Dalam Identifikasi *information asset container* dibagi menjadi tiga tiga yaitu *technical*, *physical* dan *people* dari ketiga tersebut memiliki sisi internal dan juga eksternal yang di dapat dengan worksheet *Information Asset Risk Environment Map.* Berikut contoh *Information Asset Risk Environment Map (Technical)* – Transaksi Nilai Mahasiswa.

### Tabel IV. Informasi Asset *Risk Environtment (Technical)* dan Transaksi Nilai Mahasiswa.

|  |  |
| --- | --- |
| **Data Transaksi Nilai Mahasiswa** |  |
| ***Information Asset Risk Environment Map (Technical)*** |  |
| ***Internal*** |  |
| ***Container Description*** | **Owner(s)** |
| Modul: Transaksi Input Nilai  Input transaksi nilai mahasiswa untuk proses pengolahan nilai mahasiswa. | Administrasi Kemahasiswaan, Staff Jurusan |
| ***External*** | **Owner(s)** |
| Container Description | Mahasiswa |
| Aplikasi: Web Nilai |  |
| Mahasiswa dapat melihat nilai |  |

1. **Langkah 4**

Kemudian Identifikasi *areas of concern* yaitu dengan meninjau ulang setiap *container* untuk melihat dan menentukan *areas of concern* yang potensial dengan melakukan dokumentasi setiap areas of oncern yang sudah diidentifikasi. Kemudian diperluas untuk mendapatkan *threat scenarios* kemudian didokumentasikan untuk melihat apakah mempengaruhi *security requirements.*

### Tabel V. Area Concern dan Transaksi Nilai Mahasiswa.

|  |  |
| --- | --- |
| **No** | ***Area of Concern*** |
| 1 | Jumlah data nilai yang banyak dapat menyebabkan kesalahan *input* data oleh staf administrasi kemahasiswaan. |
| 2 | Penyebaran akses *password* transaksi nilai oleh staf bagian administrasi yang memiliki akses. |
| 3 | Celah keamanan pada aplikasi web nilai mahasiswa yang dapat dieksploitasi oleh pihak dalam/luar. |
| 4 | *Error* yang terjadi pada saat proses *insert/update/delete* modul transaksi nilai dilakukan secara bersama-sama. |

1. **Langkah 5**

Kemudian Identifikasi *threat scenario* yang memberikan gambaran secara rinci mengenai property dari ancaman. antara lain *actor, means, motives, outcome* dan *security requirement.* Untuk melengkapi *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum. Berikut contoh *properties of threat* hasil perluasan dari *areas of concern* transaksi nilai mahasiswa.

### Tabel VI. Properties of Threat dan Transaksi Nilai Mahasiswa.

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | ***Area of Concern*** | ***Threat of Properties*** | |
| Jumlah data nilai yang banyak menyebabkan kesalahan input data nilai oleh staf administrasi kemahasiswaan. | ***1. Actors*** | Staf administrasi  Kemahasiswaan. |
| ***2. Means*** | Staf menggunakan  modul aplikasi nilai mahasiswa. |
| ***3. Motives*** | *Human error*  *(accidental)* |
| ***4. Outcome*** | *Modification, interruption* |
| ***5. Security Requirements*** | 1. Validasi *input* data nilai pada *field.* 2. Dosen atau Staf Jurusan melakukan verifikasi nilai yang telah di*input* oleh staf administrasi kemahasiswaan. |

|  |  |  |  |
| --- | --- | --- | --- |
| **2** | ***Area of Concern*** | ***Threat of Properties*** | |
| Penyebaran akses password transaksi nilai oleh staff administrasi kemahasiswaan yang memiliki akses | ***1. Actors*** | Staf administrasi |
| ***2. Means*** | Modul aplikasi nilai  mahasiswa |
| ***3. Motives*** | Secara sengaja/tidak sengaja memberitahukan *password* (*deliberate,*  *accidental*). |
| ***4. Outcome*** | *Disclosure, Modification,* dan *Interruption.* |
| ***5. Security Requirements*** | Memberikan pemahaman untuk menjaga kerahasiaan *password* dan hukuman bagi stff yang sengaja menyebarkan *password.* |

1. **Langkah 6**

Tujuan dari Identifikasi risiko untuk menentukan bagaiman *threat scenario* memberikan dampak baik bagi organisasi serta menentukan tingkatannya. Dilanjutkan dengan menghitung *relative score* untuk membantu organisasi dalam menganalisis risiko. Berikut table menunjukan cara menghitung *relative score*.

### Tabel VII. Cara Menghitung *Relative Score.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Impact areas*** | *Priority* | *Low*  *(1)* | *Medium*  *(2)* | *High*  *(3)* |
| Reputasi dan kepercayaan pelanggan | 5 | 5 | 10 | 15 |
| Finansial | 4 | 4 | 8 | 12 |
| Produktivitas | 3 | 3 | 6 | 9 |
| Keamanan dan Kesehatan | 1 | 1 | 2 | 3 |
| Denda dan Penalti | 2 | 2 | 4 | 6 |

1. **Langkah 7**

Dalam setiap *area of concern* diperlukan Analisis risiko dari information asset untuk bisa mengukur konsekuensi yang terjadi berdasarkan *relative risk score*. Berikut tabel contoh analisis risiko – transaksi nilai mahasiswa.

### Tabel VIII. Analisis Risiko dan Transaksi Nilai Mahasiswa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Area of Concern*** | ***Risk*** | | | |
| Jumlah data nilai yang banyak menyebabkan kesalahan *input* data nilai oleh staf administrasi kemahasiswaan. | ***Consequences*** | Diperlukan waktu tambahan untuk memperbaiki kesalahan input data nilai, | | |
| ***Severity*** | ***Impact Area*** | ***Value*** | ***Score*** |
| Reputasi dan kepercayaan  pelanggan | Med | 10 |
| Finansial | Low | 4 |
| Produktivitas | High | 9 |
| Keamanan dan  Kesehatan | Low | 1 |
| Denda dan Penalti | Low | 2 |
| ***Relative Risk Score*** | | 26 |

1. **Langkah 8**

Pendekatan mitigasi dilakukan berdasarkan pengelompokan risiko yaitu berdasarkan *Relative Risk Matrix* dan *Area of Concern.*

### Tabel IX. Relative Risk Matrix.

|  |  |  |
| --- | --- | --- |
| ***RISK SCORE*** | | |
| **30 TO 45** | **16 TO 29** | **0 TO 15** |
| POOL 1 | POOL 2 | POOL 3 |

### Tabel X. Mitigation Approach.

|  |  |
| --- | --- |
| **Pool** | ***Mitigation Approach*** |
| Pool 1 | *Mitigate* |
| Pool 2 | *Mitigate or Defer* |
| Pool 3 | *Accept* |

### Tabel XI. Contoh Mitigasi Risiko Berdasarkan *Area of Concern.*

|  |  |
| --- | --- |
| ***Risk Mitigation*** | |
| ***Area of Concern*** | Jumlah data nilai yang banyak menyebabkan kesalahan input data nilai oleh staf administrasi kemahasiswaan. |
| ***Action*** | *Mitigate* |
| ***Container*** | *Control* |
| Modul data nilai  mahasiswa | Dibuat validasi *input* pada *field* tertentu. |
| Staf Jurusan / Dosen | Dosen atau staff jurusan dapat melakukan verifikasi nilai yang telah diinputkan oleh staf administrasi kemahasiswaan. |

# **BAB V**

# **PENUTUP**

* 1. **Kesimpulan**

Dari penelitian diatas dapat disimpulkan bahwa Octave Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perguruan tinggi. Selain itu, penilaian risiko yang dilakukan menghasilkan temuan dan rekomendasi yang dapat digunakan sebagai referensi untuk meningkatkan pengelolaan dan penilaian risiko teknologi informasi yang ada.

* 1. **Saran**

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika scenario ancaman benar-benar terjadi.

# **DAFTAR PUSTAKA**

Jakaria, D. A., & Dirgahayu, R. T. (2013, June). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)* (Vol. 1, No. 1).

Nelmiawati, N., Destrianto, F. R., & Sitorus, M. A. R. (2017). Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE. *Jurnal Integrasi*, *9*(1), 35-47.

Kuntari, N. L., Chrisnanto, Y. H., & Hadiana, A. I. (2018, July). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro. In *Seminar Nasional Teknologi Informasi* (Vol. 1, pp. 551-559).