NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)

Vol. 01, No. 1, Desember 2024

ANALISA MANAJEMEN RISIKO IT DENGAN MENGGUNAKAN METODE OCTAVE-S UNTUK MENINGKATKAN KEAMANAN SISTEM DI PTIPD UNIVERSITAS XYZ

Ayuni Fachrunisa Lubis[1], Diana Nadha[2], Megawati[3]

[1, 2, 3]Fakultas Sains dan Teknologi/Program Studi Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia

email: 12150322141@students.uin-suska.ac.id

Abstract

The Center for Information Technology and Databases (PTIPD) at XYZ University has important responsibilities in managing information systems to support university operations. However, high dependence on information technology increases security risks that can threaten institutional data and reputation. This research uses the OCTAVE-S method to manage information security risks systematically. This method includes three main stages: identification of critical assets, risk analysis, and development of mitigation strategies. The analysis results show that PTIPD's critical information assets include the iRaise system, Internal Quality Audit, E-Learning, Scholarships, and Integrated SIVIL, as well as human assets. The security evaluation showed three security practices were at "Red", five at "Yellow", and seven at "Green". "Red" status requires increased attention to significantly reduce risks. The proposed recommendations include improvements in three key areas: Contingency Planning to ensure operational continuity during a crisis Vulnerability Management through identification and mitigation of system weaknesses, and Incident Management for rapid response to security incidents. Implementation of these recommendations is expected to improve PTIPD information security and ensure the protection of critical university assets..

Keywords: *Oktave-S, Risk Management, Center for Information Technology and Database, XYZ University*

Abstrak

Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) Universitas XYZ memiliki tanggung jawab penting dalam mengelola sistem informasi untuk mendukung operasional universitas. Namun, tingginya ketergantungan pada teknologi informasi meningkatkan risiko keamanan yang dapat mengancam data dan reputasi institusi. Penelitian ini menggunakan metode OCTAVE-S untuk mengelola risiko keamanan informasi secara sistematis. Metode ini mencakup tiga tahap utama: identifikasi aset kritis, analisis risiko, dan pengembangan strategi mitigasi. Hasil analisis menunjukkan bahwa aset informasi kritis PTIPD meliputi sistem *iRaise*, Audit Mutu Internal, *E-Learning*, Beasiswa, dan Integrated SIVIL, serta aset manusia. Evaluasi keamanan menunjukkan tiga praktik keamanan berada pada status "*Red*", lima pada "*Yellow*", dan tujuh pada "*Green*". Status "*Red*" memerlukan perhatian lebih untuk mengurangi risiko secara signifikan. Rekomendasi yang diajukan mencakup peningkatan pada tiga area utama: Perencanaan Kontinjensi untuk memastikan kelangsungan operasional selama krisis Manajemen Kerentanan melalui identifikasi dan mitigasi kelemahan sistem, serta Manajemen Insiden untuk respons cepat terhadap insiden keamanan. Implementasi rekomendasi ini diharapkan dapat meningkatkan keamanan informasi PTIPD dan memastikan perlindungan aset kritis universitas.

Kata kunci: Oktave-S, Manajemen Resiko, Pusat Teknologi Informasi dan Pangkalan Data, Universitas XYZ

Diajukan: 11 Desember 2024; Direvisi: 20 Januari 2025; Diterima: 21 Januari 2025;

PENDAHULUAN

Seiring dengan perkembangan teknologi informasi yang pesat, penggunaan sistem informasi di berbagai institusi pendidikan menjadi semakin penting untuk menunjang operasional dan layanan. Di Universitas XYZ, Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) memainkan peran vital dalam mengelola berbagai sistem informasi yang digunakan oleh fakultas, staf, dan mahasiswa. Sistem-sistem ini

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 1, Desember 2024

mencakup akademik, administrasi, keuangan, dan layanan lainnya yang sangat bergantung pada teknologi informasi [1].

Namun, dengan meningkatnya penggunaan sistem informasi, risiko keamanan juga meningkat. Ancaman seperti peretasan, kebocoran data, serangan malware, serta kegagalan sistem dapat mengakibatkan kerugian besar baik dari segi finansial maupun reputasi universitas [2]. Untuk itu, diperlukan suatu sistem manajemen risiko yang efektif agar PTIPD Universitas XYZ dapat memastikan keamanan, kelancaran, dan efisiensi sistem yang dikelolanya [3].

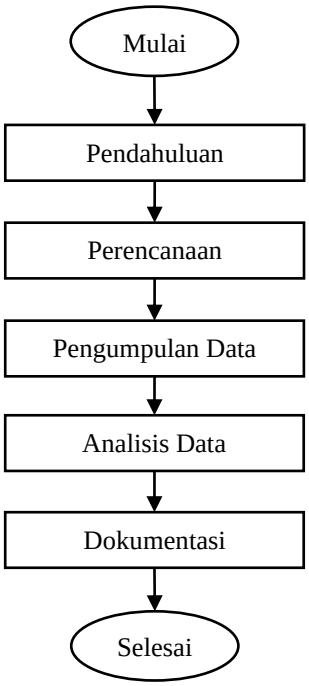
Metode Octave S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation – Simplified*) adalah salah satu pendekatan yang bisa digunakan dalam melakukan manajemen risiko keamanan informasi. Metode ini memungkinkan organisasi untuk mengidentifikasi risiko keamanan, menilai dampaknya, serta merancang langkah-langkah mitigasi yang tepat [4]. Metode OCTAVE-S dipilih dalam analisis manajemen risiko di PTIPD Universitas XYZ karena keunggulannya yang relevan untuk organisasi skala kecil hingga menengah, termasuk unit layanan teknologi informasi seperti PTIPD.

Metode ini menawarkan pendekatan yang terstruktur namun sederhana, memudahkan identifikasi aset-aset kritis, ancaman, dan kerentanan tanpa memerlukan sumber daya yang besar atau pelatihan intensif. Selain itu, OCTAVE-S dirancang untuk berfokus pada kebutuhan organisasi secara spesifik, memungkinkan PTIPD untuk memahami risiko yang paling relevan terhadap layanan utamanya, seperti infrastruktur IT, keamanan data, dan operasional harian. Dengan orientasi pada pemangku kepentingan internal, metode ini juga memfasilitasi kolaborasi antar tim dan menghasilkan rekomendasi mitigasi risiko yang praktis serta dapat segera diimplementasikan sesuai prioritas organisasi.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis manajemen risiko IT di PTIPD Universitas XYZ dengan menggunakan metode OCTAVE-S, guna meningkatkan keamanan dan efisiensi sistem informasi yang ada. Penelitian ini diharapkan dapat memberikan kontribusi nyata dalam pengelolaan risiko IT serta mendukung tercapainya sistem yang lebih aman, andal, dan efisien.

METODE

Pada Tahap Pendahuluan, langkah awal dalam penelitian ini dimulai dengan menentukan topik. Proses ini diawali dengan identifikasi berbagai topik potensial yang kemudian dikaji melalui literatur dan referensi terkait. Hasilnya, topik yang dipilih adalah Analisa Manajemen Risiko IT dengan menggunakan Metode Octave-S untuk Meningkatkan Keamanan dan Efisiensi Sistem di PTIPD UIN Suska Riau. Selanjutnya, studi kasus ditentukan berdasarkan topik, yaitu di PTIPD UIN Suska Riau. Peneliti juga menetapkan subjek penelitian, yaitu manajemen risiko IT dengan fokus pada peningkatan keamanan dan efisiensi sistem.



Gambar 1. Metodologi Penelitian.

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 1, Desember 2024

Tahap Perencanaan, peneliti memulai dengan mengidentifikasi masalah melalui penyebaran kuesioner kepada pegawai PTIPD yang relevan dengan metode Octave-S. Selanjutnya, dibuat rumusan masalah, batasan, tujuan, dan manfaat penelitian. Peneliti juga menentukan data yang diperlukan, yaitu data primer yang diperoleh langsung dari karyawan PTIPD serta data sekunder dari literatur, jurnal, buku, atau dokumen terkait topik penelitian.

Tahap Pengumpulan Data melibatkan dua metode utama: studi literatur dan penyebaran kuesioner. Studi literatur digunakan untuk memperoleh data sekunder yang relevan, seperti dari buku dan jurnal. Kuesioner yang disusun berdasarkan literatur ahli di bidangnya kemudian disebarkan dalam format dokumen kepada karyawan PTIPD sebagai responden utama penelitian.

Tahap Analisis Data dilakukan dengan mempelajari responden, yang meliputi karyawan dari berbagai divisi di PTIPD, seperti Kepala PTIPD, Divisi Tata Kelola Layanan Umum, Divisi Aplikasi & Data, serta Divisi Server & Keamanan Data. Data yang diperoleh dari kuesioner diolah untuk mendapatkan hasil analisis yang mendalam [5].

Tahap Dokumentasi adalah tahap akhir penelitian dengan mendokumentasikan seluruh proses dan hasil penelitian secara sistematis. Semua data dari tahap awal hingga rekomendasi hasil analisis dirangkum dalam laporan penelitian yang berfungsi sebagai sumber informasi berguna bagi peneliti maupun pembaca.

Metode Octave-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation – Standard*) adalah kerangka kerja yang dirancang untuk membantu organisasi dalam mengelola risiko keamanan informasi dengan pendekatan sistematis [6][7]. OCTAVE-S adalah metode yang menyeluruh, metodis, terfokus, dan dapat diterapkan sendiri untuk mengevaluasi risiko keamanan informasi. Metode Octave-S meneliti masalah teknologi dalam tiga tahap untuk memberikan gambaran menyeluruh tentang persyaratan keamanan informasi suatu organisasi [8]. Penelitian ini menggunakan metode OCTAVE-S yang terdiri dari tiga tahap utama:

1. Identifikasi Aset Kritis
   Mengidentifikasi aset-aset TI yang memiliki peran penting dalam operasional PTIPD, seperti server database, jaringan lokal, aplikasi akademik, dan data mahasiswa. Data dikumpulkan melalui wawancara dengan tim IT dan dokumentasi aset.
2. Analisis Risiko
   Melakukan penilaian risiko dengan menganalisis ancaman dan kerentanan pada masing-masing aset kritis. Data diperoleh melalui observasi sistem, analisis *log* keamanan, dan survei kepada pengguna sistem.
3. Pengembangan Strategi Mitigasi
   Berdasarkan hasil analisis, dikembangkan strategi mitigasi risiko dengan prioritas pada ancaman yang memiliki tingkat risiko tertinggi. Strategi ini mencakup penguatan keamanan jaringan, pelatihan pengguna, dan peningkatan kebijakan keamanan TI.

Metode Octave-S dipilih karena pendekatannya yang sistematis, terstruktur, dan fokus pada aset kritis organisasi. Metode ini dirancang khusus untuk membantu organisasi kecil hingga menengah dalam mengevaluasi risiko keamanan informasi. Octave-S menyediakan kerangka kerja yang menyeluruh, melibatkan identifikasi aset kritis, ancaman, dan kerentanan, sehingga memungkinkan organisasi untuk merumuskan strategi mitigasi risiko secara efektif. Penelitian ini diharapkan menjadi langkah awal untuk membantu PTIPD mengelola risiko keamanan informasi secara efektif dan menciptakan lingkungan TI yang lebih aman dan efisien.

HASIL DAN PEMBAHASAN

1. Analisis Resiko

Analisis risiko dilakukan untuk mengetahui tingginya risiko yang memiliki dampak pada instansi dan teknologi informasi yang digunakan. Penilaian dilaksanakan berdasarkan lembar kerja metode Octave-S dapat dilihat pada Tabel 1.

Tabel 1. RACI Chart.

No.	Variable	Kepala PTIPD	Devisi Tata Kelola Layanan Umum	Divisi Aplikasi & Data	Divisi Server & Keamanan Data
1.	Kesadaran Keamanan Dan Pelatihan	A	C	C	C

No.	Variable	Kepala PTIPD	Devisi Tata Kelola Layanan Umum	Divisi Aplikasi & Data	Divisi Server & Keamanan Data
2.	Strategi Keamanan	A	C	R	C
3.	Manajemen Keamanan	A	C	C	R
4.	Peraturan dan Kebijakan Keamanan	A	R	C	C
5.	Manajemen Keamanan dan Kolaborasi	A	R	C	R
6.	Perencanaan Contigency	A	I	R	R
7.	Pengendalian Akses Fisik	A	I	I	R
8.	Pemantauan dan Audit Keamanan Fisik	A	I	C	R
9.	Sistem dan Manajemen Jaringan	A	I	I	R
10.	Pemantauan dan Audit Keamanan It	A	I	C	R
11.	Pengesahan dan Otoritas	A	I	R	R
12.	Manajemen Kerentanan	A	I	R	R
13.	Enkripsi	A	I	R	R
14.	Perencanaan dan Arsitektur Keamanan	A	C	R	R
15.	Manajemen Insiden	A	I	I	R

2. Identifikasi Informasi Organisasi

Langkah pertama dalam penilaian risiko adalah mengumpulkan informasi dari PTIPD untuk menentukan tingkat risiko yang dapat memengaruhi kemampuan perusahaan untuk terus beroperasi dan membuat rencana tindakan risiko.

a. Membangun Dampak Dari Kriteria Evaluasi

Berikut adalah data dari identifikasi risiko dari kriteria dampak evaluasi berdasarkan metode Oktave S, dapat dilihat pada Tabel 2.

Tabel 2. Data Identfikasi Resiko dari Kriteria Dampak Evaluasi.

No.	Kriteria Dampak	Tipe/Dampak	Level
1.	Reputasi dan Kehilangan Data	Reputasi	Sedang
		Kehilangan Data	Tinggi
2.	Keuangan	Biaya Operasional	Sedang
		Kehilangan Pendapatan	Rendah

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 1, Desember 2024

No.	Kriteria Dampak	Tipe/Dampak	Level
3.	Produktivitas	Jam Kerja	Sedang
4.	Kesehatan/Keselamatan	Kesehatan/Keselamatan Pegawai	Sedang

Berdasarkan tabel 2 diketahui bahwa Indikator reputasi berada pada level sedang dan kehilangan data berada pada tinggi, dikarenakan PTIPD Universitas XYZ telah memiliki sistem informasi *iRaise*, Audit Mutu Internal, *E-Learning*, Beasiswa dan Integrated SIVIL tetapi belum dilaksanakan dengan baik. Karena sistem dan layanan saat ini sangat bermanfaat bagi karyawan dan mahasiswa dalam pekerjaan mereka, sistem tersebut sudah memiliki reputasi yang positif. Namun, data tertentu dalam sistem tersebut kurang aman dan tidak tersedia, yang berdampak pada posisi lembaga di mata orang dan kelompok yang mungkin tertarik dengan data tersebut.

PTIPD Universitas XYZ dinilai pada tingkat sedang dalam evaluasi indikator keuangan untuk jenis dampak biaya operasional karena biaya yang diperlukan untuk pengembangan sistem, akuisisi aset, dan pemeliharaan tidak tinggi. Karena pendapatan tidak terpengaruh, dampak kehilangan pendapatan menjadi minimal. Karena karyawan akan bekerja lebih lama jika lembaga dalam bahaya, indikator produktivitas berada pada tingkat sedang. Indikator kesehatan/keselamatan PTIPD Universitas XYZ berada pada tingkat sedang karena anggota staf tidak pernah menghadapi risiko atau masalah kesehatan yang signifikan, dan masalah kesehatan apa pun yang mereka alami dapat diatasi dengan istirahat dua hingga tiga hari. Ini karena hal ini juga terkait dengan potensi pencapaian proses bisnis lembaga yang lebih rendah.

b. Identifikasi Aset Organisasi

Pada tahap ini, informasi dikumpulkan untuk upaya identifikasi aset lembaga menggunakan lembar kerja OCTAVE-S, yang berfungsi sebagai penilaian aset PTIPD. Tabel 3 menunjukkan aset organisasi berupa sistem aplikasi yang mendukung operasional PTIPD. Setiap sistem memiliki informasi, layanan, dan aset lainnya yang mendukung fungsinya. Aplikasi ini menunjukkan peran penting teknologi informasi dalam mendukung layanan organisasi, namun juga membutuhkan pengelolaan keamanan dan keberlanjutan operasional yang baik.

Tabel 4 mengidentifikasi peran dan keahlian kunci yang mendukung operasional PTIPD. Struktur sumber daya manusia mencerminkan pembagian tugas yang jelas dengan spesialisasi pada setiap divisi. Namun, efektivitas pelaksanaan tanggung jawab perlu ditinjau melalui praktik keamanan yang berjalan untuk memastikan pengelolaan yang optimal dan konsisten di setiap bagian. Pada tabel 5 memberikan kriteria evaluasi risiko berdasarkan tingkat dampak.

Tabel 3. Data Aset Organisasi Aplikasi

No.	Sistem	Informasi	Aplikasi/ Layanan	Aset Lainnya
1.	Integrated Academic Information System (IRaise)	Aktifitas Akademik, Perkuliahan, Data-Data Mahasiswa, Kinerja Dosen dan Perkuliahan Dosen.	Server, Jaringan internet, PC Tinggi Sedang Rendah Sedang	*Xampp, VS-Code/ Sublime Text, Wordpress, Laravel, Hostinger*
2.	Audit Mutu Internal	Penjadwalan Audit, Manajemen Dokumen, Pengumpulan Data, dan Pelaporan Hasil Audit.		
3.	E-Learning	Arsip Digital Dan Konten Perkuliahan Antara Dosen dan Mahasiswa.		
4.	Beasiswa	Pendaftaran Online, Pengumpulan Dokumen, Seleksi dan Penilaian, Serta Pelaporan dan Pemantauan Penerimaan Beasiswa		
5.	Integrated SIVIL	Modul Penerimaan Ijazah, Modul Penomoran, dan Modul Cetak Ijazah		

NIVEDITA
JOURNAL INFORMATICS
ISSN 3089-8366
(Media Online)
Vol. 01, No. 1, Desember 2024

Tabel 4. Data Aset Organisasi Sumber Daya Manusia

No.	Jabatan	Keahlian
1.	Kepala PTIPD	Memimpin dan mengawasi kegiatan PTIPD, mengembangkan kebijakan dan strategi TI, mengelola anggaran, berkomunikasi dengan pimpinan dan divisi lain, serta menilai kinerja TI.
2.	Divisi Tata Kelola Layanan Umum	Mengelola layanan TI, menetapkan standar, memantau kualitas layanan, dan menangani umpan balik pengguna
3.	Divisi Tata Kelola Manajemen Keuangan	Mengelola anggaran proyek TI, melakukan analisis keuangan, mengawasi pengeluaran, dan menyusun laporan keuangan untuk pengambilan keputusan
4.	Divisi Pusat Layanan Umum/Helpdesk (C3)	Memberikan dukungan teknis, mengelola tiket layanan, menyusun panduan pengguna, dan melakukan pelatihan sistem
5.	Divisi Aplikasi & Data	Mengembangkan dan memelihara aplikasi, menjaga integritas dan keamanan data, menganalisis kebutuhan pengguna, dan merencanakan pemulihan data
6.	Divisi Server & Keamanan Data	Mengelola infrastruktur server, menerapkan kebijakan keamanan data, memantau ancaman keamanan, dan menyusun rencana pemulihan bencana.
7.	Divisi Infrastruktur & Jaringan	Mengelola infrastruktur jaringan, menjamin konektivitas, memantau kinerja jaringan, dan menerapkan kebijakan keamanan jaringan

c. Mengevaluasi Praktek Keamanan Organisasi

Status lampu lalu lintas dievaluasi menggunakan temuan kuesioner, yang ditunjukkan pada Tabel 5, untuk melakukan evaluasi pada bagian praktik keselamatan.

Tabel 5. Definisi Tingkat Resiko

No.	Tingkat Level	Nilai Dampak	*Status Stoplight*	Deskripsi Tingkat Resiko dan Tindakan Diperlukan
1.	Rendah	1	*Green*	Dapat disimpulkan bahwa organisasi telah menerapkan prosedur keamanan yang baik di wilayah tersebut jika pengamatan dianggap berisiko rendah, sehingga meniadakan perlunya tindakan perbaikan.
2.	Sedang	2-3	*Yellow*	Apabila hasil observasi dinilai berisiko sedang, dapat disimpulkan bahwa bisnis hanya menerapkan prosedur keamanan pada area tertentu saja, sehingga masih terdapat celah yang mungkin memerlukan tindakan perbaikan.
3.	Tinggi	4-5	*Red*	Tindakan perbaikan harus diambil jika hasil observasi dianggap berisiko tinggi, karena ini menunjukkan bahwa organisasi tidak menerapkan praktik keamanan di area tersebut.

Tabel 6. Evaluasi Praktek Keamanan Instansi

No.	Praktek Keamanan	Stoplight		
		Red	Yellow	Green
1.	Kesadaran Keamanan dan Pelatihan			✓
2.	Strategi Keamanan		✓	
3.	Manajemen Keamanan			✓
4.	Peraturan dan Kebijakan Keamanan			✓
5.	Manajemen Keamanan dan Kolaborasi			✓
6.	Perencanaan Contingency	✓		
7.	Pengendalian Akses Fisik			✓
8.	Pemantauan dan Audit Keamanan Fisik		✓	
9.	Pemantauan dan Audit Keamanan IT			✓
10.	Pengesahan dan Otoritas		✓	
11.	Kesadaran Keamanan dan Pelatihan		✓	

No.	Praktek Keamanan	Stoplight		
		Red	Yellow	Green
12.	Manajemen Kerentanan	✓		
13.	Enkripsi			✓
14.	Perencanaan dan Arsitektur Keamanan		✓	
15.	Manajemen Insiden	✓		

Berdasarkan analisis terhadap indikator praktik keamanan PTIPD, ditemukan bahwa tiga prosedur keamanan berada dalam status lampu merah, menunjukkan belum diterapkannya prosedur keamanan di area tersebut. Tujuh praktik keamanan telah berada dalam status hijau, menandakan bahwa PTIPD berhasil menerapkan praktik keamanan dengan baik, sementara lima praktik keamanan berada dalam status kuning, yang menunjukkan adanya penerapan kebijakan keamanan, meski masih kurang memadai. Indikator pelatihan dan kesadaran keamanan menunjukkan status hijau karena PTIPD secara berkala melaksanakan program kesadaran keamanan yang efektif bagi karyawan.

Namun, indikator rencana keamanan berada pada status kuning karena meskipun ada kebijakan keamanan yang diimplementasikan, pencatatannya belum dilakukan dengan baik. Manajemen keamanan dan aturan serta pedoman keamanan berada dalam status merah-hijau karena meskipun ada tim dan kebijakan yang sesuai dengan standar ISO 27001, pelaksanaannya belum sepenuhnya optimal.

Indikator manajemen kolaborasi dan keamanan menunjukkan status hijau, mencerminkan pengelolaan yang baik dalam kerja sama tim. Sebaliknya, kesiapsiagaan darurat masih dalam status merah akibat tidak adanya persiapan kontinjensi. Pengendalian akses fisik menunjukkan status hijau karena pengelolaan yang rutin dan baik, termasuk pelabelan aset untuk identifikasi dan pelacakan. Audit dan pemantauan keamanan fisik berada dalam status merah-kuning karena meskipun terdapat sistem pemantauan, belum dilakukan audit keamanan secara rutin. Sistem dan manajemen jaringan memiliki beberapa variasi: firewall dan IDS/IPS yang baik memberikan status hijau, tetapi audit keamanan yang tidak rutin dan kurangnya manajemen kerentanan menempatkan indikator lain pada status merah-kuning atau merah.

Indikator enkripsi menunjukkan status hijau karena implementasi enkripsi ujung ke ujung, sedangkan perencanaan dan arsitektur keamanan berada dalam status kuning karena belum ada standar desain keamanan yang konsisten. Manajemen insiden berada pada status merah karena tidak adanya mekanisme manajemen insiden yang memadai. Analisis ini mencerminkan bahwa meskipun ada beberapa aspek keamanan yang dikelola dengan baik, banyak area yang memerlukan perhatian dan perbaikan untuk meningkatkan keamanan PTIPD secara keseluruhan.

3. Rekomendasi Hasil Analisis

Berdasarkan analisis prosedur keamanan PTIPD, tiga di antaranya berstatus merah, yang menunjukkan bahwa lembaga tersebut tidak menerapkan prosedur keamanan di area tersebut. Oleh karena itu, tindakan korektif harus diterapkan. Berdasarkan Tabel 7, berikut ini adalah daftar tindakan berisiko terhadap praktik keamanan yang mungkin diterapkan di masa mendatang.

Tabel 7. Daftar Tindakan Resiko

No.	Praktek Keamanan	Tindakan Resiko
1.	Perencanaan *Contingency*	Merancang langkah-langkah darurat untuk menghadapi situasi krisis, seperti kegagalan sistem atau bencana alam, guna memastikan kelangsungan operasional dan pemulihan yang cepat
2.	Manajemen Kerentanan	Mengidentifikasi, mengevaluasi, dan mengatasi kelemahan atau kerentanan dalam sistem it sebelum mereka dapat dieksploitasi oleh ancaman eksternal atau internal. Proses ini mencakup pemindaian rutin terhadap sistem, pembaruan perangkat lunak (*patching*), serta pelatihan pengguna untuk mengurangi risiko akibat human error
3.	Manajemen Insiden	Penanganan respons cepat terhadap insiden keamanan yang terjadi, seperti serangan siber, kebocoran data, atau gangguan sistem. Manajemen insiden melibatkan identifikasi insiden, mitigasi dampaknya, serta pemulihan sistem agar dapat kembali berfungsi secara normal secepat mungkin

KESIMPULAN

Berdasarkan analisis yang dilakukan, dapat disimpulkan bahwa PTIPD Universitas XYZ memiliki aset informasi kritis yaitu sistem *iRaise*, Audit Mutu Internal, *E-Learning*, Beasiswa dan Integrated SIVIL dan untuk aset manusia. Secara keseluruhan, PTIPD memiliki sistem keamanan yang kuat. Terdapat 3 praktek keamanan berada pada status *stoplight Red* yang menyimpulkan PTIPD belum melaksanakan praktek keamanan pada bagian tersebut. 5 praktek keamanan berada pada status *Yellow* hal ini menyimpulkan PTIPD sudah menerapkan praktek keamanan namun belum cukup baik, dan 7 praktek keamanan berada pada status *Green* yang menyimpulkan PTIPD sudah melaksanakan praktek keamanan tersebut dengan baik. Praktek keamanan yang berada pada status *Red* membutuhkan perhatian lebih untuk memastikan bahwa risiko dapat diminimalkan dan sistem keamanan dapat ditingkatkan ke tingkat yang lebih tinggi.

Rekomendasi yang dapat penulis berikan berdasarkan analisis yaitu pada praktek keamanan Perencanaan *Contingency*, dapat merancang langkah-langkah darurat untuk menghadapi situasi krisis, seperti kegagalan sistem atau bencana alam, guna memastikan kelangsungan operasional dan pemulihan yang cepat. Praktek keamanan Manajemen Kerentanan, dapat mengidentifikasi, mengevaluasi, dan mengatasi kelemahan atau kerentanan dalam sistem IT sebelum mereka dapat dieksploitasi oleh ancaman eksternal atau internal.

Proses ini mencakup pemindaian rutin terhadap sistem, pembaruan perangkat lunak (*patching*), serta pelatihan pengguna untuk mengurangi risiko akibat *human error*, dan pada praktek keamanan Manajemen Insiden, dapat penanganan respons cepat terhadap insiden keamanan yang terjadi, seperti serangan siber, kebocoran data, atau gangguan sistem. Manajemen insiden melibatkan identifikasi insiden, mitigasi dampaknya, serta pemulihan sistem agar dapat kembali berfungsi secara normal secepat mungkin.

DAFTAR PUSTAKA

[1] Alberts, C., & Dorofee, A. (2003). *OCTAVE Method Implementation Guide Version 2.0*. Carnegie Mellon University.

[2] Stallings, W. (2016). *Computer Security: Principles and Practice*. Pearson Education.

[3] Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Elsevier.

[4] Gui, A., Gondodiyoto, S., & Timotius, I. (2008). PENGUKURAN RESIKO Teknologi Informasi (TI) DENGAN METODE OCTAVE-S. CommIT (Communication and Information Technology) Journal, 2(1), 33. https://doi.org/10.21512/commit.v2i1.489

[5] Kurniawan, A. N., & Hanggara, B. T. (2020). Penerapan Manajemen Risiko Teknologi Informasi menggunakan Metode OCTAVE-S pada UPT Pusat Komputer Politeknik Negeri Malang. Pengembangan Teknologi Informasi Dan Ilmu Komputer, 4(6), 1802–1808.

[6] Nisa, F., Megawati, M., Hamzah, M. L., & Maita, I. (2022). Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S. Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi, 8(1), 62. https://doi.org/10.24014/rmsi.v8i1.14334

[7] Nurfadilah, D. R., Putra, W. N. H., & Rachmadi, A. (2020). Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001 : 2013 (Studi Kasus : Aplikasi E-Kinerja). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, Universitas Brawijaya, 4(9), 3014–3020.

[8] Octave, I., Dalam, -S, Manajemen, E., Sistem, R., Pada, I., Pelatihan, B., & Batam, K. (2018). Implementasi Octave-S Dalam Evaluasi Manajemen Resiko Sistem Informasi Pada Balai Pelatihan Kesehatan Batam. Jurnal Ilmiah Informatika, 6(01), 17–22. https://ejournal.upbatam.ac.id/index.php/jif/article/view/413

[9] Prabawati, V. A., Rachmadi, A., & Perdanakusuma, A. R. (2019). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 3(3), 2829–2836.

[10] Rido Butar Butar, F., Saputra, E., Marsal, A., Hamzah, M. L., Fronita, M., Studi, P., Informasi, S., Sains, F., Teknologi, D., & Riau, K. (2023). Analisis Manajemen Risiko Keamanan Sistem

Pengolahan Data Accurate Menggunakan Metode OCTAVE-S. Jurnal Sains Komputer & Informatika (J-SAKTI, 7(2), 675–685.

[11] Rohman, A. F., Ambarwati, A., & Setiawan, E. (2020). Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S. INTECOMS: Journal of Information Technology and Computer Science, 3(2), 298–310. https://doi.org/10.31539/intecoms.v3i2.1854

[12] Syamsuar, D., Firdaus, A., & Lonando, P. T. (2023). Analisis Manajemen Risiko It Pada Ikest Muhammadiyah Palembang Menggunakan Metode Octave – S. Journal of Information System Management (JOISM), 5(1), 77–83. https://doi.org/10.24076/joism.2023v5i1.1077