JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

# Analisis Manajemen Risiko Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) Menggunakan Metode OCTAVE Allegro

**Utin Kasma**[1*]
[1]Sistem Informasi, Sistem Informasi, STMIK Pontianak, Pontianak, Indonesia
Email: [1*]utin_kasma@stmikpontianak.ac.id
(*Email Corresponding Author: utin_kasma@stmikpontianak.ac.id)
*Received: May 26, 2026 | Revision: June 2, 2026 | Accepted: June 6, 2026*

**Abstrak**

Transformasi digital dalam sektor pendidikan telah mendorong implementasi Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) berbasis daring sebagai upaya untuk meningkatkan efektivitas, efisiensi, akuntabilitas, dan transparansi dalam proses penerimaan peserta didik. Meskipun demikian, pemanfaatan sistem informasi tersebut tidak terlepas dari berbagai potensi risiko, khususnya yang berkaitan dengan keamanan informasi, ketersediaan layanan, serta integritas data. Penelitian ini bertujuan untuk melakukan analisis manajemen risiko pada Sistem Informasi PPDB pada SMU Bina Utama dengan menggunakan metode *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro*. Metode ini dipilih karena memiliki pendekatan yang berorientasi pada identifikasi aset informasi kritis, analisis ancaman, evaluasi kerentanan, serta penentuan prioritas mitigasi risiko berdasarkan tingkat dampak terhadap organisasi. Penelitian menggunakan pendekatan deskriptif kualitatif melalui teknik observasi, wawancara, dan studi dokumentasi terhadap sistem yang dianalisis. Hasil penelitian menunjukkan bahwa aset informasi yang memiliki tingkat kritikalitas tertinggi meliputi data peserta didik, basis data sistem, dan infrastruktur server. Risiko utama yang teridentifikasi mencakup kebocoran data, gangguan layanan akibat *server downtime*, akses tidak sah terhadap sistem, serta kesalahan operasional pengguna. Berdasarkan hasil evaluasi risiko, kebocoran data peserta didik dan gangguan server merupakan risiko prioritas yang memerlukan penanganan segera. Strategi mitigasi yang direkomendasikan meliputi implementasi enkripsi data, autentikasi multi-faktor, peningkatan kapasitas infrastruktur, serta penerapan prosedur pencadangan data secara berkala.

**Kata Kunci:** Manajemen Risiko, Sistem Informasi, PPDB, OCTAVE Allegro, Keamanan Informasi.

***Abstract***

*Digital transformation in the education sector has driven the implementation of an online-based New Student Admissions Information System (PPDB) as an effort to increase effectiveness, efficiency, accountability, and transparency in the student admissions process. However, the use of this information system is not without various potential risks, particularly those related to information security, service availability, and data integrity. This study aims to conduct a risk management analysis on the PPDB Information System of SMU Bina Utama using the Allegro Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method. This method was chosen because it has an approach oriented towards identifying critical information assets, analyzing threats, evaluating vulnerabilities, and determining risk mitigation priorities based on the level of impact on the organization. The study used a qualitative descriptive approach through observation, interviews, and documentation studies of the analyzed system. The results show that the information assets with the highest level of criticality include student data, system databases, and server infrastructure. The main risks identified include data leaks, service disruptions due to server downtime, unauthorized access to the system, and user operational errors. Based on the results of the risk evaluation, student data leaks and server disruptions are priority risks that require immediate attention. Recommended mitigation strategies include implementing data encryption, multi-factor authentication, increasing infrastructure capacity, and implementing regular data backup procedures.*

***Keywords:*** *Risk Management, Information Systems, PPDB, OCTAVE Allegro, Information Security.*

## 1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan kontribusi signifikan terhadap transformasi digital pada berbagai sektor, termasuk sektor pendidikan. Salah satu bentuk implementasi transformasi digital tersebut adalah penerapan Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) berbasis daring yang dirancang untuk mendukung proses administrasi penerimaan siswa secara lebih efektif, efisien, dan transparan. 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]. Sistem Informasi PPDB merupakan platform digital yang dirancang untuk mengotomatisasi proses penerimaan peserta didik baru, mulai dari tahap registrasi hingga proses seleksi akhir. Implementasi sistem ini bertujuan untuk meningkatkan kualitas layanan administrasi pendidikan melalui pemanfaatan teknologi informasi. Penerapan system informasi PPDB juga dilakukan oleh SMU Bina Utama Pontianak untuk mendukung proses penerimaan siswa baru secara daring. Penerapan sistem PPDB berbasis teknologi informasi pada SMU Bina Utama ini memungkinkan proses pendaftaran, verifikasi dokumen, seleksi, hingga pengumuman hasil dilakukan secara terintegrasi melalui platform digital. Namun demikian, ketergantungan yang tinggi terhadap teknologi informasi juga meningkatkan potensi munculnya berbagai risiko, seperti

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

ancaman terhadap kerahasiaan data pribadi peserta didik, gangguan ketersediaan layanan akibat kegagalan sistem, serta potensi manipulasi data oleh pihak yang tidak berwenang.

Risiko-risiko tersebut dapat berdampak langsung terhadap kualitas layanan pendidikan, menurunkan tingkat kepercayaan masyarakat terhadap institusi penyelenggara, serta menimbulkan kerugian operasional maupun reputasional. Oleh karena itu, diperlukan suatu pendekatan manajemen risiko yang sistematis dan terstruktur guna mengidentifikasi, menganalisis, dan memitigasi potensi ancaman yang dapat memengaruhi keberlangsungan sistem. Manajemen risiko merupakan suatu proses sistematis yang mencakup identifikasi, analisis, evaluasi, dan pengendalian risiko yang berpotensi menghambat pencapaian tujuan organisasi [2]. Dalam konteks sistem informasi, manajemen risiko berperan penting dalam menjaga aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi.

Manajemen risiko sistem informasi Penerimaan Peserta Didik Baru (PPDB) adalah proses proaktif untuk mengidentifikasi, mengevaluasi, dan memitigasi potensi gangguan teknis maupun operasional seperti server *down*, kebocoran data, atau ketidaksesuaian data calon siswa. Tujuannya adalah memastikan kelancaran operasional, efisiensi administrasi, dan keamanan data [3]. Data peserta didik yang dikelola dalam sistem PPDB termasuk kategori data sensitif karena memuat identitas pribadi, dokumen administratif, serta informasi akademik calon peserta didik. Apabila data tersebut mengalami kebocoran atau penyalahgunaan, maka institusi pendidikan tidak hanya menghadapi kerugian operasional, tetapi juga berpotensi mengalami penurunan reputasi, hilangnya kepercayaan publik, serta konsekuensi hukum akibat pelanggaran regulasi perlindungan data. Kelemahan dalam tata kelola keamanan informasi pada institusi pendidikan dapat meningkatkan potensi insiden keamanan siber secara signifikan [4].

Sistem Informasi PPDB merupakan bentuk inovasi digital yang dirancang untuk mengotomatisasi proses penerimaan peserta didik mulai dari tahap registrasi, verifikasi dokumen, seleksi administrasi, hingga pengumuman hasil penerimaan secara terintegrasi melalui platform digital. Implementasi sistem ini memberikan berbagai manfaat strategis, seperti peningkatan transparansi proses seleksi, pengurangan penggunaan dokumen fisik, percepatan layanan administrasi, serta kemudahan akses layanan bagi masyarakat tanpa batasan geografis [5]. Selain itu, digitalisasi layanan PPDB juga mendukung prinsip tata kelola pendidikan modern yang menekankan aspek efisiensi, akuntabilitas, dan pelayanan publik berbasis teknologi. Dalam konteks Sistem Informasi PPDB, berbagai ancaman dapat terjadi seperti erupa kebocoran data pribadi peserta didik (*data breach*), akses tidak sah (*unauthorized access*), manipulasi data oleh pihak internal maupun eksternal, serangan *malware*, *phishing*, hingga gangguan layanan akibat kegagalan infrastruktur teknologi seperti *server downtime* atau *network failure*.

Selain risiko terhadap kerahasiaan data, tantangan utama lain dalam implementasi Sistem Informasi PPDB adalah aspek ketersediaan layanan (*availability*). Pada periode pendaftaran, sistem umumnya mengalami lonjakan akses secara simultan (*high concurrent traffic*) yang berpotensi menyebabkan penurunan performa sistem hingga kegagalan layanan (*system failure*). Kondisi ini dapat menghambat proses administrasi penerimaan peserta didik, meningkatkan tingkat keluhan pengguna, serta menurunkan kualitas layanan pendidikan berbasis digital [6]. Institusi pendidikan memiliki tingkat kerentanan tinggi terhadap gangguan operasional sistem apabila tidak didukung oleh manajemen risiko teknologi informasi yang memadai [3]. Dalam menghadapi kompleksitas risiko tersebut, organisasi memerlukan pendekatan manajemen risiko yang sistematis, terukur, dan berbasis aset informasi. Manajemen risiko merupakan proses terstruktur yang mencakup identifikasi, analisis, evaluasi, dan mitigasi risiko untuk meminimalkan dampak negatif terhadap tujuan organisasi [2]. Dalam konteks keamanan sistem informasi, proses ini menjadi bagian integral dari tata kelola teknologi informasi (*IT governance*) yang bertujuan memastikan keberlangsungan layanan dan perlindungan aset digital organisasi.

Salah satu metode yang relevan dalam konteks manajemen risiko keamanan informasi adalah OCTAVE Allegro. Metode ini berfokus pada aset informasi organisasi. OCTAVE Allegro telah dilengkapi dengan guidance, lembar kerja hingga kuesioner [7]. Metode ini dikembangkan oleh Carnegie Mellon University dan dirancang untuk membantu organisasi mengidentifikasi risiko berdasarkan aset informasi kritis, ancaman yang melekat pada aset tersebut, serta dampaknya terhadap tujuan organisasi. Keunggulan utama metode OCTAVE Allegro terletak pada pendekatan berbasis aset (*asset-based risk assessment*), sehingga organisasi dapat menentukan prioritas mitigasi berdasarkan tingkat sensitivitas dan nilai strategis aset informasi [8]. Metode ini menitikberatkan pada identifikasi aset informasi sebagai elemen utama dalam proses analisis risiko, sehingga memungkinkan organisasi untuk menentukan prioritas pengamanan berdasarkan tingkat nilai dan sensitivitas aset tersebut.

OCTAVE Allegro merupakan kerangka kerja manajemen risiko keamanan informasi yang dikembangkan oleh Carnegie Mellon University. Metode ini menekankan evaluasi risiko berdasarkan aset informasi organisasi melalui delapan tahapan analisis yang sistematis, sehingga mampu menghasilkan rekomendasi mitigasi yang terukur [9].

Berdasarkan uraian diatas, dapat dipahami bahwa Sistem Informasi PPDB merupakan bagian dari layanan digital pendidikan yang memiliki tingkat kompleksitas risiko yang cukup tinggi, sehingga membutuhkan evaluasi keamanan secara komprehensif. Oleh karena itu, penelitian ini dilakukan untuk menganalisis manajemen risiko pada Sistem Informasi PPDB pada SMU Bina Utama dengan menggunakan metode OCTAVE Allegro dengan tujuan untuk mengidentifikasi aset informasi kritis, menganalisis ancaman dan kerentanan, menentukan tingkat prioritas risiko, serta merumuskan strategi mitigasi yang tepat guna meningkatkan keamanan, keandalan, dan keberlanjutan layanan sistem informasi pendidikan pada SMU tersebut.

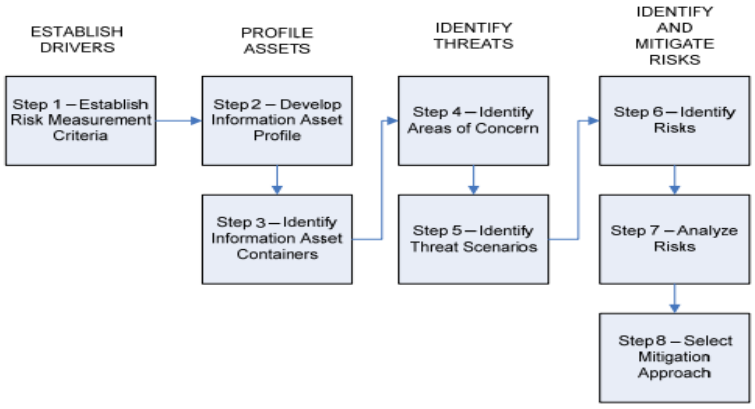
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

# 2. METODOLOGI PENELITIAN

## 2.1 Metode Penelitian

Metode analisis data yang digunakan dalam penelitian ini dengan mengisi semua worksheet sesuai dengan kerangka kerja OCTAVE Allegro. Ada empat tingkatan dengan delapan langkah dalam melakukan penilaian risiko keamanan terhadap asset informasi. Proses ini akan menghasilkan sepuluh tabel W*orksheet* hasil penilaian. Dari hasil tahapan identifikasi risiko mengacu pada asset risk worksheet OCTAVE Allegro maka akan didapatkan tabel area terdampak. OCTAVE Allegro dikembangkan oleh tim CERT dengan tujuan utama untuk membantu organisasi memastikan bahwa kegiatan keamanan informasi mereka selaras dengan tujuan organisasi [8].

OCTAVE Allegro merupakan sebuah kerangka kerja yang menggunakan pendekatan OCTAVE dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan. Tujuannya adalah untuk menghasilkan hasil penilaian profil risiko yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko atau audit. [10]. *Framework* OCTAVE Allegro terdiri atas delapan tahapan yang diklasifikasikan menjadi empat fase.




**Gambar 1** : Octave Allegro

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

A. Menetapkan Kriteria Pengukuran Risiko (*Establish Risk Measurement Criteria*)
Tahapan awal dalam metode OCTAVE Allegro berfokus pada penyusunan kriteria yang digunakan sebagai dasar dalam mengukur tingkat risiko. Aktivitas utama pada fase ini meliputi identifikasi parameter penilaian risiko yang relevan dengan tujuan organisasi, seperti dampak terhadap produktivitas, reputasi, keuangan, keamanan, serta kepatuhan regulasi. Setelah kriteria ditentukan, dilakukan proses prioritisasi menggunakan *Impact Area Ranking Worksheet* untuk menetapkan tingkat urgensi masing-masing area dampak sebagai acuan dalam proses analisis risiko selanjutnya.

B. Penyusunan Profil Aset Informasi (*Develop an Information Asset Profile*)
Tahap ini bertujuan untuk mengidentifikasi dan mendokumentasikan aset informasi yang memiliki nilai kritis bagi organisasi. Proses yang dilakukan mencakup inventarisasi aset informasi, penentuan tingkat kritikalitas aset, pendefinisian ruang lingkup aset, pemberian identitas atau nama aset, serta identifikasi kebutuhan keamanan informasi berdasarkan tiga aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Hasil dari tahap ini berupa profil aset informasi yang menjadi fokus utama dalam analisis risiko.

C. Identifikasi Kontainer Aset Informasi (*Identify Information Asset Containers*)
Pada fase ini dilakukan identifikasi terhadap seluruh media atau kontainer yang digunakan untuk menyimpan, memproses, maupun mentransmisikan aset informasi. Kontainer dapat berupa perangkat keras, perangkat lunak, jaringan, dokumen fisik, maupun sumber daya manusia yang berinteraksi dengan aset tersebut. Selain itu, tahap ini juga mencakup evaluasi terhadap mekanisme perlindungan yang telah diterapkan pada masing-masing kontainer serta identifikasi potensi ancaman yang dapat memengaruhi keamanan aset informasi.

D. Identifikasi Area Permasalahan (*Identify Areas of Concern*)
Tahap ini merupakan langkah awal dalam proses analisis ancaman dengan tujuan mengidentifikasi berbagai kondisi atau situasi yang berpotensi menimbulkan risiko terhadap aset informasi. Analisis dilakukan melalui eksplorasi kemungkinan ancaman, kelemahan sistem, serta faktor-faktor internal maupun eksternal yang dapat memengaruhi keberlangsungan keamanan informasi dalam organisasi.

E. Identifikasi Skenario Ancaman (*Identify Threat Scenarios*)
Pada tahap ini dilakukan perumusan skenario ancaman secara lebih rinci berdasarkan area permasalahan yang telah diidentifikasi sebelumnya. Proses ini meliputi penentuan ancaman tambahan yang relevan serta pengisian *OCTAVE Allegro Worksheet* untuk mendokumentasikan karakteristik ancaman secara terstruktur. Skenario ancaman disusun

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

untuk menggambarkan bagaimana suatu ancaman dapat terjadi, pihak yang terlibat, serta potensi dampak yang mungkin ditimbulkan terhadap aset informasi.

F. Identifikasi Risiko (*Identify Risks*)
Tahapan ini berfokus pada identifikasi konsekuensi atau dampak yang muncul dari setiap skenario ancaman yang telah dirumuskan. Dengan menggunakan *Information Asset Risk Worksheet*, organisasi dapat menilai bagaimana ancaman tertentu dapat memengaruhi aset informasi, baik dari sisi operasional, finansial, hukum, maupun reputasi. Hasil tahap ini berupa daftar risiko yang telah terdefinisi secara spesifik berdasarkan skenario ancaman yang ada.

G. Analisis Risiko (*Analyze Risks*)
Pada fase analisis risiko, setiap risiko yang telah diidentifikasi diberikan nilai berdasarkan tingkat dampak dan kemungkinan terjadinya. Penilaian dilakukan dengan membandingkan konsekuensi risiko terhadap prioritas area dampak yang telah ditentukan pada tahap awal. Hasil analisis ini menghasilkan *relative risk score* yang digunakan untuk menentukan tingkat prioritas penanganan risiko, sehingga organisasi dapat memfokuskan sumber daya pada risiko yang paling signifikan.

H. Pemilihan Strategi Mitigasi (*Select Mitigation Approach*)
Tahap akhir dalam metode OCTAVE Allegro adalah penentuan strategi mitigasi terhadap risiko yang telah diprioritaskan. Proses ini mencakup evaluasi tingkat urgensi risiko, pemilihan pendekatan mitigasi yang sesuai seperti menghindari (*avoid*), mengurangi (*mitigate*), mentransfer (*transfer*), atau menerima (*accept*) risiko serta penyusunan rencana pengendalian yang selaras dengan nilai aset dan tujuan organisasi. Output dari tahap ini berupa rekomendasi mitigasi risiko yang dapat diimplementasikan untuk meningkatkan keamanan sistem informasi.

### 2.2 Tahapan Analisis Menggunakan OCTAVE Allegro

Tahapan analisis dilakukan berdasarkan delapan langkah utama metode OCTAVE Allegro, yaitu:

1. Penetapan kriteria pengukuran risiko;
2. Identifikasi aset informasi kritis;
3. Identifikasi kontainer aset informasi;
4. Identifikasi area perhatian (*areas of concern*);
5. Penyusunan skenario ancaman (*threat scenarios*);
6. Identifikasi risiko;
7. Analisis dan prioritisasi risiko;
8. Penentuan strategi mitigasi risiko.

## 3. HASIL DAN PEMBAHASAN

Metode analisis data yang digunakan dalam penelitian ini dengan mengisi semua worksheet sesuai dengan kerangka kerja OCTAVE Allegro. OCTAVE Allegro merupakan sebuah kerangka kerja yang menggunakan pendekatan OCTAVE dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan. Tujuannya adalah untuk menghasilkan hasil penilaian profil risiko yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko atau audit.

### 3.1. Penetapan Kriteria Pengukuran Risiko (*Establish Risk Measurement Criteria*)

Tahapan awal dalam penerapan metode OCTAVE Allegro adalah penetapan kriteria pengukuran risiko (*establish risk measurement criteria*). Tahap ini memiliki peran fundamental karena menjadi dasar dalam proses evaluasi dan prioritisasi risiko pada tahapan selanjutnya. Tujuan utama dari tahap ini adalah menetapkan parameter penilaian yang digunakan untuk mengukur tingkat konsekuensi atau dampak yang ditimbulkan apabila suatu ancaman terhadap aset informasi terjadi. Dalam konteks Sistem Informasi Penerimaan Peserta Didik Baru (PPDB), penetapan kriteria pengukuran risiko dilakukan dengan mengidentifikasi berbagai area dampak yang berpotensi memengaruhi keberlangsungan operasional sistem, kualitas layanan, serta reputasi institusi penyelenggara. Kriteria ini berfungsi sebagai kerangka evaluasi yang memungkinkan organisasi melakukan penilaian risiko secara sistematis, terukur, dan objektif. Mengacu pada pendekatan OCTAVE Allegro, terdapat lima area dampak utama (impact areas) yang digunakan sebagai acuan dalam proses pengukuran risiko, yaitu:

1. Reputasi dan Kepercayaan (*Reputation and Customer Confidence*)
   Menggambarkan tingkat pengaruh suatu risiko terhadap citra institusi dan tingkat kepercayaan pengguna atau masyarakat terhadap layanan PPDB.
2. Keuangan (*Financial*)
   Menunjukkan besarnya potensi kerugian finansial yang dapat dialami organisasi sebagai akibat dari insiden keamanan informasi atau gangguan sistem.
3. Produktivitas (*Productivity*)
   Mengukur sejauh mana risiko dapat menghambat efektivitas proses bisnis, khususnya pada proses administrasi dan operasional layanan PPDB.
4. Keamanan dan Keselamatan (*Safety and Health*)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

Menilai kemungkinan dampak risiko terhadap keselamatan pengguna maupun pihak yang terlibat dalam operasional sistem, meskipun pada sistem PPDB aspek ini umumnya memiliki tingkat relevansi yang lebih rendah dibanding area lainnya.

5. Hukum dan Regulasi (*Legal and Regulatory*)
   Menilai konsekuensi hukum yang mungkin timbul akibat ketidaksesuaian terhadap regulasi, khususnya yang berkaitan dengan perlindungan data pribadi dan tata kelola informasi

**Tabel. 1. Kriteria Pengukuran Risiko Sistem Informasi PPDB**

| SKALA | TINGKAT DAMPAK | DEFINISI |
|---|---|---|
| **1** | Rendah | Risiko menimbulkan dampak minimal terhadap operasional organisasi dan tidak mengganggu fungsi utama sistem |
| **2** | Sedang | Risiko menimbulkan gangguan operasional yang dapat ditangani melalui sumber daya internal organisasi |
| **3** | Tinggi | Risiko memberikan dampak signifikan terhadap layanan dan memerlukan tindakan korektif secara segera |
| **4** | Sangat Tinggi | Risiko menyebabkan gangguan kritis terhadap operasional organisasi dan berpotensi menimbulkan kerugian strategis |

Adapun kriteria pengukuran resiko pada Sistem Informasi PPDB pada SMU Bina Utama Pontianak ini dibagi dalam 4 tingkatanm dampak yaitu dampak Rendah, Sedang, Tinggi dan Sangat Tinggi.

**Tabel 2. Prioritas Area Dampak (*Impact Area Ranking Worksheet*)**

| NO. | AREA DAMPAK | DESKRIPSI | PRIORITAS |
|---|---|---|---|
| **1** | Reputasi dan Kepercayaan | Penurunan kepercayaan masyarakat apabila sistem gagal atau data bocor | 5 |
| **2** | Hukum dan Regulasi | Pelanggaran perlindungan data pribadi peserta didik | 4 |
| **3** | Produktivitas | Terganggunya proses pendaftaran dan seleksi siswa | 3 |
| **4** | Keuangan | Potensi biaya tambahan akibat perbaikan sistem | 2 |
| **5** | Keamanan dan Kesehatan | Dampak tidak langsung terhadap pengguna | 1 |

Sementara itu Area Dampak yang sangat prioritas adalah Reputasi dan Kepercayaan yang akan mengalami penurunan kepercayaan masyarakat apabila system gagal atau terjadinya kebocoran data. Untuk Area dampak yang prioritasnya sanbgat rendah adalah Keamanan dan Kesehatan karena area dampak ini tidak terjadi secara langsung kepada pengguna.

**Tabel 3. Prioritas**

| PRIORITAS | KETERANGAN |
|---|---|
| **5** | Sangat Prioritas |
| **4** | Prioritas Tinggi |
| **3** | Prioritas Sedang |
| **2** | Prioritas Rendah |
| **1** | Prioritas Sangat Rendah |

### 3.2. Identifikasi Aset Informasi Kritis

**Tabel 4. Identifikasi Aset Informasi Kritis**

| NO | ASET INFORMASI | DESKRIPSI | TINGKAT PRIORITAS |
|---|---|---|---|
| **1** | Data peserta didik | Informasi pribadi calon siswa | 4 |
| **2** | Basis data | Penyimpanan data seluruh transaksi sistem | 4 |
| **3** | Server aplikasi | Infrastruktur utama layanan PPDB | 4 |
| **4** | Jaringan internet | Media konektivitas sistem | 3 |

Untuk identifikasi asset informasi kritis, yang menjadi prioritas paling tinggi adalah Data Peserta Didik yang memuat informasi tentang pribadi calon siswa. Setelah itu diikuti dengan asset basis data, server aplikasi dan terakhir jaruingan internet.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

### 3.3. Identifikasi Ancaman dan Kerentanan

Analisis terhadap ancaman menunjukkan bahwa setiap aset memiliki kerentanan yang berbeda sesuai dengan karakteristik dan tingkat sensitivitasnya.

**Tabel 5. Identifikasi Ancaman dan Kerentanan**

| ASET | ANCAMAN | KERENTANAN |
|---|---|---|
| **Data peserta didik** | Kebocoran informasi | Mekanisme enkripsi belum optimal |
| **Basis data** | Akses tidak sah | Kebijakan kata sandi lemah |
| **Server Aplikasi** | Gangguan layanan | Tidak tersedia server redundan |
| **Jaringan Internet** | Koneksi tidak stabil | Kapasitas bandwidth terbatas |

### 3.4. Analisis dan Penilaian Risiko

Penilaian risiko dilakukan berdasarkan kombinasi tingkat dampak dan probabilitas kejadian.

**Tabel 6. Hasil Penilaian Risiko**

| RISIKO | DAMPAK | PROBABILITAS | SKOR | KATEGORI |
|---|---|---|---|---|
| **Kebocoran data peserta didik** | 5 | 3 | 15 | Tinggi |
| **Gangguan server** | 4 | 4 | 16 | Tinggi |
| **Human error** | 3 | 4 | 12 | Sedang |
| **Gangguan jaringan** | 3 | 3 | 9 | Sedang |

Hasil analisis menunjukkan bahwa gangguan server memiliki skor risiko tertinggi, diikuti oleh potensi kebocoran data peserta didik.

### 3.5. Matriks Mitigasi Resiko

Berdasarkan hasil prioritisasi risiko, strategi mitigasi disusun sesuai tingkat urgensi masing-masing risiko.

**Tabel 7. Matriks Mitigasi Risko**

| RISIKO | STRATEGI MITIGASI | PRIORITAS |
|---|---|---|
| **Kebocoran data peserta didik** | Implementasi enkripsi, autentikasi multi faktor, audit akses | Sangat Tinggi |
| **Gangguan server** | Redundansi server, *load balancing*, backup sistem | Sangat Tinggi |
| **Human error** | Pelatihan pengguna dan validasi data otomatis | Sedang |
| **Gangguan jaringan** | Penyediaan koneksi cadangan dan monitoring jaringa | Sedang |

### 3.6. Pembahasan

Hasil penelitian menunjukkan bahwa data peserta didik merupakan aset informasi dengan tingkat sensitivitas tertinggi karena mengandung informasi pribadi siswa SMU Bina Utama yang wajib dijaga kerahasiaannya sesuai prinsip keamanan informasi. Risiko kebocoran data menjadi prioritas utama karena berpotensi menimbulkan dampak hukum, reputasi, dan kepercayaan publik terhadap institusi pendidikan. Selain itu, risiko gangguan server menjadi ancaman signifikan karena sistem PPDB memiliki karakteristik penggunaan bersamaan (*concurrent access*) yang tinggi, terutama pada periode pendaftaran. Kondisi ini dapat menyebabkan *server overload* dan menurunkan kualitas layanan sistem.

Penerapan metode OCTAVE Allegro dalam penelitian ini terbukti mampu memberikan pendekatan yang komprehensif dalam proses identifikasi dan evaluasi risiko, karena analisis dilakukan berdasarkan nilai aset informasi serta potensi ancaman yang melekat pada aset tersebut. Dengan demikian, organisasi dapat menetapkan strategi mitigasi secara lebih terukur dan berbasis prioritas.

## 4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan menggunakan metode OCTAVE Allegro pada Sistem Informasi Penerimaan Peserta Didik Baru (PPDB) pada SMU Bina Utama, dapat disimpulkan bahwa penerapan manajemen risiko memiliki peranan yang sangat penting dalam mendukung keamanan, keandalan, dan keberlangsungan layanan sistem informasi pada institusi pendidikan. Sistem Informasi PPDB sebagai salah satu bentuk transformasi digital di bidang pendidikan memiliki ketergantungan yang tinggi terhadap teknologi informasi, sehingga keberadaan potensi risiko harus dikelola secara sistematis agar tidak mengganggu operasional layanan. Hasil identifikasi aset menunjukkan bahwa data peserta didik, basis data, server aplikasi, dan infrastruktur jaringan merupakan aset informasi

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 1 Juni 2026
Hal: 659-665
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i1.1066

utama yang memiliki tingkat kritikalitas tinggi. Dari seluruh aset tersebut, data peserta didik yang tersimpan pada basis data Sistem Informasi PPDB pada SMU Bina Utama Pontianak menjadi aset paling sensitif karena memuat informasi pribadi siswa yang harus dilindungi berdasarkan prinsip keamanan informasi *Confidentiality, Integrity, and Availability*, khususnya pada aspek kerahasiaan, integritas, dan ketersediaan data. Gangguan atau pelanggaran terhadap aset tersebut berpotensi menimbulkan dampak besar terhadap reputasi institusi, kualitas layanan, dan kepatuhan terhadap regulasi perlindungan data. Hasil analisis risiko menunjukkan bahwa risiko utama yang dihadapi Sistem Informasi PPDB pada SMU Bina Utama meliputi kebocoran data peserta didik, gangguan layanan akibat *server downtime*, akses tidak sah terhadap sistem, serta kesalahan operasional pengguna (*human error*). Berdasarkan evaluasi menggunakan matriks risiko relatif, kebocoran data peserta didik dikategorikan sebagai risiko dengan tingkat prioritas tertinggi karena memiliki dampak yang sangat signifikan terhadap organisasi. Selain itu, risiko gangguan server juga berada pada kategori tinggi karena berpotensi menghambat seluruh proses pendaftaran dan pelayanan kepada calon peserta didik. Penerapan metode OCTAVE Allegro dalam penelitian ini terbukti efektif dalam membantu SMU Bina Utama Pontianak mengidentifikasi, menganalisis, dan memprioritaskan risiko secara terstruktur berdasarkan nilai aset informasi yang dimiliki. Dengan demikian, SMU Bina Utama Pontianak dapat merumuskan strategi mitigasi yang tepat, seperti implementasi enkripsi data, autentikasi multi-faktor, peningkatan kapasitas server, pencadangan data secara berkala, serta penyusunan *disaster recovery plan*. Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan manajemen risiko berbasis OCTAVE Allegro dapat menjadi landasan strategis dalam meningkatkan tata kelola keamanan Sistem Informasi PPDB pada SMU Bina Utama secara berkelanjutan.

## REFERENCES

[1] U. Kasma, “Manajemen Risiko Sistem Informasi Akademik pada SMA Panca Setya Menggunakan Metoda Octave Allegro,” SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi, vol. 2, no. 3, pp. 245-256, 2024. doi: 10.59841/saber.v2i3.1525.

[2] U. Kasma, “Identifikasi Risiko Keamanan Data Sistem Informasi Perpustakaan,” Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, vol. XIV, no. 2, pp. 9-17, 2025.

[3] International Organization for Standardization, "ISO 31000:2018 Risk Management—Guidelines," Geneva, Switzerland: ISO, 2018.

[4] J. S. Suroso and M. A. Fakhrozi, “Assessment of Information System Risk Management with OCTAVE Allegro at Education Institution,” Procedia Computer Science, vol. 135, pp. 202–213, 2018. doi: 10.1016/j.procs.2018.08.170.

[5] P. Ramjanati et al., “Penilaian Risiko Keamanan Informasi Menggunakan OCTAVE Allegro,” JUSIFO, vol. 7, no. 1, pp. 1–12, 2021.

[6] A. Putra, “Analisis Risiko Sistem Informasi Menggunakan Metode OCTAVE,” Jurnal Teknologi Informasi, vol. 8, no. 2, pp. 45–53, 2020.

[7] J. J. L. Tobing and A. K. P., “Analisis Manajemen Resiko untuk Evaluasi Asset menggunakan Metode Octave Allegro,” Expert: Jurnal Manajemen Sistem Informasi Dan Teknologi, vol. 5, no. 1, pp. 12-20, 2015.

[8] J. Hom et al., “The OCTAVE Allegro Method in Risk Management Assessment of Educational Institutions,” Aptisi Transactions on Technopreneurship, vol. 2, no. 2, pp. 167–179, 2020.

[9] S. R. Wicaksono, C. L. D. Rizka, and G. A. Immanuel, “Risk Assessment Menggunakan Pendekatan OCTAVE Allegro (Studi Kasus: Schoology.com),” Information Communication & Technology, vol. 18, no. 2, pp. 123–129, 2019.

[10] V. Gerardo and A. N. Fajar, “Academic Information System Risk Management Using OCTAVE Allegro in Educational Institution,” Journal of Information Systems and Informatics, vol. 4, no. 3, pp. 687–708, 2022. doi: 10.51519/journalisi.v4i3.319.

[11] Haeruddin, “Pemetaan Information Asset Profile dalam Penerapan Manajemen,” JITE (Journal of Informatics and Telecommunication Engineering), vol. 3, no. 1, pp. 67–75, 2019.

[12] R. Ramadhintia and R. Bisma, “Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik,” JEISBI (Journal of Emerging Information Systems and Business Intelligence), vol. 2, no. 2, pp. 80-88, 2021.

[13] Megawati and M. Kazmaini, “Analisa Manajemen Resiko Sistem Informasi Perpustakaan Menggunakan Cobit 4.1 Pada Domain Po9,” Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, vol. 4, no. 1, pp. 73-76, 2018.

[14] D. Sari, “Evaluasi Keamanan Sistem Informasi Akademik Berbasis OCTAVE Allegro,” Jurnal Sistem Informasi, vol. 10, no. 1, pp. 22–30, 2021.

[15] L. K. Ronald and D. V. Russell, The CISSP Prep Guide - Mastering the Ten Domains of Computer Security. California: John Wiley & Sons, Inc., 2006