SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi
Vol. 2, No. 3 Juli 2024
e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal 327-340
DOI: https://doi.org/10.59841/saber.v2i3.1525
Available online at: https://jurnal.stikes-ibnusina.ac.id/index.php/SABER

Manajemen Risiko Sistem Informasi Akademik pada SMA Panca Setya Menggunakan Metoda Octave Allegro

Utin Kasma
STMIK Pontianak

Jl. Merdeka, No. 372
utin.kasma@yahoo.co.id

Abstract. *The success of implementing information systems in a school environment is significantly influenced by effective risk management. This research aims to implement the OCTAVE Allegro method to identify, assess, and manage risks associated with the information system at Panca Setya High School. The OCTAVE Allegro method was chosen for its systematic and structured approach to information security risk management. This research adopts a qualitative approach using a case study method. Data were collected through in-depth interviews with school staff, direct observations, and document analysis. The findings revealed several key risks threatening the information system at Panca Setya High School, including threats to student data confidentiality, weaknesses in technological infrastructure, and a lack of security awareness among users. Through the implementation of the OCTAVE Allegro method, this research successfully identified effective mitigation strategies, such as enhancing information security training for staff, updating security policies and procedures, and strengthening data protection technologies. The conclusion of this research highlights that comprehensive and sustainable risk management is crucial for protecting the school's information assets and ensuring operational continuity. The recommendations from this study are intended to assist the management of Panca Setya High School in enhancing their information system risk management, thereby better supporting the achievement of educational objectives.*

Keywords: *Risk Management, Information System, OCTAVE Allegro.*

Abstrak. Keberhasilan implementasi sistem informasi di lingkungan sekolah sangat dipengaruhi oleh manajemen risiko yang efektif. Penelitian ini bertujuan untuk menerapkan metode OCTAVE Allegro dalam mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan sistem informasi di SMA Panca Setya. Metode OCTAVE Allegro dipilih karena kemampuannya dalam memberikan pendekatan sistematis dan terstruktur dalam manajemen risiko keamanan informasi. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Data diperoleh melalui wawancara mendalam dengan staf sekolah, observasi langsung, dan analisis dokumen. Hasil penelitian mengungkapkan bahwa terdapat beberapa risiko utama yang mengancam sistem informasi di SMA Panca Setya, termasuk ancaman terhadap kerahasiaan data siswa, kelemahan dalam infrastruktur teknologi, dan kurangnya kesadaran keamanan di kalangan pengguna. Melalui penerapan metode OCTAVE Allegro, penelitian ini berhasil mengidentifikasi langkah-langkah mitigasi yang efektif, seperti peningkatan pelatihan keamanan informasi untuk staf, pembaruan kebijakan dan prosedur keamanan, serta penguatan teknologi perlindungan data. Kesimpulan dari penelitian ini menunjukkan bahwa penerapan manajemen risiko yang komprehensif dan berkelanjutan sangat penting untuk melindungi aset informasi sekolah dan memastikan kontinuitas operasional. Rekomendasi yang dihasilkan dari penelitian ini diharapkan dapat membantu pihak manajemen SMA Panca Setya dalam meningkatkan manajemen risiko sistem informasi mereka, sehingga mampu mendukung pencapaian tujuan pendidikan dengan lebih baik

Kata kunci: Manajemen Resiko, Sistem Informasi, Octave Allegro.

LATAR BELAKANG

Received: Mei 12, 2024; Revised: Juni 18, 2024;Accepted: Juli 6, 2024; Published: Juli 8, 2024;
* **Utin Kasma,** utin.kasma@yahoo.co.id

Dalam era digital saat ini, sistem informasi telah menjadi bagian integral dari operasional sekolah, memungkinkan pengelolaan data akademik, administrasi, dan keuangan secara efisien dan efektif. Namun, penggunaan sistem informasi juga membawa berbagai risiko yang dapat mengancam keamanan, integritas data, dan kelangsungan operasional sekolah. Risiko-risiko ini termasuk serangan siber, kegagalan sistem, kesalahan manusia, dan ancaman lainnya yang dapat merugikan institusi pendidikan. Dalam upaya untuk mengendalikan dan mengurangi kerugian yang terjadi, dibutuhkan manajemen risiko terhadap keamanan informasi yang telah dihasilkan (Prihatini, dkk, 2021).

Sebagai institusi pendidikan yang telah mengadopsi sistem informasi dalam operasional sehari-hari, SMA Panca Setya menghadapi tantangan dalam mengelola risiko-risiko ini. Meskipun sudah ada upaya untuk melindungi sistem informasi, belum ada pendekatan manajemen risiko yang terstruktur dan komprehensif di sekolah ini. Oleh karena itu, diperlukan metode yang mampu mengidentifikasi, menilai, dan mengelola risiko secara efektif.

Metode OCTAVE Allegro adalah salah satu pendekatan manajemen risiko yang berfokus pada keamanan informasi dan dirancang untuk membantu organisasi dalam mengidentifikasi dan mengelola risiko terhadap aset informasi mereka. Pendekatan ini menekankan pada partisipasi aktif dari berbagai pihak dalam organisasi untuk mengidentifikasi risiko secara mendalam dan mengembangkan strategi mitigasi yang sesuai. Metode ini berfokus pada aset informasi organisasi. OCTAVE Allegro telah dilengkapi dengan guidance, lembar kerja hingga kuesioner (Wicaksono, dkk, 2019).

Penelitian ini bertujuan menerapkan metode OCTAVE Allegro dalam manajemen risiko sistem informasi di SMA Panca Setya untuk mendapatkan gambaran profil risiko dan langkah mitigasi yang efektif. Diharapkan hasil penelitian ini dapat meningkatkan keamanan dan keberlanjutan operasional sistem informasi di SMA Panca Setya, serta menjadi acuan bagi institusi pendidikan lainnya dalam mengelola risiko sistem informasi mereka.

Penelitian ini memberikan kontribusi baru dalam manajemen risiko sistem informasi di sekolah menengah dengan menerapkan dan mengadaptasi metode OCTAVE Allegro, yang umumnya digunakan di industri dan sektor bisnis. Penelitian ini menunjukkan bagaimana metode tersebut dapat disesuaikan untuk kebutuhan institusi

pendidikan seperti SMA Panca Setya. Hasil penelitian berupa strategi manajemen risiko yang spesifik, termasuk peningkatan kesadaran keamanan di kalangan staf dan siswa, pembaruan kebijakan keamanan informasi, serta penguatan infrastruktur teknologi.

Dengan mengadopsi metode OCTAVE Allegro, SMA Panca Setya dapat mengelola risiko sistem informasi secara komprehensif dan terstruktur. Ini akan meningkatkan keamanan dan integritas data, serta memastikan operasional sekolah berjalan efisien tanpa gangguan yang signifikan. Penelitian ini sangat relevan untuk memberikan solusi praktis dan strategis bagi manajemen risiko sistem informasi di sekolah. Tujuannya adalah untuk mengidentifikasi, menilai, dan mengelola risiko terkait sistem informasi di SMA Panca Setya menggunakan metode OCTAVE Allegro.

KAJIAN TEORITIS

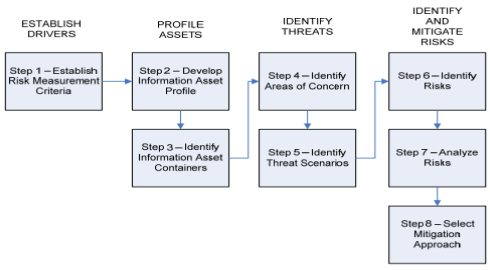
Manajemen risiko sistem informasi adalah proses identifikasi, penilaian, dan pengendalian risiko yang terkait dengan penggunaan teknologi informasi dalam organisasi. Proses ini bertujuan untuk melindungi aset informasi dari berbagai ancaman yang dapat mengganggu operasional organisasi, mengakibatkan kerugian finansial, atau merusak reputasi. Manajemen risiko sistem informasi adalah proses identifikasi, penilaian, dan pengendalian risiko yang terkait dengan penggunaan teknologi informasi dalam organisasi. Proses ini bertujuan untuk melindungi aset informasi dari berbagai ancaman yang dapat mengganggu operasional organisasi, mengakibatkan kerugian finansial, atau merusak reputasi (Bavian, 2020). Prinsip utama keamanan sistem informasi terdiri dari confidentiality (kerahasiaan), integrity (integritas) dan availability (ketersediaan) atau sering disingkat CIA (Ronald & Russell, 2006).

OCTAVE Allegro adalah proses yang disederhanakan dengan memberikan hasil penilaian risiko yang kuat dengan investasi waktu dan sumber daya yang lebih kecil dan tidak memerlukan keamanan sistem informasi yang luas atau pengalaman manajemen risiko (Haeruddin. (2019). OCTAVE Allegro telah dilengkapi dengan guidance, lembar kerja hingga kuesioner (Ronald & Russell, 2006). OCTAVE Allegro adalah proses yang disederhanakan dengan memberikan hasil penilaian risiko yang kuat dengan investasi waktu dan sumber daya yang lebih kecil dan tidak memerlukan keamanan sistem informasi yang luas atau pengalaman manajemen risiko (Keating, 2014).

METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode OCTAVE Allegro. Metode ini berfokus pada aset informasi organisasi. OCTAVE Allegro

dikembangkan oleh tim CERT® Survivable Enterprise Management dengan tujuan utama untuk membantu organisasi memastikan bahwa kegiatan keamanan informasi mereka selaras dengan tujuan organisasi . OCTAVE Allegro terdiri dari 8 langkah yang dibagi dalam 4 fase yang dapat dilihat pada gambar 1 berikut (Ronald & Russell, 2006):



Gambar 1 : Octave Allegro

Gambar diatas dapat dijelaskan sebagai berikut :

A. Establish Risk Measurement Criteria (Membangun Kriteria Pengukuran Risiko).

Untuk membuat kriteria pengukuran risiko terdapat 2 aktivitas, diawali dengan identifikasi kriteria pengukuran risiko dan memberikan prioritas sesuai tingkat kepentingan menggunakan impact area ranking worksheet.

B. Develop an Information Asset Profile (Pembutan Profil Aset)

Pembuatan profil aset melibatkan beberapa aktivitas, yaitu mengidentifikasi aset informasi, menilai risiko pada aset yang berdampak buruk, mengumpulkan informasi tentang aset kritis, mendokumentasikan aset tersebut, mendeskripsikan ruang lingkup aset, memberikan nama aset, dan mencatat kebutuhan keamanan informasi.

C. Identify Information Asset Containers (Mengidentifikasi Kontainer dari Aset Informasi).

Langkah ini mengidentifikasi keamanan dan penyimpanan aset informasi yang dilindungi serta ancaman terhadap kontainer dari aset informasi.

D. Identify Areas of Concern (Mengindentifikasi Area Masalah)

Pada langkah keempat memulai proses pengembangan profil aset informasi. Langkah ini mulai membahas komponen ancaman dari risiko dengan memikirkan mengenai kemungkinan kondisi yang dapat mengancam aset informasi.

E. Identify Threat Scenarios (Mengidentifikasi Skenario Ancaman)

Dalam mengidentifikasi skenario ancaman terdapat 2 aktivitas, diawali dengan mengidentifikasi skenario ancaman tambahan. Aktivitas dua melengkapi lembar kerja OCTAVE Allegro untuk skenario ancaman yang umum.

F. Identify Risks (Mengidentifikasi Risiko)

Pada langkah keenam yaitu menentukan dampak dari skenario ancaman yang telah didokumentasikan pada Information Asset Risk Worksheets. Dari skenario yang telah dibuat akan ditemukan konsekuensi jika ancaman tersebut terjadi.

G. Analyze Risks (Menganalisis Risiko)

Dalam aktivitas ini akan menghasilkan skor risiko relative yang diperoleh dengan mempertimbangkan sejauh mana konsekuensi risiko mempengaruhi organisasi dibandingkan dengan kepentingan relatif dari berbagai bidang dampak.

H. Select Mitigation Approach

Pada langkah 8 mempertimbangkan risiko mana yang perlu mitigasi dan strategi mitigasi. Ini dilakukan dengan memprioritaskan risiko, memutuskan pendekatan untuk memitigasi risiko yang penting berdasarkan sejumlah faktor organisasi, dan mengembangkan strategi mitigasi yang mempertimbangkan nilai aset.

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk merencanakan manajemen risiko sistem informasi sekolah pada SMA Panca Setya. Data yang dikumpulkan kemudian dinilai risikonya menggunakan metode OCTAVE Allegro, yang terdiri dari delapan langkah berikut ini :

A. Establish Risk Measurement Criteria (Membangun Kriteria Pengukuran Risiko).

Pada tahap ini, wawancara dilakukan dengan guru dan operator IT untuk menetapkan kriteria pengukuran risiko. Langkah pertama melibatkan penentuan kriteria pengukuran risiko dan menetapkan prioritas pada area dampak. Kriteria pengukuran risiko dibuat berdasarkan panduan dan hasil wawancara. Berikut adalah kriteria pengukuran risiko:

Tabel 1 Kriteria Pengukuran Risiko 1

Reputasi dan Kepercayaan Pelanggan			
Impact Area	Low	Medium	High
Reputasi	Kepercayaan guru dan siswa terhadap sistem informasi sekolah sedikit sekali atau tidak terpengaruh	Kepercayaan guru dan siswa terhadap sistem informasi sekolah terpengaruh	Kepercayaan guru dan siswa terhadap sistem informasi sekolah sangat terpengaruh
Kehilangan user	Tidak ada dampak kehilangan user karena sistem informasi sekolah digunakan untuk internal sekolah		

Tabel 2 Kriteria Pengukuran Risiko 2

Keuangan			
Impact Area	Low	Medium	High
Biaya Operasional	Peningkatan biaya operasional saat implementasi sistem informasi sekolah kurang dari 2.5%	Peningkatan biaya operasional saat implementasi sistem informasi sekolah sebesar 2.5% - 5%	Peningkatan biaya operasional saat implementasi sistem informasi sekolah lebih dari 5%
Kerugian	Kurang dari 2 juta kerugian tahunan jika sistem informasi sekolah terjadi gangguan	Antara 2 juta – 5 juta kerugian tahunan jika sistem informasi sekolah terjadi gangguan	Lebih dari 5 juta kerugian tahunan jika sistem informasi sekolah terjadi gangguan

Langkah berikutnya adalah menetapkan prioritas untuk area dampak yang paling penting. Nilai tertinggi akan diberikan pada area dampak yang dianggap paling berpengaruh.

Tabel 3 Prioritas Area Dampak

Area yang berdampak	**Prioritas**
Keamanan dan kesehatan	1
Keuangan	2
Keuangan	3
Reputasi dan kepercayaan siswa	4

B. Develop an Information Asset Profile (Mengembangkan profil aset informasi)

Pada langkah ini akan didata profil aset informasi yang dimiliki organisasi dengan mendokumentasikan hasil profil aset kritis ke lembar kerja. Profil aset ini dilengkapi dengan alasan rasionalis aset kritis dan persyaratan kemanan aset tersebut. Pengisian lembar kerja profil aset sebagai berikut:

Tabel 4 Profil Aset Kritis I

Allegro Worksheet		**Profil Aset Kritis**
Aset Kritikal		Data Guru
Rasional Seleksi		Guru sebagai pengguna sistem Informasi Sekolah.
Deskripsi		Aset ini berisi informasi guru seperti nama, nomer induk pegawai, mata pelajaran, jadwal ujian
Owner		Operator IT
Security Requirements	Confidentiality	Hanya operator IT yang memiliki akses untuk menambahkan data guru
	Integrity	Perubahan data guru pada sistem informasi sekolah yang dilakukan oleh operator IT
	Availability	Aset informasi ini harus tersedia untuk setiap guru dan operator IT
Most Important Security Requirement		Integrity Data guru harus sesuai karena jika terjadi kesalahan guru tidak dapat input soal ke dalam sistem informasi sekolah

Data guru dianggap sebagai aset kritis karena guru merupakan pengguna sistem informasi sekolah dan data tersebut mencakup informasi seperti nama, nomor induk pegawai, mata pelajaran, dan jadwal mengajar. Pada aset kritis ini, yang memiliki hak akses adalah

operator IT, setelah dilakukan identifikasi, persyaratan keamanan yang paling penting adalah integritas.

Tabel 5 Profil Aset Risiko 2

Allegro Worksheet		**Profil Aset Kritis**
Aset Kritikal		Data Siswa
Rasional Seleksi		Siswa sebagai pengguna sistem informasi sekolah
Deskripsi		Aset ini berisi informasi siswa seperti nama, nomer induk siswa, kelas, tahun angkatan
Owner		Operator IT
Security Requirements	Confidentiality	Hanya operator IT yang memiliki akses untuk menambahkan data siswa
	Integrity	Perubahan data siswa pada sistem informasi sekolah yang dilakukan oleh operator IT
	Availability	Aset informasi ini harus tersedia untuk setiap siswa, guru, dan operator IT
Most Important Security Requirement		Integrity Data siswa harus sesuai jika terjadi kesalahan dapat mempengaruhi penggunaan sistem informasi sekolah tersebut, karena dalam data siswa mencakup nama, nomor induk siswa, kelas, mata pelajaran, dan alamat siswa.

Data siswa dianggap sebagai aset kritis karena siswa adalah pengguna dari sistem informasi sekolah dan data tersebut mencakup informasi seperti nama, nomor induk siswa, kelas, mata pelajaran dan alamat siswa. Akses terhadap aset kritis ini dimiliki oleh operator IT, dan setelah dilakukan identifikasi, persyaratan keamanan yang paling penting adalah integritas.

C. Identify Information Asset Containers

Pada langkah ini, setiap kontainer aset informasi diidentifikasi. Kontainer biasanya dikategorikan sebagai beberapa jenis aset teknis, objek fisik (seperti kertas), dan individu penting bagi organisasi. Setiap kontainer aset ini didokumentasikan dalam tabel peta lingkungan risiko aset informasi sebagai berikut:

Tabel 6 Information Asset Risk Environment Map (Technical)

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	Owner
server	Sekolah
PC	Sekolah
Switch/Hubs	Sekolah
Database (data siswa, data guru dan data nilai)	Sekolah
Sistem operasi windows 10	Sekolah
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	Guru
Eksternal	
Container Description	Owner

D. Identify Areas of Concern (Mengindentifikasi Area Masalah)

Pada langkah keempat ini, pembahasan dimulai dengan meninjau komponen ancaman, yaitu mempertimbangkan berbagai kondisi atau situasi yang dapat mengancam aset informasi. Berikut adalah area-area yang menjadi perhatian yang telah diidentifikasi:

Tabel 8 Areas Of Concern

Areas of concern	**Aset terkait**
Kesalahan input data soal	Sistem Informasi
Listrik mati	Sistem Informasi
Penyalahgunaan file folder back up data siswa dan guru	File folder

Area of concern adalah pernyataan deskriptif yang menggambarkan kondisi yang dapat mempengaruhi aset informasi. Area ini diidentifikasi berdasarkan profil aset pada langkah sebelumnya. Misalnya, dalam situasi pertama, kesalahan input data soal mempengaruhi aset aplikasi yang termasuk dalam aset teknis.

E. Identify Threat Scenarios (Mengidentifikasi Skenario Ancaman)

Pada langkah kelima, area of concern dikembangkan menjadi skenario ancaman. Setiap area diidentifikasi dan didokumentasikan dalam lembar kerja OCTAVE Allegro. Lembar kerja ini mencatat ancaman, dampak terkait risiko, menghitung skor risiko relatif, dan mencatat rencana mitigasi. Lembar kerja risiko aset informasi ini terdiri dari:

1. Aset informasi :aset yang penting bagi organisasi.
2. Actor :siapa pelaku dari ancaman tersebut .
3. Means : bagaimana cara pelaku mengakses aset tersebut (hanya berlaku untuk human actor)
4. Motive : Apa maksud dari pelaku terhadap ancaman apakah dilakukan secara sengaja atau tidak sengaja (hanya berlaku untuk human actor)
5. Outcome : hasil langsung dari pelanggaran persyaratan keamanan terhadap aset terdapat 4 pilihan (disclosure, modification, interruption,loss)

6. Security requirements: apa pelanggaran persyaratan keamanan yang dilanggar. 7. Probability : kemungkinan terjadinya ancaman tersebut termasuk pada kategori low, medium atau high

Berikut lembar kerja yang berisi threat scenario :

Tabel 9 Information Asset Risk Worksheet I

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

Pada areas of concern, kesalahan input data nilai yang sama dilakukan oleh guru karena adanya human error. Dampak yang ditimbulkan adalah modification karena terjadi perubahan pada aset informasi. Pelanggaran persyaratan keamanan termasuk dalam integrity karena informasi mengenai nilai harus benar. Kemungkinan terjadinya ancaman ini berada pada kategori medium.

Tabel 10 Information Asset Risk Worksheet 2

Allegro Worksheet	**Information Asset Risk worksheet**
Aset Informasi	Sistem informasi sekolah
Areas of concern	Listrik mati yang menghambat jalannya sistem informasi sekolah
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 sekolah
Motive (Apa alasan aktor melakukannya?)	Sengaja
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 area of concern, pemadaman listrik merupakan tindakan yang dilakukan oleh pihak luar. Ancaman ini muncul karena adanya gangguan yang menyebabkan pemadaman listrik, dengan dampak terhadap aset berupa gangguan karena aplikasi menjadi tidak tersedia atau tidak dapat digunakan, melanggar persyaratan keamanan ketersediaan. Kemungkinan ancaman ini dikategorikan sebagai rendah karena pemadaman listrik jarang terjadi.

F. Identify Risks (Mengidentifikasi Risiko)

Pada langkah ini akan dilakukan identifikasi konsekuensi yang mungkin timbul jika ancaman terjadi. Berikut adalah hasil dari identifikasi risiko:

Tabel 11 Identify Risks

No.	Threat Scenarios	Konsekuensi
1	Kesalahan input data nilai	Dibutuhkan tambahan waktu untuk menginputkan nilai yang sama
2	Listrik mati	Sistem informasi sekolah terganggu karena tidak adanya pasokan listrik
3	Penyalahgunaan file folder back up data siswa dan guru	Dapat mempengaruhi reputasi dan kepercayaan karena data mengenai siswa atau guru terungkap

G. Analyze Risks (Menganalisis Risiko)

Langkah ketujuh dimulai dengan meninjau kriteria pengukuran risiko untuk mengukur dampak yang ditimbulkan oleh ancaman. Sebelum melakukan penilaian, penting untuk mengulas kembali kriteria pengukuran risiko yang telah ditetapkan pada langkah 1 aktivitas 1. Dalam menentukan nilai dampak, nilai prioritas dikalikan dengan nilai 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 siswa	4	4	8	12

Nilai prioritas dapat ditinjau kembali dari langkah pertama di mana area dampak diberi nilai. Nilai skor dampak (impact score) diperoleh dengan mengalikan nilai prioritas dengan nilai setiap kategori, seperti kategori rendah (low) bernilai 1, kategori sedang (medium) bernilai 2, dan kategori tinggi (high) bernilai 3. Untuk mendapatkan nilai dampak (impact value), perlu dipertimbangkan sejauh mana konsekuensi tersebut mempengaruhi area dampak berdasarkan kriteria pengukuran risiko pada langkah pertama. Nilai tersebut kemudian dijumlahkan untuk mengetahui skor risiko relatif (relative risk score). Hasil dari analisis risiko untuk area of concern yang telah diidentifikasi adalah sebagai berikut:

Tabel 13 Analyze Risks I

Areas of concern	Risiko

Kesalahan dalam input nilai	Consequences	Dibutuhkan tambahan waktu untuk menginputkan nilai 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

Pada area of concern, kesalahan input data nilai setelah dianalisis merupakan kejadian dengan kemungkinan besar terjadi. Setelah mempertimbangkan konsekuensi menggunakan kriteria pengukuran risiko, area dampak yang terpengaruh adalah produktivitas serta reputasi dan kepercayaan pelanggan dalam kategori sedang (medium). Selain itu, area keuangan, produktivitas, serta keamanan dan kesehatan berada dalam kategori rendah (low). Area of concern ini menghasilkan Skor Risiko Relatif (Relative Risk Score) sebesar 17.

Tabel 14 Analyze Risks II

Areas of concern	**Risiko**			
Listrik Mati	Consequences	Memberikan dampak gangguan atau terhentinya sistem informasi sekolah		
	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

Pada area of concern, pemadaman listrik dapat menyebabkan layanan sistem informasi sekolah terhenti. Hal ini dapat mengganggu operasional aplikasi, sehingga setelah mempertimbangkan konsekuensi tersebut menggunakan kriteria pengukuran risiko, area dampak pada produktivitas serta reputasi dan kepercayaan pelanggan masuk dalam kategori sedang (medium). Sedangkan, keamanan dan kesehatan serta keuangan berada dalam kategori rendah (low). Area of concern ini menghasilkan Skor Risiko Relatif (Relative Risk Score) sebesar 17.

Tabel 15 Analyze Risks III

Areas of concern	**Risiko**			
Penyalahgunaan file folder back up data siswa dan guru	Consequences	Memberikan dampak gangguan atau terhentinya aplikasi ujian online		
	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

Pada area of concern, penyalahgunaan folder cadangan data guru dan siswa memiliki konsekuensi yang mempengaruhi reputasi dan kepercayaan pelanggan, sementara dampak pada area lain berada dalam kategori rendah (low). Area of concern ini menghasilkan Skor Risiko Relatif (Relative Risk Score) sebesar 17.

H. Select Mitigation Approach

Pemilihan risiko yang akan dimitigasi hanya mencakup risiko dengan prioritas tinggi. Untuk mengklasifikasikan risiko, digunakan Matriks Risiko Relatif (Relative Risk Matrix).

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

Pada setiap area of concern, terdapat kategori probabilitas yang ditentukan pada langkah kelima untuk menetapkan skenario risiko. Berdasarkan nilai probabilitas dan hasil skor risiko relatif (relative risk score), risiko tersebut 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

Aktivitas kedua adalah menentukan pendekatan mitigasi untuk setiap area of concern berdasarkan kategori probabilitas dan hasil analisis risiko. Pemilihan pendekatan mitigasi ini perlu didiskusikan dengan pihak organisasi. Berikut adalah hasil dari pendekatan mitigasi yang telah diidentifikasi untuk setiap area of concern:

Tabel 18 Pendekatan Mitigasi

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

Untuk menentukan pendekatan mitigasi pertama melihat dari probabilitas risiko tersebut kemudian nilai relative risk score termasuk ke dalam pool berapa. Pada kesalahan input data soal memiliki kategori probabilitas medium dengan relative risk score 17 dari nilai tersebut termasuk ke dalam pool 2 yang berarti mitigate atau diperlukan penanganan mengenai risiko tersebut. Areas of concern listrik mati juga memiliki nilai yang sama yaitu 17 tetapi termasuk pada pendekatan mitigasi accept karena kategori probabilitas low dan berada pada pool 3. Pendekatan accept berarti risiko dapat diterima oleh organisasi dan tidak dibutuhkan penanganan. Penyalahgunaan file folder back up data siswa dan guru memiliki nilai 14 dengan kategori probabilitas medium dan termasuk pada pool 3. Untuk areas of concern yang membutuhkan mitigasi telah diidentifikasi sebagai berikut:

Tabel 19 Mitigasi I

Risk Mitigation	
Areas of Concern	**Kesalahan input data nilai**
Action	Mitigate
Container	Kontrol
Sistem Informasi Sekolah	Menambahkan coding untuk pengecekan data yang sama dengan memberikan identifikasi mengenai data yang sebelumnya telah dimasukkan pada sistem

KESIMPULAN DAN SARAN

Dari hasil penelitian ini, diketahui bahwa area dampak yang paling krusial adalah reputasi dan kepercayaan pelanggan, produktivitas, keuangan, serta keamanan dan kesehatan. Ditemukan bahwa aset kritis termasuk database, server, switch, dan file folder. Terdapat tiga area concern, yaitu kesalahan input data soal, pemadaman listrik, dan penyalahgunaan file folder cadangan data siswa dan guru. Skor risiko relatif masing-masing adalah 17, 17, dan 14. Terdapat dua risiko yang masuk dalam pendekatan mitigasi accept dan satu risiko yang masuk dalam pendekatan mitigasi mitigate.

Saran yang dapat diberikan untuk penelitian ini adalah memberikan rekomendasi kepada SMA Panca Setya mengenai kemungkinan risiko yang mungkin terjadi dan langkah-langkah untuk meminimalkan risiko pada aplikasi ujian online. Selain itu, untuk penelitian selanjutnya, disarankan untuk memperluas analisis risiko terkait keamanan informasi pada semua aset informasi yang dimiliki oleh organisasi.

UCAPAN TERIMA KASIH

Pada kesempatan ini saya mengucapkan terima kasih kepada pihak-pihak yang telah memberikan kontribusi dan dukungan selama saya menulis penelitian ini.

DAFTAR REFERENSI

Prihatini, R., Freddy, K.W., & Muhamad, S.M. (2021). Penilaian Risiko Keamanan Informasi Menggunakan Octave Allegro: Studi Kasus pada Perguruan Tinggi. In *JUSIFO* (Vol. 7, No. 1, pp. 10-20). https://doi.org/10.19109/jusifo.v7i1.5870.

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.

Keating, C.G. (2014).Validating the OCTAVE Allegro Information System Risk Assessment Methodology: A Case Study. *NSUWorks*. Nova Southeastern University. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1191&context=gscis_etd.

Bavian, A.N., Andi, R.P., dan Aditya R. (2020). Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800- 30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. In *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* (Vol. 4, no. 1).

https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6884.

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*

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.

Raihan, R. A. & Rahadian, B. (2021). Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik. IN *JEISBI (*Vol. 02, No. 02). https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/39087.