Jurnal Infosecure Vol.5 No.2, Oktober 2024
p-ISSN: 2087-1023
MTI-UNLA

Pengelolaan Risiko Aset Teknologi Informasi Pada Sistem Akademik di Politeknik Harapan Bersama Kota Tegal

Arrahman Mukhlis Harimadi[1], Purnomo Yustianto[2], Ashwin Sasongko Subroto[3]

Magister Teknik Informatika, Universitas Langlang Buana[1]

[1]arrahmanmuclis@gmail.com,

Abstrak— Meningkatnya ketergantungan terhadap teknologi informasi (TI) di institusi akademik telah menimbulkan risiko baru yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan aset penting. Penelitian ini bertujuan untuk mengembangkan kerangka manajemen risiko aset TI pada sistem akademik di Politeknik Harapan Bersama Kota Tegal. Penelitian ini mengidentifikasi dan menilai potensi risiko yang terkait dengan aset TI, termasuk perangkat keras, perangkat lunak, dan data. Pendekatan metode campuran, yang menggabungkan pengumpulan dan analisis data kualitatif dan kuantitatif, digunakan untuk mengumpulkan wawasan dari para pemangku kepentingan dan pakar. Studi ini mengungkapkan bahwa institusi tersebut menghadapi risiko yang signifikan, termasuk serangan dunia maya, pelanggaran data, dan kegagalan sistem, yang dapat berdampak buruk pada operasional dan reputasi akademik. Kerangka kerja manajemen risiko diusulkan, yang menggabungkan strategi identifikasi, penilaian, mitigasi, dan pemantauan risiko. Kerangka kerja ini dirancang untuk memberikan pendekatan terstruktur dalam mengelola risiko TI, memastikan perlindungan aset penting, dan menjaga kepercayaan pemangku kepentingan. Studi ini berkontribusi terhadap pengembangan sistem manajemen risiko yang kuat, meningkatkan ketahanan institusi akademis dan mendorong budaya kesadaran risiko di kalangan pemangku kepentingan.

Kata Kunci: Manajemen Risiko, Aset Teknologi Informasi, Sistem Akademik, Politeknik Harapan Bersama Kota Tegal.

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini sangat cepat sehingga menjadi kebutuhan yang sangat penting untuk kehidpan sehari-hari. Karena setiap kegiatan yang manusia lakukan di bumi telah menggunakan teknologi informasi. Salah satunya adalah kegiatan yang dilakukan dalam dunia pendidikan sekarang sudah menggunakan teknologi informasi, dimulai dari administrasi sampai dengan kegiatan pembelajaran. (Ain, Ambarwati, and Junaedi 2022)

Risiko adalah potensi bahaya, yang mengarah pada aktivitas bisnis instansi yang kurang ideal. Risiko adalah sesuatu yang tidak pasti dan mempengaruhi peluang instansi untuk mencapai suatu tujuan atau ambisi. Risiko adalah bagian yang tidak terpisahkan dari aktifitas manusia, ibarat seperti tidak ada kehidupan tanpa adanya risiko . Ketika sistem yang dikerahkan tidak berfungsi secara efektif, sebuah institusi yang bergantung pada sistem informasi untuk sebagian besar proses bisnisnya dapat mengalami gangguan serius. Jika timbul bahaya dalam penggunaan perangkat lunak dan perangkat keras, instansi harus siap mengambil tindakan yang tepat. Penanganan risiko ditujukan pada aset yang memiliki kemungkinan terjadinya risiko dengan mengidentifikasi penyebab dan mencari solusi yang tepat. Analisis manajemen risiko merupakan suatu proses yang dilakukan pada tingkat manajemen pelaksana, yaitu berupa proses analisis sistematis dari setiap kerugian yang dapat dihadapi oleh sebuah kampus, akibat dari suatu risiko juga cara pengendalian yang tepat guna mengatasi kerugian pada instansi, Manajemen risiko teknologi informasi diperlukan untuk mengurangi kemungkinan dan dampak dari potensi risiko berdasarkan potensi tingkat risiko tersebut. Manajemen risiko merupakan kegiatan mengurangi atau mengendalikan kemungkinan kesalahan atau kerugian yang diakibatkan oleh semua risiko. Manajemen risiko harus dilakukan sebagai bagian dari manajemen instansi. Proses manajemen risiko ini merupakan salah satu langkah yang dapat diikuti untuk menciptakan perbaikan berkelanjutan. Selain itu, manajemen risiko adalah proses yang sering dikaitkan dengan pengambilan keputusan di instansi engan demikian keberhasilan manajemen risiko bergantung pada manusiamanusia yang melaksanakannya. Lebih spesifik lagi, keberhasilan manajemen risiko bergantung pada kemampuan (kapabilitas), cara pandang (persepsi), dan niat (intensi) orang-orang yang melaksanakannya. Meskipun risiko tidak dapat sepenuhnya dihilangkan, setidaknya dapat dikelola, menjadikan aset Teknologi Informasi (TI) suatu instansi lebih fungsional dan berguna. (Fahlepi et al. 2023)

Pada penelitian ini penulis mengambil salah satu metode untuk manajemen risiko yang sesuai untuk penanganan permasalahan diatas. Metode yang dipilih yaitu menggunakan ISO/IEC 27001:2013 yang dapat digunakan untuk organisasi, kampus public, kampus swasta, organisasi nirlaba, kelompok ataupun perseorangan. Standar ini digunakan selama masa hidup organisasi dan untuk berbagai kegiatan, proses, fungsi, proyek, produk, jasa, aset, operasi dan pengambilan keputusan. Terdapat lima kegaitan risiko yang termasuk dalam proses manajemen risiko yaitu komunikasi dan konsultasi, menentukan konteks, asesmen risiko, perlakuan risiko dan monitoring serta review. Identifikasi risiko, analisis risiko

dan evaluasi risiko ketiga hal tersebut termasuk dalam bagian asesmen risiko.(Nikmat 2024)

Hasil akhir dari tujuan penelitian ini terdapat aset yang harus dilindungi, kemudian mengevaluasi level risiko bernilai tinggi, menentukan penanganan risiko berupa dokumen penilaian beserta penyusunan kontrol risiko untuk menjamin keamanan pada aset TI.

II. METODE

Beberapa tantangan yang mungkin dihadapi pada saat implementasi sebagai metodologi peniliaian risiko sistem informasi antara lain :

1. Penetepan Konteks
   Menetapkan konteks penilaian risiko keamanan informasi, meliputi:
   - Penetapan pendekatan manajemen risiko serta kriteria kemungkinan (likelihood), kriteria dampak, nilai/tingkat risiko, dan keberterimaan risiko.
   - Pendefinisian ruang lingkup dan batasan manajemen risiko keamanan informasi, misalnya: aplikasi, infrastruktur TI, proses bisnis, dll.
   - Penetapan organisasi dan tanggung jawabnya terhadap pelaksanaan manajemen risiko keamanan informasi.
2. Identifikasi Aset
   Aset adalah segala sesuatu yang memiliki nilai bagi organisasi, operasi bisnisnya, dan kelangsungannya.
   Tiga Jenis Aset Utama yaitu:
   - Informasi murni (dalam format apapun)
   - Aset fisik seperti gedung dan sistem computer
   - Perangkat lunak yang digunakan untuk memproses atau mengelola informasi

   Contohnya :
   - Website
   - Laptop (inventaris)
   - Data keuangan
3. Identifikasi Ancaman
   Ancaman adalah penyebab potensial dari suatu insiden yang dapat mengakibatkan kerusakan pada sistem atau organisasi.
4. Analisis Nilai Dampak
   Dampak adalah akibat dari insiden keamanan informasi, yang disebabkan oleh ancaman, yang memengaruhi aset. Serta Identifikasi tingkat kerusakan atau biaya bagi organisasi disebabkan oleh peristiwa keamanan informasi.
5. Identifikasi Kerentanan
   Kerentanan adalah kelemahan aset atau kelompok aset yang dapat dimanfaatkan oleh satu atau lebih ancaman.
6. Analisis Probabilitas Ancaman
   Menganalisis probabilitas atau kemungkinan (*likelihood*) terjadinya setiap ancaman atau serangan terhadap aset dikarenakan masih adanya kerentanan yang dimiliki aset.
7. Analisis Risiko
   Menentukan nilai atau tingkat risiko keamanan informasi untuk setiap aset berdasarkan hasil analisis dampak dan kemungkinan terjadinya insiden berdasarkan kriteria yang dijadikan acuan penentuan nilai atau tingkat risiko.
   - Qualitative Estimation – Tingkat risiko: Low, Medium and High – Dampak: Low, Medium and High
   - Quantitative Estimation – Tingkat risiko = asset x threat x vulnerability – Dampak: kalkulasi nilai uang yang hilang
8. Evaluasi Risiko
   Untuk mengevaluasi risiko, organisasi harus membandingkan risiko yang diperkirakan (menggunakan metode atau pendekatan yang dipilih) dengan risiko kriteria evaluasi yang ditentukan selama penetapan konteks.
   Output: Daftar risiko yang diprioritaskan menurut evaluasi risiko kriteria dalam kaitannya dengan skenario insiden yang mengarah pada risiko tersebut.
9. Rencana Penanganan Risiko
   Memilih dan menerapkan satu opsi atau lebih untuk menangani risiko yang akan dimitigasi.

Berikut ini adalah gambaran penanganan risiko di politeknik harapan bersama sebagai berikut:

Gambar 2. 1 Penanganan Risiko Di Politeknik Harapan Bersama

III. HASIL DAN PEMBAHASAN

Beberapa tantangan yang mungkin dihadapi pada saat implementasi sebagai metodologi peniliaian risiko sistem informasi antara lain :

1. Penetepan Konteks
   Menetapkan konteks penilaian risiko keamanan informasi, meliputi:
   a. Penetapan pendekatan manajemen risiko serta kriteria kemungkinan (*likelihood*), kriteria dampak, nilai/tingkat risiko, dan keberterimaan risiko.
   b. Pendefinisian ruang lingkup dan batasan manajemen risiko keamanan informasi, misalnya: aplikasi, infrastruktur TI, proses bisnis, dll.
   c. Penetapan organisasi dan tanggung jawabnya terhadap pelaksanaan manajemen risiko keamanan informasi.
2. Identifikasi Aset
   Aset adalah segala sesuatu yang memiliki nilai bagi organisasi, operasi bisnisnya, dan kelangsungannya.
   Tiga Jenis Aset Utama yaitu:

a. Informasi murni (dalam format apapun);
b. Aset fisik seperti gedung dan sistem computer;
c. Perangkat lunak yang digunakan untuk memproses atau mengelola informasi.

Contohnya :

a. Website
b. Laptop (inventaris)
c. Data keuangan

3. Identifikasi Ancaman
   Ancaman adalah penyebab potensial dari suatu insiden yang dapat mengakibatkan kerusakan pada sistem atau organisasi.
4. Analisis Nilai Dampak
   Dampak adalah akibat dari insiden keamanan informasi, yang disebabkan oleh ancaman, yang memengaruhi aset. Serta Identifikasi tingkat kerusakan atau biaya bagi organisasi disebabkan oleh peristiwa keamanan informasi.
5. Identifikasi Kerentanan
   Kerentanan adalah kelemahan aset atau kelompok aset yang dapat dimanfaatkan oleh satu atau lebih ancaman.
6. Analisis Probabilitas Ancaman
   Menganalisis probabilitas atau kemungkinan (*likelihood*) terjadinya setiap ancaman atau serangan terhadap aset dikarenakan masih adanya kerentanan yang dimiliki aset.
7. Analisis Risiko
   Menentukan nilai atau tingkat risiko keamanan informasi untuk setiap aset berdasarkan hasil analisis dampak dan kemungkinan terjadinya insiden berdasarkan kriteria yang dijadikan acuan penentuan nilai atau tingkat risiko.
   a. Qualitative Estimation – Tingkat risiko: Low, Medium and High – Dampak: Low, Medium and High
   b. Quantitative Estimation – Tingkat risiko = asset x threat x vulnerability – Dampak: kalkulasi nilai uang yang hilang.
8. Evaluasi Risiko
   Untuk mengevaluasi risiko, organisasi harus membandingkan risiko yang diperkirakan (menggunakan metode atau pendekatan yang dipilih) dengan risiko kriteria evaluasi yang ditentukan selama penetapan konteks.
   Output: Daftar risiko yang diprioritaskan menurut evaluasi risiko kriteria dalam kaitannya dengan skenario insiden yang mengarah pada risiko tersebut.
9. Rencana Penanganan Risiko
   Memilih dan menerapkan satu opsi atau lebih untuk menangani risiko yang akan dimitigasi.

4.1. ***Penilaian Risiko***

Tahap pertama pelaksanaan penilaian risiko dimulai dengan menghubungi pihak – pihak pengelola di divisi TI antara lain pimpinan UPT IT, sistem analis serta programmer untuk mendapatkan data – data yang diperlukan. Tahap selanjutnya adalah melakukan wawancara untuk mendapatkan informasi mengenai aset operational kritis bagi kampus.

Langkah 1 - setelah membangun *organizational drivers* maka dilakukan penentuan *impact* area yang paling penting serta memberikan nilai skala prioritas pada *impact* area yang telah ditentukan. Sebagai pertimbangan untuk menentukan *impact* area adalah misi dan tujuan bisnis organisasi tersebut. Prioritas *impact* area yang dipilih pertama adalah reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan serta denda dan penalti. Tabel 1 berisi hasil penentuan *impact* area – reputasi dan kepercayaan pelanggan dan tabel 2 adalah skala prioritas *impact* area.

Tabel 3. *1* Kriteria Kemungkinan

Tingkat	Frekuensi Kejadian
Sangat Rendah	Ancaman Terjadi sekali > 5 Tahun
Rendah	Ancaman Dapat Terjadi sekali diatas 2 tahun sampai 5 Tahun
Menengah	Ancaman mungkin Terjadi sekali dalam 1-2 Tahun
Tinggi	Ancaman mungkin Terjadi beberapa kali dalam 1 tahun
Sangat Tinggi	Ancaman terjadi hampir setiap minggu/bulan

Tabel 3.1 berisi kriteria kemungkinan terjadinya ancaman yang dikategorikan berdasarkan frekuensi kejadian. Tabel ini digunakan untuk menilai seberapa sering sebuah ancaman atau risiko mungkin terjadi dalam suatu periode waktu tertentu. Berikut adalah penjelasan setiap tingkat kemungkinan dan frekuensi kejadiannya:

1. Sangat Rendah:
   Frekuensi Kejadian: Ancaman terjadi sekali dalam lebih dari 5 tahun. Ini menggambarkan kejadian yang sangat jarang terjadi, kemungkinan ancaman hampir tidak ada atau hanya muncul dalam jangka waktu yang sangat panjang.
2. Rendah:
   Frekuensi Kejadian: Ancaman dapat terjadi sekali dalam 2 hingga 5 tahun. Kemungkinan ancaman cukup kecil, tetapi masih mungkin terjadi dalam rentang waktu beberapa tahun.
3. Menengah:
   Frekuensi Kejadian: Ancaman mungkin terjadi sekali dalam 1-2 tahun. Ancaman memiliki kemungkinan sedang untuk terjadi, dengan frekuensi kejadian yang lebih terukur, biasanya dalam jangka waktu setahun hingga dua tahun.
4. Tinggi:
   Frekuensi Kejadian: Ancaman mungkin terjadi beberapa kali dalam satu tahun. Kemungkinan ancaman

cukup besar, dengan kejadian yang bisa berulang dalam satu tahun kalender.

5. Sangat Tinggi:
   Frekuensi Kejadian: Ancaman terjadi hampir setiap minggu atau bulan. Ini menunjukkan bahwa ancaman sering terjadi dengan frekuensi tinggi, baik secara mingguan maupun bulanan.

Tabel 3. 2 Kriteria Dampak

Tingkat	Dampak Operasional	Dampak Reputasi
Tidak Signifikat	Menimbulakan gangguan pada sistem kurang dari 5 jam	Ancaman Terjadi sekali > 5 Tahun
Kecil	Menimbulkan gangguan pada fungsi sistem (5 jam hingga 1 hari)	Ancaman Dapat Terjadi sekali diatas 2 tahun sampai 5 Tahun
Menengah	Menimbulkan gangguan pada fungsi sistem (lebih dari 1 hari hingga 7 hari)	Ancaman mungkin Terjadi sekali dalam 1-2 Tahun
Besar	Menimbulkan gangguan pada fungsi sistem (lebih dari 7 hari hingga 1 bulan)	Ancaman mungkin Terjadi beberapa kali dalam 1 tahun
Sangat Besar	Menimbulkan gangguan pada fungsi sistem (lebih dari 1 tahun)	Ancaman terjadi hampir setiap minggu/bulan

Tabel 3.2 ini menguraikan tingkat dampak dari suatu ancaman terhadap dua aspek utama: Dampak Operasional dan Dampak Reputasi. Setiap tingkatan dampak menunjukkan seberapa parah gangguan yang disebabkan oleh suatu ancaman terhadap operasi sistem dan reputasi organisasi. Berikut penjelasan lebih lanjut:

1. Tidak Signifikan
   Dampak Operasional: Menimbulkan gangguan pada sistem selama kurang dari 5 jam. Gangguan ini dianggap sangat ringan dan tidak menyebabkan dampak besar pada kelangsungan operasi.
   Dampak Reputasi: Ancaman terjadi sekali dalam lebih dari 5 tahun. Dampaknya terhadap reputasi sangat kecil dan jarang terjadi, sehingga tidak memengaruhi persepsi publik secara signifikan.
2. Kecil
   Dampak Operasional: Menimbulkan gangguan pada fungsi sistem selama 5 jam hingga 1 hari. Gangguan ini dapat menghambat operasi, tetapi masih dalam tingkat yang dapat diatasi dalam waktu relatif cepat.
   Dampak Reputasi: Ancaman dapat terjadi sekali dalam 2 hingga 5 tahun. Dampaknya terhadap reputasi masih rendah, namun ada kemungkinan terjadi, dan bisa menimbulkan sedikit perhatian publik.
3. Menengah
   Dampak Operasional: Menimbulkan gangguan pada fungsi sistem selama lebih dari 1 hari hingga 7 hari. Gangguan ini cukup signifikan, menghambat operasi untuk jangka waktu yang lebih lama dan memerlukan waktu lebih banyak untuk pemulihan.
   Dampak Reputasi: Ancaman mungkin terjadi sekali dalam 1-2 tahun. Dampak reputasi berada di tingkat sedang, dengan kemungkinan adanya gangguan pada citra atau kepercayaan publik yang perlu diperbaiki.
4. Besar
   Dampak Operasional: Menimbulkan gangguan pada fungsi sistem selama lebih dari 7 hari hingga 1 bulan. Gangguan ini berdampak besar, sangat mengganggu operasi organisasi dan berpotensi menyebabkan kerugian signifikan.
   Dampak Reputasi: Ancaman mungkin terjadi beberapa kali dalam satu tahun. Reputasi organisasi bisa mengalami penurunan yang signifikan, dengan publik atau pihak terkait sering mengalami gangguan kepercayaan.
5. Sangat Besar
   Dampak Operasional: Menimbulkan gangguan pada fungsi sistem selama lebih dari 1 tahun. Dampak ini sangat besar dan serius, dapat menyebabkan disrupsi besar-besaran pada operasi dan memerlukan waktu lama untuk pemulihan.
   Dampak Reputasi: Ancaman terjadi hampir setiap minggu atau bulan. Reputasi organisasi mengalami kerugian besar, dengan ancaman terus-menerus yang memperburuk kepercayaan publik dan citra perusahaan secara keseluruhan.

Tabel 3.2 ini membantu dalam menilai tingkat keparahan ancaman terhadap operasional dan reputasi, dan biasanya digunakan dalam manajemen risiko untuk memahami dan memitigasi risiko yang mungkin terjadi pada sistem atau organisasi.

Tabel 3. *3* Kriteria Nilai / Tingkat Risiko

Kemungkinan (*Likelihood*)	**Dampak (*Impact/Consequences*)**				
	Tidak Sigifikan	**Kecil**	**Menengah**	**Besar**	**Sangat Besar**
Sangat Rendah	Rendah	Rendah	Rendah	Menengah	Tinggi

Kemungkinan (*Likelihood*)	**Dampak (*Impact/Consequences*)**				
	Tidak Sigifikan	**Kecil**	**Menengah**	**Besar**	**Sangat Besar**
Rendah	Rendah	Rendah	Menengah	Tinggi	Sangat Tinggi
Menengah	Rendah	Menengah	Menengah	Tinggi	Sangat Tinggi
Tinggi	Menengah	Menengah	Tinggi	Sangat Tinggi	Sangat Tinggi
Sangat Tinggi	Tinggi	Tinggi	Sangat Tinggi	Sangat Tinggi	Sangat Tinggi

Tabel 3.3 merupakan matriks penilaian risiko yang menggabungkan dua faktor utama: Kemungkinan (Likelihood) dan Dampak (*Impact/Consequences*). Matriks ini sering digunakan dalam analisis risiko untuk menentukan tingkat risiko dengan mengevaluasi seberapa sering suatu ancaman mungkin terjadi (kemungkinan) dan seberapa besar dampaknya jika terjadi (dampak).

Setiap sel di tabel menunjukkan tingkat risiko berdasarkan kombinasi antara kemungkinan dan dampak. Berikut penjelasan setiap kolom dan baris:

1. Kolom Dampak (*Impact/Consequences*)
   Kolom ini menggambarkan seberapa parah konsekuensi atau dampak yang dihasilkan dari ancaman atau kejadian risiko. Dampak dibagi menjadi lima tingkatan:
   a. Tidak Signifikan: Dampak yang sangat kecil, hampir tidak mempengaruhi operasional atau reputasi.
   b. Kecil: Dampak yang ringan, tetapi dapat diatasi dengan mudah.
   c. Menengah: Dampak sedang, membutuhkan upaya lebih untuk menanganinya.
   d. Besar: Dampak yang signifikan dan sangat mempengaruhi operasional atau reputasi.
   e. Sangat Besar: Dampak yang sangat serius dan merusak, memerlukan penanganan besar.
2. Baris Kemungkinan (*Likelihood*)
   Baris ini menggambarkan seberapa sering ancaman atau risiko mungkin terjadi. Kemungkinan dibagi menjadi lima tingkatan:
   a. Sangat Rendah: Ancaman atau risiko hampir tidak pernah terjadi.
   b. Rendah: Ancaman mungkin terjadi, tetapi jarang.
   c. Menengah: Ancaman berpeluang terjadi dengan frekuensi yang wajar.
   d. Tinggi: Ancaman sering terjadi.
   e. Sangat Tinggi: Ancaman sangat mungkin terjadi secara terus-menerus atau sangat sering.
3. Isi Tabel
   Matriks ini menunjukkan tingkat risiko yang diperoleh dari kombinasi antara kemungkinan dan dampak. Setiap sel dalam tabel menggambarkan tingkat risiko dengan kategori:
   a. Rendah: Risiko kecil dan biasanya tidak memerlukan tindakan khusus.
   b. Menengah: Risiko yang lebih serius dan mungkin membutuhkan perhatian, tetapi masih dapat dikelola.
   c. Tinggi: Risiko signifikan yang membutuhkan rencana mitigasi atau tindakan segera.
   d. Sangat Tinggi: Risiko yang sangat serius, memerlukan perhatian segera dan tindakan darurat untuk menghindari dampak yang parah.

Contohnya:

a. Jika suatu ancaman memiliki kemungkinan rendah tetapi dampaknya besar, maka tingkat risikonya adalah Tinggi.
b. Jika ancaman memiliki kemungkinan menengah dan dampak menengah, maka tingkat risikonya juga berada di tingkat Menengah.

Matriks ini membantu organisasi dalam menentukan prioritas tindakan berdasarkan kombinasi risiko yang berbeda. Semakin tinggi tingkat risiko, semakin penting untuk segera melakukan mitigasi atau pencegahan.

Tabel 3. *4* Kriteria Keberterimaan Risiko

Nilai Risiko	**Keriteria Keberterimaan Risiko**	**Aksi Kendali**
Rendah	Risiko diabaikan	Tidak perlu aksi kendali, cukup di pantau
Menengah	Risiko Diterima	Dilakukan pengendalian (mitigasi) risiko dengan sumber daya yang tersedia
Tinggi	Risiko Diterima	Dilakukan pengendalian (mitigasi) risiko dengan sumber daya yang dibutuhkan terlebih dahulu

Nilai Risiko	Keriteria Keberterimaan Risiko	Aksi Kendali
Sangat Tinggi	Risiko Ditransfer	pengendalian (mitigasi) risiko dilakukan oleh pihak eksternal/ pihak ke tiga

Tabel 3.4 menjelaskan penilaian risiko berdasarkan tiga elemen utama: Nilai Risiko, Kriteria Keberterimaan Risiko, dan Aksi Kendali. Tabel ini digunakan untuk menentukan bagaimana organisasi harus menangani berbagai tingkat risiko yang teridentifikasi, serta langkah-langkah apa yang perlu diambil untuk mengelola atau mengurangi risiko tersebut.

1. Nilai Risiko
   Nilai risiko menunjukkan seberapa besar tingkat risiko setelah mempertimbangkan kombinasi antara kemungkinan dan dampak dari suatu ancaman. Risiko biasanya dikategorikan menjadi beberapa tingkat:
   a. Rendah: Risiko dianggap kecil dan tidak memiliki dampak signifikan.
   b. Menengah: Risiko berada pada tingkat sedang dan memerlukan perhatian.
   c. Tinggi: Risiko signifikan dan membutuhkan tindakan pengendalian yang lebih serius.
   d. Sangat Tinggi: Risiko yang sangat besar dan memerlukan tindakan cepat serta penanganan yang lebih intensif.
2. Kriteria Keberterimaan Risiko
   Bagian ini menentukan apakah risiko dapat diterima dan bagaimana pendekatannya:
   a. Rendah: Risiko diabaikan – risiko ini dianggap tidak memerlukan tindakan khusus karena dampaknya minimal.
   b. Menengah: Risiko Diterima – risiko ini dapat diterima, tetapi tetap memerlukan tindakan mitigasi untuk mengurangi dampak atau kemungkinan terjadinya.
   c. Tinggi: Risiko Diterima – risiko cukup besar untuk diterima, tetapi membutuhkan pengelolaan yang lebih serius dan mungkin membutuhkan sumber daya tambahan untuk mitigasi.
   d. Sangat Tinggi: Risiko Ditransfer – risiko sangat tinggi sehingga organisasi memilih untuk mentransfer risiko tersebut kepada pihak eksternal, seperti menggunakan asuransi atau bekerja sama dengan pihak ketiga untuk pengelolaan risiko.
3. Aksi Kendali
   Bagian ini menggambarkan tindakan yang harus diambil untuk mengelola risiko pada setiap tingkatan:
   a. Rendah: Tidak perlu aksi kendali, cukup dipantau – karena dampak risikonya minimal, tindakan pengendalian tidak diperlukan, tetapi tetap harus dipantau.
   b. Menengah: Dilakukan pengendalian (mitigasi) risiko dengan sumber daya yang tersedia – organisasi melakukan pengendalian risiko dengan menggunakan sumber daya yang sudah ada untuk mengurangi dampaknya.
   c. Tinggi: Dilakukan pengendalian (mitigasi) risiko dengan sumber daya yang dibutuhkan terlebih dahulu – pengendalian risiko dilakukan dengan memastikan bahwa sumber daya yang diperlukan untuk mitigasi sudah tersedia dan mencukupi.
   d. Sangat Tinggi: Pengendalian (mitigasi) risiko dilakukan oleh pihak eksternal/pihak ketiga – karena risiko sangat tinggi, tindakan pengelolaan mungkin dialihkan ke pihak eksternal (misalnya, melalui kontrak, asuransi, atau outsourcing).

Contohnya:

   a. Jika risiko dinilai Rendah, maka cukup dipantau secara berkala tanpa perlu tindakan lebih lanjut.
   b. Jika risiko dinilai Menengah, maka dilakukan mitigasi menggunakan sumber daya internal yang sudah tersedia.
   c. Jika risiko dinilai Tinggi, tindakan mitigasi membutuhkan sumber daya tambahan untuk mengurangi dampaknya.
   d. Jika risiko dinilai Sangat Tinggi, organisasi bisa memilih untuk mentransfer pengelolaan risiko tersebut ke pihak eksternal, seperti perusahaan asuransi.

Tabel 3.4 membantu organisasi dalam mengidentifikasi strategi pengelolaan risiko yang tepat berdasarkan tingkat risikonya.

Tabel 3. 5 Data Aset

No	Nama Aset
1	Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal
2	Komputer Sever
3	Data Nilai Mahasiswa

Tabel 3.5 ini adalah daftar aset yang penting untuk sebuah institusi, dalam hal ini adalah Politeknik Harapan Bersama Tegal. Aset-aset ini kemungkinan terkait dengan infrastruktur teknologi informasi dan data yang dimiliki serta dioperasikan oleh kampus. Berikut adalah penjelasan untuk setiap baris:

1. Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal
   Deskripsi: Sistem ini merupakan perangkat lunak atau aplikasi yang digunakan oleh kampus untuk mengelola berbagai aspek akademik, seperti pendaftaran mata

kuliah, pengelolaan jadwal perkuliahan, pencatatan nilai, absensi, dan layanan administrasi lainnya.
Pentingnya Aset: Sistem informasi akademik sangat krusial untuk kelancaran operasional kampus, khususnya dalam hal pengelolaan data akademik mahasiswa dan dosen. Kerusakan atau gangguan pada sistem ini bisa berdampak besar pada layanan akademik dan administrasi kampus.

2. Komputer Server
Deskripsi: Komputer server adalah perangkat keras yang berfungsi sebagai pusat penyimpanan data dan pengoperasian berbagai sistem, termasuk Sistem Informasi Akademik. Server ini menyimpan data penting dan memastikan akses ke berbagai aplikasi dan sistem berjalan lancar.
Pentingnya Aset: Server merupakan pusat dari operasional teknologi informasi kampus. Jika server mengalami gangguan, maka seluruh sistem yang terhubung dengannya, seperti sistem akademik, website kampus, dan aplikasi lainnya bisa terganggu atau tidak berfungsi.
3. Data Nilai Mahasiswa
Deskripsi: Data ini mencakup catatan nilai akademik mahasiswa yang dihasilkan selama masa perkuliahan. Data ini sangat penting dalam menentukan kelulusan, transkrip akademik, dan berbagai keputusan terkait prestasi akademik.
Pentingnya Aset: Data nilai mahasiswa adalah aset informasi yang sangat berharga. Kehilangan atau kerusakan pada data ini dapat menyebabkan masalah serius, seperti hilangnya catatan akademik mahasiswa, yang dapat berdampak pada kelulusan atau pendaftaran lanjut mahasiswa.

Ketiga aset ini merupakan bagian penting dari infrastruktur teknologi informasi kampus, yang saling terhubung dan berperan dalam mendukung operasional akademik. Sistem Informasi Akademik dan Komputer Server memastikan bahwa layanan berjalan, sementara Data Nilai Mahasiswa adalah salah satu informasi yang harus dijaga keamanan dan integritasnya agar proses akademik berjalan dengan lancar.

Tabel 3. 6 Kriteria Ancaman

No	Nama Aset	Ancaman
1	Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal	*Deface*
		Ddos
		Virus
		Pengolahan data ilegal
2	Komputer Sever	Pencurian
		Komputer Server Tidak Berfungsi
		Kerusakan *Software*
3	Data Nilai Mahsiswa	Diakses Oleh Pihak Lain
		Pencurian Data
		Menerobos pertahanan sistem informasi

Tabel 3.6 adalah daftar aset penting milik Politeknik Harapan Bersama Tegal, beserta ancaman yang berpotensi menyerang masing-masing aset tersebut. Setiap aset memiliki beberapa ancaman yang perlu diperhatikan dalam konteks keamanan informasi dan teknologi. Berikut penjelasan terperinci mengenai aset dan ancamannya:

1. Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal
Ancaman:
   a. Deface: Ini adalah ancaman di mana tampilan situs atau sistem informasi diubah secara tidak sah oleh pihak eksternal. Biasanya pelaku mengubah halaman web atau konten agar menampilkan pesan yang tidak diinginkan atau merusak reputasi kampus.
   b. DDoS (Distributed Denial of Service): Serangan ini bertujuan untuk membanjiri sistem dengan lalu lintas data yang sangat tinggi, membuat sistem menjadi lambat atau tidak dapat diakses oleh pengguna yang sah.
   c. Virus: Malware yang masuk ke dalam sistem informasi dapat merusak data, memperlambat kinerja, atau bahkan menyebabkan hilangnya informasi penting.
   d. Pengolahan data ilegal: Ancaman ini muncul ketika data yang ada dalam sistem informasi akademik digunakan atau dimanipulasi secara tidak sah oleh orang dalam atau peretas. Ini bisa mengubah informasi penting seperti nilai atau status akademik mahasiswa.
2. Komputer Server
Ancaman:
   a. Pencurian: Fisik komputer server bisa menjadi sasaran pencurian oleh orang yang berusaha mendapatkan akses ke data atau perangkat keras penting.
   b. Komputer Server Tidak Berfungsi: Ancaman ini bisa terjadi karena kegagalan teknis, seperti kerusakan komponen, gangguan listrik, atau kesalahan konfigurasi yang menyebabkan server tidak dapat beroperasi.
   c. Kerusakan Software: Ancaman ini terjadi ketika perangkat lunak yang menjalankan server mengalami masalah, seperti bug, kegagalan pembaruan, atau serangan malware yang membuat software menjadi tidak berfungsi dengan baik.

3. Data Nilai Mahasiswa
Ancaman:
   a. Diakses oleh Pihak Lain: Data nilai mahasiswa adalah informasi sensitif. Jika data ini diakses oleh pihak yang tidak berwenang, bisa terjadi pelanggaran privasi yang serius. Ini bisa dilakukan oleh peretas atau oleh orang dalam yang menyalahgunakan akses mereka.

b. Pencurian Data: Ancaman ini terjadi ketika data nilai dicuri oleh pihak yang berniat menyalahgunakannya untuk tujuan pribadi, seperti memalsukan nilai atau menjual informasi.
c. Menerobos pertahanan sistem informasi: Ini adalah ancaman ketika seseorang berusaha menembus lapisan keamanan yang ada untuk mengakses atau merusak data nilai. Serangan ini bisa dilakukan melalui eksploitasi celah keamanan, phishing, atau malware.

Tabel 3.6 mencantumkan berbagai ancaman yang dapat memengaruhi aset teknologi kampus, termasuk Sistem Informasi Akademik, Komputer Server, dan Data Nilai Mahasiswa. Setiap ancaman membutuhkan strategi mitigasi yang berbeda, seperti memperkuat keamanan sistem, memonitor lalu lintas jaringan, menjaga keamanan fisik server, dan memastikan bahwa hanya pihak berwenang yang memiliki akses ke data sensitif.

Tindakan pengamanan yang tepat akan membantu melindungi aset penting kampus dari serangan siber, pencurian, dan kerusakan teknis yang dapat mengganggu operasi dan reputasi institusi.

Tabel 3.7 menguraikan aset-aset milik Politeknik Harapan Bersama Tegal, ancaman yang mungkin dihadapi oleh masing-masing aset, serta deskripsi dan tingkat dampak dari ancaman tersebut terhadap operasional sistem. Berikut adalah penjelasan terperinci:

1. Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal
   Ancaman:
   a. Deface:
      i. Deskripsi: Serangan ini mengubah tampilan sistem informasi akademik secara tidak sah.
      ii. Dampak: Gangguan fungsi sistem selama 5 jam hingga 1 hari.
      iii. Tingkat: Kecil – Gangguan ini berdampak sementara dan tidak terlalu merusak operasional, tetapi masih mengganggu aktivitas harian.

   b. *DDoS* (*Distributed Denial of Service*):
      i. Deskripsi: Serangan *DDoS* membuat sistem tidak dapat diakses dengan membanjiri server dengan lalu lintas berlebihan.
      ii. Dampak: Gangguan fungsi sistem selama 1 hari hingga 7 hari.
      iii. Tingkat: Menengah – Dampak lebih serius dan dapat mengganggu operasional kampus dalam jangka waktu yang lebih lama.
   c. Virus:
      i. Deskripsi: Infeksi virus pada sistem informasi yang menyebabkan kerusakan atau kehilangan data.
      ii. Dampak: Gangguan fungsi sistem selama 7 hari hingga 14 hari.
      iii. Tingkat: Besar – Dampaknya cukup signifikan, memerlukan waktu lama untuk perbaikan dan pemulihan.
   d. Pengolahan Data Ilegal:
      i. Deskripsi: Penggunaan atau manipulasi data akademik secara tidak sah oleh pihak yang berwenang atau tidak berwenang.
      ii. Dampak: Gangguan fungsi sistem selama 14 hingga 30 hari.
      iii. Tingkat: Sangat Besar – Dampak yang serius dan lama, dapat merusak kepercayaan dan menyebabkan masalah hukum.
2. Komputer Server
   Ancaman:
   a. Pencurian:
      i. Deskripsi: Pencurian fisik server, menyebabkan hilangnya perangkat keras dan data.
      ii. Dampak: Gangguan fungsi sistem selama 1 hingga 7 hari.
      iii. Tingkat: Menengah – Pemulihan memerlukan waktu untuk mengganti server dan memulihkan data, sehingga operasional terganggu.
   b. Komputer Server Tidak Berfungsi:
      i. Deskripsi: Server mengalami kerusakan teknis atau gangguan operasional.
      ii. Dampak: Gangguan fungsi sistem selama 5 jam hingga 1 hari.
      iii. Tingkat: Kecil – Masalah ini dapat diatasi dengan cepat, namun tetap menyebabkan gangguan sementara.
   c. Kerusakan Software:
      i. Deskripsi: Gangguan pada perangkat lunak yang mengakibatkan server tidak dapat beroperasi secara normal.
      ii. Dampak: Gangguan fungsi sistem selama 5 jam hingga 1 hari.
      iii. Tingkat: Kecil – Mirip dengan kerusakan fisik, kerusakan perangkat lunak juga menyebabkan gangguan sementara tetapi mudah diperbaiki.
3. Data Nilai Mahasiswa
   Ancaman:
   a. Diakses Oleh Pihak Lain:
      i. Deskripsi: Akses tidak sah ke data nilai mahasiswa oleh pihak yang tidak berwenang.
      ii. Dampak: Kehilangan kepercayaan stakeholder seperti mahasiswa, dosen, dan orang tua.
      iii. Tingkat: Besar – Dampaknya besar pada reputasi kampus, walaupun sistem mungkin tidak langsung terganggu secara teknis.
   b. Pencurian Data:
      i. Deskripsi: Pencurian data akademik mahasiswa yang dapat digunakan untuk tujuan jahat.
      ii. Dampak: Gangguan fungsi sistem selama 1 hari hingga 7 hari.
      iii. Tingkat: Menengah – Pemulihan data dan memperbaiki celah keamanan membutuhkan waktu, dan reputasi kampus juga bisa terkena dampak.
   c. Menerobos Pertahanan Sistem Informasi:
      i. Deskripsi: Upaya peretasan untuk menembus keamanan sistem informasi dan mengakses data.
      ii. Dampak: Gangguan fungsi sistem selama 5 jam hingga 1 hari.
      iii. Tingkat: Kecil – Peretasan dapat menyebabkan gangguan jangka pendek, tetapi jika segera diatasi, dampaknya bisa diminimalisir.

Tabel 3.7 mengklasifikasikan ancaman terhadap Sistem Informasi Akademik, Komputer Server, dan Data Nilai Mahasiswa berdasarkan dampak dan tingkat keparahan. Tindakan mitigasi risiko perlu difokuskan pada ancaman dengan dampak besar dan sangat besar, seperti pengolahan data ilegal atau akses tidak sah ke data, karena dampaknya bisa merusak reputasi serta operasional kampus dalam jangka panjang.

Tabel 3. *8* Identifikasi Kerentanan

No	Nama Aset	Kerentanan Aset
1	Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal	Kontrol standar dari *development tools*
		Pengaturan *User* Akses
		Pengaturan Anti Virus
		Update Sistem

2	Komputer Sever	Komputer tanpa pengawasan
		Software yang sudah terlalu lama
		Pemeliharaan yang kurang berkala
3	Data Nilai Mahsiswa	Lemahnya hak akses
		Pencurian Data
		Menerobos pertahanan sistem informasi

Tabel 3.8 mengidentifikasi aset-aset penting dari Politeknik Harapan Bersama Tegal dan kerentanan yang dimiliki oleh masing-masing aset tersebut. Kerentanan ini menggambarkan titik lemah atau celah dalam sistem yang dapat dieksploitasi oleh ancaman dan berpotensi menimbulkan gangguan terhadap keamanan, integritas, atau fungsionalitas aset. Berikut adalah penjelasan lebih lanjut mengenai aset dan kerentanannya:

1. Sistem Informasi Akademik Kampus Politeknik Harapan Bersama Tegal
   Kerentanan:
   a. Kontrol standar dari development tools:
      Deskripsi: Jika pengembangan sistem tidak menerapkan kontrol keamanan yang ketat dalam alat-alat pengembangannya (development tools), hal ini dapat membuka celah bagi ancaman seperti eksploitasi kelemahan dalam kode atau infrastruktur sistem.
   b. Pengaturan User Akses:
      Deskripsi: Sistem informasi dengan pengaturan hak akses pengguna yang lemah atau tidak terkontrol dengan baik dapat memungkinkan pengguna yang tidak berwenang untuk mengakses data atau fungsi sistem yang seharusnya dibatasi.
   c. Pengaturan Anti Virus:
      Deskripsi: Sistem yang tidak dilengkapi dengan perangkat lunak antivirus yang memadai atau tidak memperbarui definisi virus secara berkala menjadi rentan terhadap serangan malware, virus, dan program jahat lainnya.
   d. Update Sistem:
      Deskripsi: Sistem yang tidak diperbarui secara teratur akan rentan terhadap eksploitasi melalui celah keamanan yang telah diketahui di versi lama. Pembaruan perangkat lunak yang tidak dilakukan tepat waktu dapat mengakibatkan sistem lebih mudah diserang.
2. Komputer Server
   Kerentanan:
   a. Komputer tanpa pengawasan:
      Deskripsi: Server yang dibiarkan tanpa pengawasan fisik atau tidak dijaga dengan baik dapat menjadi target pencurian fisik, manipulasi, atau akses oleh pihak yang tidak berwenang.
   b. Software yang sudah terlalu lama:
      Deskripsi: Perangkat lunak yang sudah kadaluarsa atau tidak mendapatkan pembaruan secara teratur bisa mengandung kelemahan keamanan yang mudah dieksploitasi oleh peretas atau malware.
   c. Pemeliharaan yang kurang berkala:
      Deskripsi: Jika server tidak mendapatkan pemeliharaan rutin (misalnya pengecekan kondisi perangkat keras, pembaruan sistem, dan keamanan), maka performa dan keamanannya akan berkurang, meningkatkan risiko kegagalan sistem atau serangan.
3. Data Nilai Mahasiswa
   Kerentanan:
   a. Lemahnya hak akses:
      Deskripsi: Jika hak akses untuk mengelola atau melihat data nilai mahasiswa tidak diatur dengan baik, maka data sensitif ini dapat diakses oleh pihak yang tidak berwenang, meningkatkan risiko manipulasi atau pelanggaran privasi.
   b. Pencurian Data:
      Deskripsi: Data nilai mahasiswa yang tidak dilindungi dengan baik berpotensi dicuri oleh peretas atau orang dalam yang berniat menjual atau menyalahgunakan data tersebut.
   c. Menerobos pertahanan sistem informasi:
      Deskripsi: Sistem pertahanan yang lemah dalam sistem manajemen data mahasiswa bisa memungkinkan pihak yang tidak sah menerobos keamanan dan mengakses, memodifikasi, atau menghancurkan data yang ada.

4.2. ***Rancangan Kontrol Keamanan***

1. Pembatasan Hak Ases menggunakan matriks CRUD :

Proses Data / Entitas	Isi KRS	Periksa KRP	Cetak KRS
Mahasiswa	R	R	R
Matakuliah	R	R	R
KRS	CRUD	RU	R

MAHASISWA	
Mahasiswa	R
Matakuliah	R
KRS	CRUD

Proses Data / Entitas	Isi KRS	Periksa KRP	Cetak KRS
Mahasiswa	R	R	R
Matakuliah	R	R	R
KRS	RU	CRUD	R

DOSEN	
Mahasiswa	R
Matakuliah	R
KRS	CRUD

2. Pembatasan data Nilai Mahsiswa

Proses Data / Entitas	Isi Nilai Semester	Periksa Nilai Semester	Cetak Nilai Semester
Mahasiswa	R	R	R
Matakuliah	R	R	R
Nilai Semester	R	R	R

MAHASISWA	
Mahasiswa	R
Matakuliah	R
Nilai Semster	R

Proses Data / Entitas	Isi Nilai Semester	Periksa Nilai Semester	Cetak Nilai Semester
Mahasiswa	R	R	R
Matakuliah	R	R	R
Nilai Semester	CRUD	CRUD	R

DOSEN	
Mahasiswa	R
Matakuliah	R
Nilai Semester	CRUD

3. Pembatasan Data Kelas Perkuliahan

Proses Data / Entitas	Isi Kelas Perkuliahan	Periksa Kelas Perkuliahan	Cetak Kelas Perkuliahan
Mahasiswa	R	R	R
Matakuliah	R	R	R
Kelas Perkuliahan	R	R	R

MAHASISWA	
Mahasiswa	R
Matakuliah	R
Kelas Perkuliahan	R

IV. SIMPULAN

Kepatuhan di politeknik harapan bersama tegal belum diterapkan dan belum memenuhi aspek keamanan informasi. Kebijakan dan prosedur yang ada di politeknik harapan bersama tegal belum memenuhi aspek keamanan informasi.Sudah dibuat rekomendasi atau saran perbaikan terhadap kebijakan dan prosedur yang akan dibuat dapat meningkatkan keamanan informasi pada SIAKAD kampus politeknik harapan bersama tegal.

REFERENSI

[1] Ain, Alma Iftina Azzahra, Awalludiyah Ambarwati, and Lukman Junaedi. 2022. "Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1." *Jurnal Ilmu Komputer dan Bisnis* 13 (2a): 155–65. https://doi.org/10.47927/jikb.v13i2a.403.

[2] Ain, Alma Iftina Azzahra, Awalludiyah Ambarwati, and Lukman Junaedi. 2022. "Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1." *Jurnal Ilmu Komputer dan Bisnis* 13 (2a): 155–65. https://doi.org/10.47927/jikb.v13i2a.403.

[3] Ardius, Enggi, and Dedy Syamsuar. 2023. "ASSESSMENT RISK TERHADAP PENGGUNAAN SISTEM INFORMASI AKADEMIK UNIVERSITAS EA MENGGUNAKAN METODE ISO 27001." *Jurnal Teknologi Informasi Mura* 15 (1): 1–13. https://doi.org/10.32767/jti.v15i1.1948.

[4] Diansyah, Risnal. 2019. "Identifikasi Risiko Aset Informasi Pada Sistem Informasi Akademik." *JURNAL FASILKOM* 8 (1): 289–98. https://doi.org/10.37859/jf.v8i1.1197.

[5] Fahlepi, Ridho, Mona Fronita, Eki Saputra, Muhammad Luthfi Hamzah, and Arif Marsal. 2023. "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000" 7.

[6] Jakaria, Deni Ahmad, and R Teduh Dirgahayu. 2013. "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro."

[7] Malyana, Fauzi. n.d. "Analisis Manajemen Risiko Teknologi Informasi pada Sistem Informasi Akademik STMIK Sumedang Menggunakan ISO 31000."

[8] Nikmat, Arifatun. 2024. "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK) UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000: indo." *Jurnal Manajemen dan Teknologi Informasi* 14 (1): 49–58. https://doi.org/10.59819/jmti.v14i1.3321.

[9] Sihombing, Rossy Pratiwy, Amsal Sanjaya Tambun, Enjel Zetta R Nababan, Jowellyta Mega Kanaya Sibuea, and Ruby Albina Shafa. 2024. "Analisis Risiko Operasional Berbasis Pendekatan Enterprise Risk Management pada Coffee Shop 90 Derajat Medan." *Jurnal Ekonomi Bisnis, Manajemen dan Akuntansi (JEBMA)* 4 (1): 485–93. https://doi.org/10.47709/jebma.v4i1.3729.

[10] Wini Astuti, Riska, Reza Ade Putra, and Imamulhakim Syahid Putra. 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): 44–54. https://doi.org/10.51519/journalcisa.v4i1.337.