Identifikasi Risiko Keamanan Data Sistem Informasi Perpustakaan

Utin Kasma
STMIK Pontianak Jl. Merdeka No. 372; Telp 0561-735555
Jurusan Sistem Informasi
e-mail: utin_kasma@stmikpontianak.ac.id

Abstrak

Efektivitas pengelolaan risiko merupakan faktor krusial dalam keberhasilan penerapan sistem informasi di lingkungan sekolah, termasuk pada sistem informasi perpustakaan. Penelitian ini menggunakan metode OCTAVE Allegro untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi secara sistematis. Pendekatan yang digunakan bersifat kualitatif studi kasus, dengan pengumpulan data melalui wawancara, observasi, dan analisis dokumen. Hasil penelitian mengungkap beberapa risiko utama, seperti kebocoran data pribadi anggota, keterbatasan infrastruktur teknologi, serta rendahnya literasi keamanan informasi pada pengguna. Melalui OCTAVE Allegro, dirumuskan strategi mitigasi meliputi peningkatan pelatihan staf, revisi kebijakan keamanan, dan penguatan sistem perlindungan data. Temuan ini menegaskan pentingnya implementasi manajemen risiko yang menyeluruh dan berkelanjutan dalam melindungi aset informasi perpustakaan, termasuk data anggota, koleksi buku, dan transaksi peminjaman. Rekomendasi dari studi ini diharapkan menjadi acuan dalam memperkuat sistem identifikasi risiko guna mendukung pencapaian tujuan perpustakaan secara optimal.

Kata kunci: *Sistem Informasi Perpustakaan, Identifikasi Resiko, Octave Allegro.*

Abstract

The effectiveness of risk management is a crucial factor in the successful implementation of information systems in school environments, including library information systems. This study employed the OCTAVE Allegro method to systematically identify, assess, and manage information security risks. A qualitative case study approach was adopted, with data collected through interviews, field observations, and document analysis. The findings revealed several key risks, such as personal data breaches, limited technology infrastructure, and low user literacy in information security practices. Through the application of OCTAVE Allegro, effective mitigation strategies were formulated, including enhanced staff training on information security, revisions to security policies and procedures, and improvements to data protection systems. These findings highlight the importance of comprehensive and continuous risk management to safeguard library information assets, such as member data, book collections, and loan transaction records. The study's recommendations are expected to serve as a reference for libraries in strengthening risk identification systems to better support the achievement of their institutional goals.

Keywords*: Library Information System, Risk Identification, OCTAVE Allegro.*

1. PENDAHULUAN

Di tengah perkembangan teknologi digital saat ini, penggunaan sistem informasi menjadi kebutuhan penting bagi institusi pendidikan, termasuk dalam pengelolaan perpustakaan sekolah. Meskipun sistem informasi menawarkan banyak kemudahan, penggunaannya juga tidak lepas dari risiko yang dapat mengganggu keamanan data, merusak integritas informasi, dan menghambat operasional sekolah [1].Penerapan sistem dan teknologi informasi bertujuan utama untuk menyederhanakan proses pengolahan data guna menghadirkan layanan informasi yang efisien, cepat dan akurat [2]. Sistem informasi perpustakaan membantu dalam pencatatan koleksi buku, proses peminjaman, serta mempermudah akses informasi bagi anggota dan staff perpustakaan. Namun, penggunaan teknologi ini juga menghadirkan tantangan baru, khususnya dalam aspek keamanan data.

Informasi yang tersimpan dalam sistem informasi perpustakaan sekolah mencakup data sensitif seperti identitas pengguna, riwayat transaksi peminjaman dan pengembalian buku, informasi denda, hingga detail akun pengguna. Tanpa adanya sistem keamanan data yang memadai, informasi tersebut rentan terhadap risiko seperti pencurian, penyalahgunaan, atau kerusakan data. Kondisi ini berpotensi

mengganggu kelancaran proses pembelajaran dan dapat menurunkan kepercayaan pengguna terhadap sistem informasi yang digunakan. Risiko merupekan suatu kondisi ketidakpastian yang berpotensi menimbulkan kerugian [3]. Oleh karena itu proses analisis dan mitigasi risiko sangat dipelukan. Selanjutnya hasil dari analisis risiko tersebut akan menjadi dasar dalam menentukan strategi mitigasi yang tepat guna menurunkan potensi terjadinya risiko [4].

SMAS Bina Utama merupakan sekolah swasta yang telah menerapkan sistem informasi perpustakaan berbasis digital. Meskipun demikian, sampai saat ini belum dilakukan proses identifikasi risiko secara menyeluruh terkait keamanan data dalam sistem tersebut. Ketiadaan analisis dan penilaian risiko yang tepat membuat sistem informasi yang digunakan menjadi rentan terhadap ancaman cyber maupun kesalahan dalam operasional proses bisnisnya. Untuk memahami bagaimana manajemen risiko diterapkan dalam sistem informasi perpustakaan, diperlukan suatu penelitian yang mengkaji sejauh mana proses tersebut dilakukan dalam menganalisis, mengurangi, dan mengevaluasi risiko terhadap aset informasi perpustakaan [5]. Dalam manajemen risiko teknologi informasi, keberadaan kerangka kerja sangat penting untuk membantu organisasi mengidentifikasi kemungkinan risiko dan menetapkan strategi mitigasi yang dapat digunakan untuk mengendalikan risiko-resiko tersebut [6],

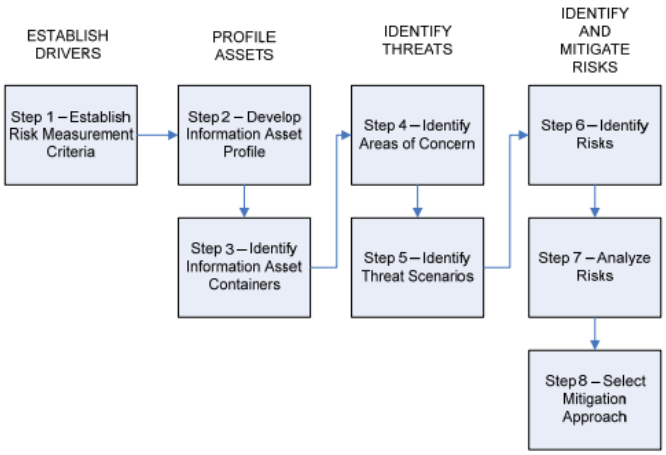
Dalam melakukan manajemen resiko, pendekatan yang digunakan adalah OCTAVE Allegro yaitu suatu metode evaluasi risiko yang telah disederhanakan. Metode ini mampu memberikan hasil yang andal tanpa memerlukan banyak waktu, sumber daya, ataupun pengalaman teknis yang mendalam dalam keamanan informasi dan manajemen risiko. [7]. OCTAVE Allegro merupakan pendekatan sistematis dalam manajemen risiko yang secara khusus menargetkan perlindungan terhadap aset informasi organisasi. Metode ini mengandalkan kolaborasi lintas fungsi di dalam organisasi guna memperoleh pemahaman menyeluruh mengenai risiko dan merancang mitigasi yang relevan. Selain itu, OCTAVE Allegro menyediakan berbagai instrumen pendukung seperti panduan pelaksanaan, lembar kerja, dan kuesioner untuk memperkuat proses identifikasi risiko [8].

Tujuan dari penelitian antara lain untuk mengidentifikasi berbagai potensi risiko keamanan data yang terdapat pada sistim informasi perpustakaan SMAS Bina Utama, serta memberikan gambaran awal mengenai fase-fase mitigasi yang memungkinkan dilakukan pihak sekolah dalam rangka untuk menambah tingkat keamanan sistem informasi perpustakaan yang diterapkan. Outcome dari penelitian ini nantinya dapat dijadikan rekomendasi bagi sekolah dalam meningkatkan perlindungan aset informasinya.

2. METODE PENELITIAN

Bentuk metode OCTAVE Allegro yang diterapkan dalam penelitian ini menitikberatkan pada perlindungan dan pengelolaan aset informasi organisasi. OCTAVE Allegro merupakan framework yang dikembangkan untuk proses identifikasi, analisis dan mengelola berbagai risiko keamanan aset informasi, khususnya dalam konteks organisasi skala kecil hingga skala menengah. OCTAVE Allegro merupakan pendekatan yang disederhanakan untuk menghasilkan efektifitas dalam proses penilaian resiko dengan penggunaan waktu yang lebih sedikit serta sumber daya yang relatif lebih rendah, serta tanpa memerlukan pengetahuan mendalam tentang keamanan sistem informasi atau pengalaman luas dalam manajemen risiko. [9].

Terdapat 4 fase yang dibagi dalam 8 langkah pada metode OCTAVE Allegro yang dipaparan melalui gambar dibawah ini [10]:



Gambar 1. Octave Allegro

Berikut adalah uraian dari masing-masing fase yang tercantum pada gambar di atas:

1. Penetapan Kriteria Evaluasi Risiko (Establish Risk Measurement Criteria)
   Dalam tahap Establish Risk Measurement Criteria, dilakukan dua aktivitas utama: identifikasi terhadap kriteria pengukuran risiko dan pemberian prioritas berdasarkan tingkat urgensi masing-masing, yang diukur menggunakan impact area ranking worksheet.
2. Pembutan Profil Aset (Develop an Information Asset Profile)
   Proses penyusunan profil aset mencakup sejumlah tahapan, antara lain identifikasi aset informasi, penilaian risiko terhadap aset yang berpotensi menimbulkan dampak negatif, pengumpulan data mengenai aset yang bersifat kritis, pendokumentasian aset, penjabaran ruang lingkup aset, penamaan aset, serta pencatatan keperluan dari keamanan aset informasi yang terkait.
3. Mengidentifikasi Kontainer dari Aset Informasi (Identify Information Asset Containers).
   Langkah ini mencakup identifikasi perlindungan yang diterapkan pada aset informasi beserta media penyimpanannya, serta analisis terhadap berbagai ancaman yang dapat memengaruhi kontainer penyimpanan aset informasi tersebut.
4. Mengindentifikasi Area Masalah (Identify Areas of Concern)
   Langkah ini merupakan inisiasi dari proces penyusunan profil aset informasi, yang diawali dengan analisis terhadap elemen-elemen ancaman melalui penelaahan berbagai kemungkinan yang dapat menimbulkan risiko terhadap aset imformasi.
5. Mengidentifikasi Skenario Ancaman (Identify Threat Scenarios)
   Terdapat dua langkah dalam mengenali skenario berbagai ancaman: yang pertama adalah penentuan skenario ancaman tambahan, sedangkan yang kedua adalah mengisi lembar kerja OCTAVE Allegro dalam konteks skenario ancaman yang bersifat umum dan tidak terperinci.
6. Mengidentifikasi Risiko (Identify Risks)
   Pada tahap ini, dilakukan penilaian terhadap dampak yang mungkin muncul dari masing-masing skenario ancaman yang telah dirancang sebelumnya. Penilaian dituangkan dalam Information Asset Risk Worksheets untuk mengidentifikasi konsekuensi konkret yang dapat terjadi jika ancaman terealisasi
7. Menganalisis Risiko (Analyze Risks)
   Skor risiko relatif dalam tahapan ini dihitung dengan mempertimbangkan dampak risiko terhadap organisasi dan membandingkannya dengan prioritas dari masing-masing area dampak.
8. Pemilihan Strategi Mitigasi Risiko (Select Mitigation Approach)
   Tahap kedelapan ini berfokus pada evaluasi risiko yang perlu dimitigasi serta penyusunan strategi mitigasinya. Proses ini melibatkan penentuan prioritas risiko, pemilihan pendekatan mitigasi yang sesuai untuk risiko-risiko signifikan berdasarkan berbagai faktor organisasi, serta rumusan dari strategi mitigasi yang disesuaikan dengan nilai aset terkait.

3. HASIL DAN PEMBAHASAN

Adapun tujuan dari penelitian yang dilakukan ini adalah guna mengidentifikasi resiko Keamanan Data pada Sistem Informasi Perpustakaan yang ada SMA Bina Utama Pontianak. Dari data yang sudah dikumpulkan melalui wawancara dengan petugas perpustakan, anggota perpustakaan serta kepala perpustakaan berupa berbagai kriteria pengukuran risiko yang dapat dilihat pada tabel 1 dan 2 berikut maka selanjutnya akan dilakukan penilaian resikonya berdasarkan tahapan yang terdapat pada metode OCTAVE Allegro.

1. Membangun Kriteria Pengukuran Risiko (Establish Risk Measurement Criteria).
   Proses wawancara pada tahap ini dilakukan dengan kepala perpustakaan, staf perpustakaan, dan anggota perpustakaan untuk merumuskan kriteria pengukuran risiko. Langkah awal mencakup penetapan kriteria tersebut serta pemberian prioritas pada area-area yang terdampak. Kriteria pengukuran risiko ini ditentukan berdasarkan hasil temuan dari wawancara yang telah dilakukan. Tabel berikut menyajikan kriteria yang digunakan dalam proses pengukuran resiko:

Tabel 1. Kriteria Pengukuran Resiko I

Impact Area	Low	Medium	High
Reputasi	Kepercayaan kepala perpustakaan, staff perpustakaan dan anggota terhadap sistem informasi perpustakaan sedikit sekali atau tidak terpengaruh	Kepercayaan kepala perpustakaan, staff perpustakaan dan anggota terhadap sistem informasi perpustakaan terpengaruh	Kepercayaan kepala perpustakaan, staff perpustakaan dan anggota terhadap sistem informasi perpustakaan sangat terpengaruh
Kehilangan user	Tidak ada dampak kehilangan user karena sistem informasi sekolah digunakan untuk internal sekolah		

Tabel 2. Kriteria Pengukuran Risiko II

Keuangan			
Impact Area	Low	Medium	High
Biaya Operasional	Kenaikan biaya operasional selama penerapan sistem informasi perpustakaan berada di bawah angka 2,5%	Kenaikan biaya operasional selama penerapan sistem informasi perpustakaan berada diantara 2,5% - 5 %	Kenaikan biaya operasional selama penerapan sistem informasi perpustakaan berada di atas angka 5%
Kerugian	Potensi kerugian tahunan akibat gangguan pada sistem informasi perpustakaan diperkirakan tidak melebihi 2 juta rupiah	Potensi kerugian tahunan akibat gangguan pada sistem informasi perpustakaan diperkirakan sekitar 2 - 5 juta rupiah	Potensi kerugian tahunan akibat gangguan pada sistem informasi perpustakaan diperkirakan melebihi 5 juta rupiah

Tahapan selanjutnya adalah menentukan prioritas terhadap area dampak yang paling signifikan. Skor yang paling tinggi untuk area yang dinilai memiliki tingkat pengaruh paling besar.

Tabel 3. Prioritas Area Dampak

Area yang berdampak	Prioritas
Keamanan dan kesehatan	1
Keuangan	2
Produktifitas	3
Reputasi dan kepercayaan anggota	4

2. Mengembangkan profil aset informasi (Develop an Information Asset Profile)
Tujuan dari langkah ini adalah untuk mengumpulkan dan mendokumentasikan data terkait profil aset informasi yang terdapat diperpustakaan dengan mencatat hasil identifikasi aset yang kritis kedalam worksheet (lembar kerja). Setiap profil aset informasi akan dilengkapi penjelasan mengapa aset tersebut dikategorikan sebagai kritis serta kebutuhan keamanan yang harus dipenuhi. Format berikut digunakan sebagai acuan dalam pengisian worksheet (lembar kerja) profil aset:

Tabel 4. Profil Aset Kritis I

Allegro Worksheet		Profil Aset Kritis
Aset Kritikal		Data anggota
Rasional Seleksi		Anggota sebagai pengguna sistem Informasi perpustakaan.
Deskripsi		Aset ini berisi informasi anggota seperti nomor anggota, nama anggota, alamat dan nomor telpon anggota.
Owner		Staff Perpustakaan
Security Requirements	Confidentiality	Hanya staff perpustakaan yang memiliki akses untuk menambahkan data anggota
	Integrity	Perubahan data anggota pada sistem informasi perpustakaan yang dilakukan oleh staff perpustakaan
	Availability	Aset informasi ini harus tersedia untuk Kepala Perpustakaan dan Staff Perpustakaan
Most Important Security Requirement		Integritas data anggota harus terjaga dengan baik, karena kesalahan pada data tersebut dapat mengakibatkan anggota tidak dapat melakukan transaksi peminjaman atau pengembalian buku

Karena berperan sebagai pengguna sistem informasi perpustakaan, data anggota dianggap sebagai aset yang sangat penting. Data ini mencakup nomor anggota, nama, alamat, dan nomor telepon. Hak akses terhadap aset tersebut dimiliki oleh staf perpustakaan. Berdasarkan hasil identifikasi, integritas merupakan kebutuhan keamanan utama untuk aset ini.

Tabel 5. Profil Aset Risiko II

Allegro Worksheet		Profil Aset Kritis
Aset Kritikal		Data Anggota
Rasional Seleksi		Anggota sebagai pengguna sistem informasi perpustakaan
Deskripsi		Aset ini berisi informasi anggota seperti nomor anggota, nama anggota, alamat dan nomor telpon anggota
Owner		Staff Perpustakaan
Security Requirements	Confidentiality	Hanya Staff Perpustakaan yang memiliki akses untuk menambahkan dan menghapus data anggota
	Integrity	Perubahan data anggota pada sistem informasi perpustakaan yang dilakukan oleh Sataff Perpustakaan
	Availability	Aset informasi ini harus tersedia untuk setiap anggota, Sataff perpustakaan dan Kepala perpustakaan
Most Important Security Requirement		Integritas data anggota harus terjamin, karena kesalahan pada data tersebut dapat berdampak pada penggunaan sistem informasi perpustakaan. Hal ini disebabkan oleh informasi penting yang tercakup dalam data anggota, seperti nomor anggota, nama, alamat, dan nomor telepon.

Data anggota dikategorikan sebagai aset kritis karena anggota merupakan pengguna utama sistem informasi perpustakaan. Data ini berisi informasi penting seperti nomor anggota, nama, alamat, dan nomor telepon. Akses terhadap aset tersebut hanya dimiliki oleh staf perpustakaan. Berdasarkan hasil identifikasi, integritas menjadi aspek keamanan yang paling utama.

3. Identify Information Asset Containers
Tahap ini melakukan identifikasi terhadap semua kontainer dari aset informasi. Kontainer tersebut umumnya dikelompokkan ke dalam beberapa kategori, seperti aset teknis, benda fisik

(misalnya dokumen kertas), dan individu yang memiliki peran penting dalam organisasi. Seluruh kontainer aset informasi ini dicatat pada tabel peta lingkungan risiko aset informasi sebagaimana berikut ini:

Tabel 6. Information Asset Risk Environment Map (Technical)

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	Owner
server	Perpustakaan
PC	Perpustakaan
Switch/Hubs	Perpustakaan
Database (data siswa, data guru dan data nilai)	Perpustakaan
Sistem operasi windows 10	Perpustakaan
External	
Container Description	Owner
Jaringan Internet	Telkom

Tabel 7. Information Asset Risk Environment Map (Physical)

Information Asset Risk Environment Map (physical)	
Internal	
Container Description	Owner
Folder file	Anggota Perpustakaan
Eksternal	
Container Description	Owner

4. Mengindentifikasi Area Masalah (Identify Areas of Concern)
   Langkah awal dalam tahap ini melibatkan analisis terhadap komponen ancaman dengan meninjau berbagai kondisi yang mungkin menimbulkan risiko terhadap aset informasi. Area-area prioritas yang relevan telah berhasil diidentifikasi dan dirinci sebagai berikut:

Tabel 8. Areas of Concern

Areas of concern	**Aset terkait**
Kesalahan input data Anggota	Sistem Informasi Perpustakaan
Listrik mati	Sistem Informasi Perpustakaan
Penyalahgunaan file folder back up data anggota dan buku	File folder

Area of concern mengacu pada deskripsi kondisi yang bisa berdampak terhadap aset informasi, dan ditentukan berdasarkan profil aset yang telah disusun sebelumnya. Contohnya, kesalahan saat memasukkan data anggota dapat memengaruhi aplikasi sebagai salah satu jenis aset teknis.

5. Penentuan Skenario Ancaman (Identify Threat Scenarios)
   Pada tahap kelima, dilakukan penyusunan skenario ancaman yang terperinci berdasarkan area of concern yang telah diidentifikasi sebelumnya. Setiap area tersebut kemudian didokumentasikan dalam lembar kerja OCTAVE Allegro yang memuat elemen-elemen penting seperti klasifikasi jenis ancaman, analisis dampak risiko, penilaian skor risiko relatif, serta strategi mitigasi yang dirancang. Struktur lembar kerja ini mencakup beberapa komponen utama, antara lain:
   a. Aset Informasi: Entitas informasi yang memiliki peran vital dalam kelangsungan operasional organisasi.
   b. Pelaku (Actor): Entitas atau pihak yang menjadi sumber munculnya ancaman.
   c. Cara Akses (Means): Metode yang digunakan pelaku untuk memperoleh akses terhadap aset, khususnya dalam konteks aktor manusia.
   d. Motivasi (Motive): Penilaian apakah tindakan ancaman dilakukan secara sengaja atau akibat kelalaian yang tidak disengaja (berlaku pada aktor manusia).
   e. Dampak (Outcome): Konsekuensi langsung dari pelanggaran terhadap aspek keamanan, yang dapat berupa pengungkapan, modifikasi, gangguan, atau kehilangan informasi.
   f. Kebutuhan Keamanan (Security Requirements): Aspek-aspek keamanan yang dilanggar akibat skenario ancaman yang terjadi.
   g. Probabilitas (Probability): Tingkat kemungkinan terjadinya ancaman diklasifikasikan ke dalam tiga kategori, yakni rendah (low), sedang (medium), dan tinggi (high).

   Dokumentasi rinci skenario ancaman disajikan dalam Tabel 9, yang menjadi instrumen evaluatif dalam pengelolaan risiko berbasis pendekatan OCTAVE Allegro.

Tabel 9. Information Asset Risk Worksheet I

Allegro Worksheet	**Information Asset Risk worksheet**
Aset Informasi	Sistem informasi perpustakaan
Areas of concern	Kesalahan dalam input data anggota
Actor (siapa yang melakukan area of concern atau ancaman?)	Staff perpustakaan
Means (bagaimana cara aktor melakukannya?)	Adanya kesalahan dalam input data anggota sehingga terdapat data yang tidak konsisten
Motive (Apa alasan aktor melakukannya?)	Human Error
Outcome (apa dampak terhadap aset informasi?)	Disclosure Modification Interruption Loss
Security Requirements (Security Requirements apa yang dilanggar?)	Anggota dapat mengakses dan memodifikasi data buku
Probability	Med - Karena kemungkinan kesalahan saat input data anggota sering terjadi

Dalam area of concern, duplikasi data anggota teridentifikasi sebagai akibat dari kesalahan manusia oleh staf perpustakaan. Insiden ini termasuk kategori modification karena melibatkan perubahan pada aset informasi. Pelanggaran ini berdampak pada prinsip integrity, mengganggu keakuratan dan keandalan data. Berdasarkan potensi kejadiannya, ancaman ini diklasifikasikan sebagai risiko sedang (medium risk).

Tabel 10. Information Asset Risk Worksheet 2

Allegro Worksheet	**Information Asset Risk worksheet**
Aset Informasi	Sistem informasi perpustakaan
Areas of concern	Listrik mati yang menghambat jalannya sistem informasi perpustakaan
Actor (siapa yang mel akukan area of concern atau ancaman?)	Pihak Luar
Means (bagaimana cara aktor melakukannya?)	Tidak adanya pasokan listrik sehingga menghambat jalannya sistem inmformasi perpustakaan
Motive (Apa alasan aktor melakukannya?)	Kesalahan teknis
Outcome (apa dampak terhadap aset informasi?)	Disclosure Modification Interruption Loss
Security Requirements (Security Requirements apa yang dilanggar?)	Aset ini harus tersedia
Probability	Low – kemungkinan terjadinya listrik mati jarang terjadi

Pada Tabel 10 diidentifikasi bahwa pemadaman listrik merupakan bentuk ancaman eksternal terhadap sistem informasi perpustakaan. Gangguan ini terjadi akibat terhentinya pasokan listrik, yang secara langsung menghambat operasional sistem dan menyebabkan layanan tidak dapat diakses oleh pengguna. Insiden ini dikategorikan sebagai pelanggaran terhadap aspek availability dalam prinsip keamanan informasi, karena keberlangsungan akses terhadap sistem menjadi terganggu. Pemadaman tersebut dipicu oleh kesalahan teknis dan tidak dilakukan secara sengaja oleh individu tertentu, kejadian ini lebih dipengaruhi oleh faktor eksternal yang tidak dapat diintervensi secara langsung oleh aktor internal. Meskipun memiliki dampak yang signifikan, seperti gangguan (interruption), perubahan (modification), kehilangan (loss), maupun pengungkapan informasi (disclosure), probabilitas terjadinya kejadian ini dinilai rendah, karena insiden pemadaman listrik jarang terjadi di lingkungan operasional sistem informasi perpustakaan.

6. Mengidentifikasi Risiko (Identify Risks).
   Proses ini bertujuan untuk mengkaji konsekuensi potensial yang mungkin terjadi jika suatu bentuk ancaman benar-benar terjadi. Hasil identifikasi risiko tersebut disajikan dalam Tabel 11 berikut:

Tabel 11. Identify Risks

No.	**Threat Scenarios**	**Konsekuensi**
1	Kesalahan input data peminjaman	Dibutuhkan tambahan waktu untuk menginputkan data transaksi peminjaman
2	Listrik mati	Sistem informasi perpustakaan terganggu karena tidak adanya pasokan listrik
3	Penyalahgunaan file folder back up data anggota dan buku	Dapat mempengaruhi reputasi dan kepercayaan karena data mengenai anggota atau buku terungkap

7. Menganalisis Risiko (Analyze Risks)
   Tahap ini diawali dengan melakukan peninjauan terhadap kriteria penilaian risiko untuk menilai sejauh mana dampak dari ancaman yang mungkin terjadi. Sebelum proses penilaian dilakukan, sangat penting untuk meninjau kembali kriteria yang telah dirumuskan pada langkah pertama aktivitas awal. Penentuan nilai dampak dilakukan dengan mengalikan nilai prioritas dengan skor kategori risiko yaitu Low (1), Medium (2), dan High (3).

Tabel 12. Impact Score

Areas of concern	Priority	Impact Score		
		Low (1)	Med (2)	High (3)
Keamanan dan kesehatan	1	1	2	3
Keuangan	2	2	4	6
Produktivitas	3	3	6	9
Reputasi dan kepercayaan anggota	4	4	8	12

Prioritas risiko ditentukan sejak tahap awal, di mana masing-masing area dampak telah diberi bobot tertentu. Skor dampak dihitung dengan mengalikan nilai prioritas dengan bobot kategori, yakni 1 untuk risiko rendah (low), 2 untuk sedang (medium), dan 3 untuk tinggi (high). Untuk menetapkan nilai dampak, dilakukan analisis terhadap tingkat pengaruh konsekuensi terhadap area yang terdampak, sesuai kriteria penilaian risiko pada tahap pertama. Total dari semua nilai ini digunakan untuk menghasilkan skor risiko relatif. Berikut ini adalah hasil analisis untuk area yang menjadi perhatian

Tabel 13. Analyze Risks I

Areas of concern	Risiko			
Kesalahan dalam input data peminjaman	Consequences	Dibutuhkan tambahan waktu untuk menginputkan data peminjaman yang sama		
	Severity	Impact Area	Impact Value	Score
		Keamanan dan kesehatan	Low	1
		Keuangan	Low	2
		Produktivitas	Med	6
		Reputasi dan kepercayaan pelanggan	Med	8
	Relative Risk Score			17

Kesalahan input data peminjaman, yang termasuk dalam area of concern, teridentifikasi memiliki kemungkinan terjadi yang tinggi. Berdasarkan evaluasi terhadap dampak menggunakan kriteria penilaian risiko, konsekuensi utama muncul pada aspek produktivitas serta reputasi dan kepercayaan pengguna, yang dikategorikan sebagai risiko sedang. Sementara itu, dampak terhadap keuangan, produktivitas tambahan, serta keamanan dan keselamatan berada pada tingkat risiko rendah. Berdasarkan hasil analisis tersebut, skor risiko relatif yang dihasilkan untuk insiden ini adalah sebesar 17.

Tabel 14. Analyze Risks II

Areas of concern	Risiko			
Listrik Mati	Consequences	Memberikan dampak gangguan atau terhentinya sistem informasi perpustakaan		
	Severity	Impact Area	Impact Value	Score
		Keamanan dan kesehatan	Low	1
		Keuangan	Low	2
		Produktivitas	Med	6
		Reputasi dan kepercayaan pelanggan	Med	8
	Relative Risk Score			17

Tabel 14 menyiratkan bahwa gangguan aliran listrik diidentifikasi sebagai faktor risiko yang berpotensi mengakibatkan terhentinya operasional sistem informasi perpustakaan. Kondisi ini dapat berdampak signifikan terhadap kontinuitas layanan dan efisiensi sistem. Berdasarkan hasil penilaian risiko, Implikasi terhadap tingkat produktivitas, serta terhadap reputasi dan tingkat kepercayaan pengguna, berada dalam klasifikasi dampak kategori sedang. Adapun pengaruh terhadap aspek keamanan dan kesehatan serta keuangan tergolong rendah (low). Total Skor Risiko Relatif yang diperoleh dari evaluasi ini senilai 17.

Tabel 15. Analyze Risks III

Areas of concern	Risiko			
Penyalahgunaan file folder back up data anggota dan buku	Consequences	Memberikan dampak gangguan atau terhentinya ssistem informasi perpustakaan		
	Severity	Impact Area	Impact Value	Score
		Keamanan dan kesehatan	Low	1
		Keuangan	Low	2
		Produktivitas	Med	6
		Reputasi dan kepercayaan pelanggan	Med	8
	Relative Risk Score			17

Penyalahgunaan folder backup yang berisi data anggota dan buku dalam area of concern berpotensi memengaruhi reputasi dan kepercayaan pengguna. Adapun dampak terhadap area lain tercatat pada tingkat risiko rendah. Area ini tercatat memiliki Relative Risk Score sebesar 17.

8. Pemilihan Strategi Mitigasi Risiko (Select Mitigation Approach)

Mitigasi risiko difokuskan pada risiko-risiko yang tergolong dalam kategori prioritas tinggi. Klasifikasi risiko dilakukan melalui pemanfaatan matriks risiko secara relatif (Relative Risk Matrix), seperti pada Tabel 16, yang menyajikan hubungan antara tingkat probabilitas dan skor risiko relatif.

Tabel 16. Relative Risk Matrix

Relative Risk Matrix			
Probability	**Risk Score**		
	30 to 45	**16 to 29**	**6 to 15**
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

Kategori probabilitas untuk masing-masing area of concern telah ditentukan pada langkah kelima dan digunakan sebagai dasar dalam merumuskan skenario risiko. Mengacu pada nilai probabilitas serta skor risiko relatif, risiko tersebut kemudian diklasifikasikan ke dalam pool 1, 2, 3, atau 4.

Tabel 17. Mitigation Approach

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

Strategi mitigasi yang diuraikan pada Tabel 17 ditetapkan berdasarkan klasifikasi kategori pool, yakni: Pool 1 (Mitigate), Pool 2 (Mitigate or Defer), Pool 3 (Mitigate or Accept), dan Pool 4 (Accept). Penentuan pendekatan mitigasi pada masing-masing area of concern dilakukan melalui analisis mendalam terhadap probabilitas kejadian dan skor risiko yang telah dihitung, serta diperkuat oleh hasil diskusi kolaboratif dengan pihak organisasi terkait:

Tabel 18. Pendekatan Mitigasi

No.	Areas of concern	Relative Risk Score	Proba bility	Pool	Pendekatan Mitigasi
1	Kesalahan input data peminjaman	17	Med	Pool 2	Mitigate
2	Listrik mati	17	Low	Pool 3	Accept
3	Penyalahgunaan file folder back up data anggota dan buku.	17	Med	Pool 3	Accept

Penentuan pendekatan mitigasi diawali dengan meninjau tingkat probabilitas risiko, kemudian melihat skor risiko relatif (relative risk score) untuk menentukan ke dalam pool mana risiko tersebut berada. Kesalahan input data peminjaman buku memiliki probabilitas sedang (medium) dan skor risiko relatif sebesar 17 termasuk dalam pool 2. Hal ini menunjukkan bahwa risiko tersebut perlu dimitigasi atau ditangani. Sementara itu, area of concern berupa pemadaman listrik juga memiliki skor 17, namun karena probabilitasnya rendah (Low), risiko ini ditempatkan dalam pool 3 dengan strategi mitigasi 'accept', menunjukkan bahwa risiko tersebut dinilai dapat diterima oleh organisasi tanpa perlunya langkah penanganan tambahan. Penyalahgunaan file cadangan yang memuat data anggota dan buku memperoleh nilai risiko sebesar 17 dengan tingkat kemungkinan sedang (medium), sehingga masuk dalam pool 3. Area of concern yang memerlukan mitigasi telah diuraikan sebagai beriku:

Tabel 19. Mitigasi I

Risk Mitigation	
Areas of Concern	**Kesalahan input data peminjaman buku**
Action	Mitigate
Container	Kontrol
Sistem Informasi perpustakaan	Mengintegrasikan fungsi pengecekan data duplikat dengan identifikasi terhadap entri data yang telah ada di sistem

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa dampak paling dominan tercermin pada aspek reputasi organisasi serta tingkat kepercayaan pengguna, efisiensi produktivitas, stabilitas finansial, dan keselamatan serta kesehatan kerja. Aset-aset yang tergolong kritis meliputi database, server, switch, dan folder berisi file. Penelitian ini mengidentifikasi tiga area of concern, yaitu kesalahan dalam input data peminjaman dengan skor risiko relatif sebesar 17 yang digambarkan pada tabel Analyze Risk I. Sementara itu untuk gangguan akibat pemadaman listrik juga memiliki skor risiko relatif sebesar 17 yang digambarkan pada tabel Analyze Risk II. Sedangkan penyalahgunaan folder cadangan data anggota dan buku yang juga memiliki skor relatif sebesar 17 digambarkan dalam tabel Analyze Risk III. Dari ketiga risiko tersebut, dua dikategorikan dalam pendekatan mitigasi "accept", sedangkan satu lainnya memerlukan pendekatan "mitigate".

5. SARAN

Sebagai tindak lanjut dari penelitian ini, direkomendasikan agar SMA Bina Utama mempertimbangkan berbagai potensi risiko serta menerapkan langkah-langkah preventif demi menjaga keamanan sistem informasi perpustakaan. Untuk pengembangan penelitian ke depan, disarankan agar analisis risiko diperluas ke seluruh aset informasi yang dimiliki oleh sekolah, khususnya dalam aspek keamanan data.

UCAPAN TERIMA KASIH

Saya ingin menyampaikan apresiasi yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam penyusunan penelitian ini.

DAFTAR PUSTAKA

[1] Kasma, U. (2024). Manajemen Risiko Sistem Informasi Akademik pada SMA Panca Setya Menggunakan Metoda Octave Allegro, in SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi, Vol. 2, No. 3. https://doi.org/10.59841/saber.v2i3.1525

[2] Widayanti, T. (2019). Analisis Teknologi Informasi Pengolahan Data Menggunakan Framework COBIT, in SENSITIF (Seminar Nasional Sistem Informasi dan Teknik Informatika), Makasar.

[3] Joshua Jenriwan L Tobing, A. K. P. (2015). Analisis Manajemen Resiko untuk Evaluasi Asset menggunakan Metode Octave Allegro. In Expert- Jurnal Manajemen Sistem Informasi Dan Teknologi, Bandar Lampung.

[4] Ramadhintia, R., Bisma, R. (2021). Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik, In JEISBI (Journal of Emerging Information Systems and Business Intelligence), Vol. 02, No. 02, Surabaya.

[5] Valena, D.S., Prabowo, R., Irawati, A.R., Aristoteles (2019). Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30, In Jurnal Komputasi, (Vol. 7, No. 1), Bandar Lampung.

[6] Megawati., Kazmaini, M. (2018), Analisa Manajemen Resiko Sistem Informasi Perpustakaan Menggunakan Cobit 4.1 Pada Domain Po9, In Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, (Vol. 4, No. 1, Hal. 73-76). E-ISSN 2502-8995, p-ISSN 2460-8181.

[7] Keating,C.G. (2014). Validating the OCTAVE Allegro Information System Risk Assessment Methodology: A Case Study. NSUWorks. Nova Southeastern University.

[8] Wicaksono, S.R., Rizka, C.L.D., & Immanuel., G.A. (2019). Risk Assessment Menggunakan Pendekatan OCTAVE Allegro (Studi kasus: Schoology.com). In Information Communication & technology (Vol. 18, No.2, pp.123-129). https://DOI: 10.36054/jict-ikmi.v18i2.42.

[9] Haeruddin. (2019). Mapping Information Asset Profile In The Implementation Of Risk Management Information System Using Octave Allergo. In JITE (Journal of Informatics and Telecommunication Engineering), (Vol 3, No. 1, pp. 67-75). https://DOI: 10.31289/jite.v3i1.2601.

[10] Ronald, L.K., Russell, D.V. (2006). The CISSP Prep Guide -Mastering the Ten Domains of Computer Security. CA: Wiley Computer Publishing John Wiley & Sons, Inc.