Informatics for Educators And Professionals: Journal of Informatics
Vol. 9, No. 1, Juni 2024, 73 - 83
E-ISSN: 2548-3412
Terakreditasi **SINTA Peringkat 5**
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Nomor: 230/E/KPT/2022
masa berlaku mulai Volume 5 Nomor 1 Tahun 2020 sampai Volume 9 Nomor 2 Tahun 2024

Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x

Mohamad Taufan Anwar [1], Utami Aryanti [2,*], Miki Wijana[3], Dwi Atmoko [4]

[1] Informatika; Universitas Masoem; Jl. Raya Cipacing No.22, Cipacing, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, (022) 7798340; e-mail: taufan0264@gmail.com
[2,3,] Sistem Informasi; Universitas Masoem; Jl. Raya Cipacing No.22, Cipacing, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, (022) 7798340; e-mail: tami.arya@gmail.com, mikiwijana@gmail.com
[4] Manajemen Informatika; Universitas Masoem; Jl. Raya Cipacing No.22, Cipacing, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, (022) 7798340; e-mail: dwiatmoko26@gmail.com

* Korespondensi: e-mail: tami.arya@gmail.com

Diterima: 4 Juni 2024 ; Review: 19 Juni 2024; Disetujui: 26 Juni 2024

Cara sitasi: Anwar MT, Aryanti U, Wijana M, Atmoko D 2024. Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x. Informatics for Educators and Professionals : Journal of Informatics. Vol 9 (1): 73-83.

Abstrak: Berbagai instansi pendidikan melakukan investasi dalam teknologi informasi sebagai upaya meningkatkan kualitas pendidikan. Perguruan Tinggi sebagai salah satu lembaga penyelenggara pendidikan tinggi yang memanfaatkan TIK dalam kegiatan operasional seperti layanan administrasi dan akademik sampai dengan kegiatan pembelajaran. Dalam implementasinya penggunaan TIK ini meningkatkan kerentanan terhadap serangan siber seperti virus, *malware, Phishing, Distributed Denial-of-service(DDoS), Ransomware*, dan pelanggaran data yang dapat menimbulkan kerugian. Penelitian ini bertujuan untuk merancang sistem manajemen pengamanan informasi (SMPI) untuk menentukan mitigasi yang tepat bagi setiap resiko keamanan informasi yang mungkin terjadi di perguruan tinggi X dengan menggunakan Standar kerangka kerja SMPI SNI ISO/IEC 27001:2013.
Standar kerangka kerja SMPI SNI ISO/IEC 27001:2013 menjelaskan panduan atau langkah-langkah dan syarat-syarat dalam membuat, menerapkan, melaksanakan, mengelola risiko, memelihara serta mendokumentasikan SMPI di lingkungan organisasi. Keberhasilan SMPI terletak pada proses manajemen risiko keamanan informasi (MRKI) dengan mengidentifikasi aset kritis untuk memprioritaskan mitigasi risiko dengan tepat. manajemen risiko keamanan informasi dilakukan menggunakan kerangka kerja Octave Allegro. Penelitian ini menghasilkan penilaian risiko berupa daftar aset, ancaman, kelemahan, nilai dampak risiko dan penanganan nya, dalam bentuk dokumen SMPI seperti ruang lingkup SMPI, Kebijakan SMPI, dan SoA (*Statement of Applicability*) untuk diimplementasikan di Perguruan Tinggi X.

Kata kunci: pendidikan tinggi, keamanan informasi, mitigasi resiko , SNI ISO/IEC 27001, OCTAVE Allegro

Abstract: *Various educational institutions ranging from elementary school to tertiary level are investing in information technology as an effort to improve the quality of education. Higher education is one of the institutions providing higher education that utilizes ICT in operational activities such as administrative and academic services to learning activities. In its*

implementation, the use of ICT increases vulnerability to cyber attacks such as viruses, malware, Phishing, Distributed Denial-of-Service (DDoS), Ransomware, and data breaches which can cause losses. This research aims to design an information security management system (SMPI) to determine appropriate mitigation for any information security risks that may occur at university X using the SMPI SNI ISO/IEC 27001:2013 framework standard.
The SMPI framework standard SNI ISO/IEC 27001:2013 explains the guidelines or steps and requirements for creating, implementing, executing, managing risk, maintaining and documenting SMPI in an organizational environment. SMPI's success lies in the information security risk management (MRKI) process by identifying critical assets to prioritize risk mitigation appropriately. Information security risk management is carried out using the Octave Allegro framework. This research produces a risk assessment in the form of a list of assets, threats, weaknesses, risk impact values and their handling, in the form of SMPI documents such as the SMPI scope, SMPI Policy, and SoA (Statement of Applicability) to be implemented at Higher Education X.

***Keywords**: higher education, information security, risk mitigation, SNI ISO/IEC 27001, OCTAVE Allegro*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) yang semakin pesat memiliki dampak besar bagi pendidikan. Berbagai instansi pendidikan melakukan investasi dalam teknologi informasi sebagai upaya meningkatkan kualitas pendidikan. Peningkatan kualitas pendidikan adalah tujuan utama sebagian besar negara berkembang seperti Indonesia[1].

Perguruan Tinggi sebagai salah satu lembaga penyelenggara pendidikan tinggi yang memanfaatkan TIK dalam kegiatan operasional seperti layanan administrasi dan akademik sampai dengan kegiatan pembelajaran. Dalam implementasinya penggunaan TIK ini meningkatkan kerentanan terhadap serangan siber seperti *virus, malware, Phishing, Distributed Denial-of-service*(DDoS), *Ransomware*, dan pelanggaran data yang dapat menimbulkan kerugian[2]. Perguruan tinggi merupakan salah satu institusi yang menjadi sasaran utama serangan siber mengingat data-data yang dimiliki perguruan tinggi merupakan data sensitif yang mencakup informasi pribadi mahasiswa, staf, dan penelitian. Termasuk nomor identifikasi, informasi keuangan, dan catatan akademik. Serangan ini tentunya dapat menimbulkan berbagai dampak bagi perguruan tinggi seperti kerugian finansial, penurunan reputasi, gangguan kegiatan operasional dan akademik, serta yang paling penting adalah kehilangan data.

Ketersediaan informasi akademik merupakan aset informasi penting bagi perguruan tinggi berdasarkan Permenrsitekdikti Nomor 61 Tahun 2016 yaitu pasal 22 bahwa perguruan tinggi bertugas dan bertanggung jawab untuk melakukan pengisian dan pengiriman data ke Pangkalan Data Pendidikan Tinggi (PDDikti). Sanksi akan dikenakan jika perguruan tinggi tidak menyampaikan laporan data akademik secara berkala dan memasukan data akademik tidak lengkap atau tidak valid ke PDDikti sebagaimana yang tercantum dalam Permenrsitekdikti Nomor 61 Tahun 2016 pada Pasal 10 butir (7) dan Pasal 12 butir (3)[3].

Mengingat informasi akademik merupakan aset penting, maka penggunaan TIK di Perguruan Tinggi harus diimbangi dengan penggunaan sistem manajemen pengamanan informasi (SMPI). Perlu adanya perencanaan pengamanan dengan mengindentifikasi resiko yang meliputi risiko serangan, bencana alam, dan kerentanan lainnya untuk menentukan mitigasi yang tepat bagi setiap resiko keamanan informasi yang mungkin terjadi.

Upaya pemerintah dalam meningkatkan keamanan informasi pada instansi pengguna TIK di Indonesia adalah dengan menerbitkan peraturan menteri terkait keamanan informasi yaitu Permenkominfo Nomor 4 Tahun 2016 mengenai Sistem Manajemen Pengamanan Informasi (SMPI) pada pasal 7 bahwa setiap penyelenggara sistem elektronik harus menerapkan standar SNI ISO/IEC 27001 dalam melakukan pengamanan informasi[4]. Standar kerangka kerja SMPI SNI ISO/IEC 27001:2013 bertujuan menjelaskan panduan atau langkah-langkah dan syarat-syarat dalam membuat, menerapkan, melaksanakan, mengelola risiko, memelihara serta mendokumentasikan SMPI di lingkungan organisasi [5].

Pada akhir tahun 2023 Perguruan Tinggi X mendapatkan serangan siber berupa serangan DdoS pada sistem pembelajaran elektronik, sistem penyimpanan dokumen daring, dan serangan malware pada beberapa website program studi. Dampak dari serangan tersebut menyebabkan layanan pembelajaran terganggu, ketersediaan sumber daya pembelajaran dan

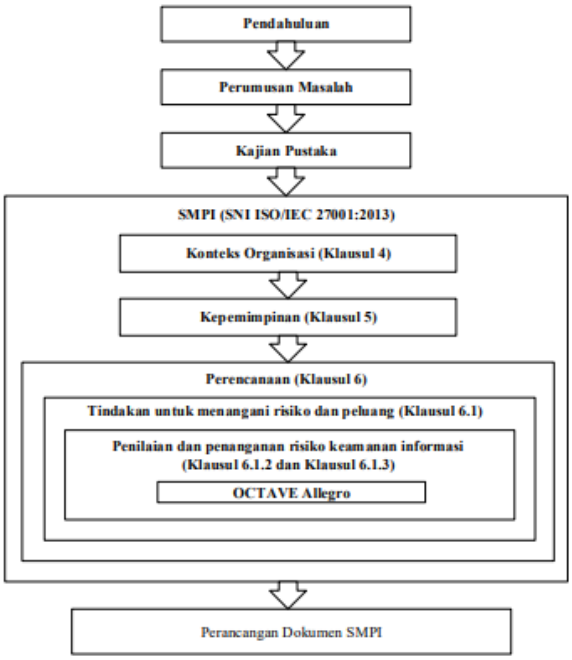
informasi menjadi tidak bisa diakses oleh civitas yang berkepentingan. Mengingat informasi akademik merupakan aset penting bagi Perguruan Tinggi, maka diperlukan suatu pengamanan informasi dalam penggunaan TIK di Perguruan Tinggi X agar setiap resiko dapat di mitigasi dengan tepat.

Penelitian pada tahun 2001 dengan judul Penilaian Resiko Teknologi Informasi dan Keamanan Informasi Menggunakan *Framework* NIST SP 800-30 (Studi Kasus : E-Learning Universitas Pembangunan Nasional Veteran Jakarta) telah dilakukan oleh Aditya Rizky,dkk[6]. Penelitian ini hanya melakukan penilaian resiko pada sistem *E-Learning* saja tanpa menentukan mitigasi untuk setiap resiko yang teridentifikasi. Selain itu, metode penilaian resiko yang digunakan adalah kerangka kerja NIST SP 800-30 yang memiliki cakupan yang luas dan dilakukan secara manual, sehingga penggunaan metode tersebut relatif membutuhkan waktu yang lebih lama.

Penelitian ini akan merancang suatu sistem manajemen pengamanan informasi dengan framework ISO 27001 berbasis manajemen resiko OCTAVE Allegro. Keberhasilan SMPI terletak pada proses manajemen risiko dengan mengidentifikasi aset kritis untuk memprioritaskan mitigasi risiko dengan tepat. OCTAVE Allegro merupakan kerangka kerja MRKI yang sangat efektif dimana tahapan dalam metode ini tersusun secara terstruktur dan sistematis dalam bentuk panduan berupa worksheet sehingga dapat membantu organisasi dalam melakukan manejemen keamanan aset informasi[7].

2. Metode Penelitian

Metode penelitian ini memaparkan tahapan-tahapan yang dilakukan untuk menentukan mitigasi resiko yang tepat untuk setiap penilaian resiko yang terdidentifikasi di perguruan tinggi X penelitian sampai dengan didapatkan hasil penelitian dan kesimpulan nya. Metode penelitian menggunakan pendekatan kualitatif yang mengkolaborasikan SNI ISO/IEC 27001:2013 sebagai kerangka kerja pembuatan sistem manajemen keamanan informasi dan OCTAVE Allegro sebagai kerangka kerja penilaian resiko.



Sumber: Hasil Penelitian (2024)

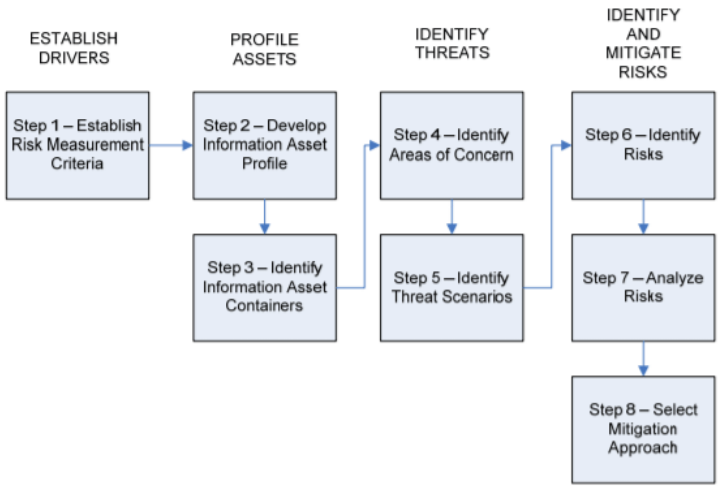
Gambar 1. Metode Penelitian

Berikut adalah tahapan yang dilakukan pada penelitian ini :

1. Tahap awal untuk memulai penelitian ini yaitu pendahuluan. Pada tahap ini penulis mengumpulkan data primer dan sekunder dengan metode wawancara, kuisoner , telaah dokumen, dan observasi.

2. Tahap selanjutnya adalah melakukan analisis terhadap hasil dari tahap pendahuluan sehingga didapatkan suatu rumusan permasalahan.
3. Kemudian dilakukan kajian pustaka terkait ISO/IEC 27001 dan OCTAVE Allegro untuk menambah pemahaman terkait kerangka kerja yang digunakan pada penelitian ini sehingga solusi bisa didapatkan.
4. Langkah selanjutnya melakukan manajemen risiko sesuai dengan standard SMPI yang dipilih yaitu SNI ISO/IEC 27001:2013. Dalam standar ini, terdapat dua komponen utama yang sering dibahas yaitu klausa dan annex. Klausa dalam ISO 27001 menguraikan persyaratan manajemen yang harus dipenuhi oleh organisasi untuk membangun, mengimplementasikan, memelihara, dan terus meningkatkan SMPI organisasi[8]. Klausa ini membentuk struktur dan kerangka kerja standar. Mitigasi risiko keamanan informasi adalah bagian penting dari ISO 27001, dan ini terutama diatur dalam beberapa klausa utama yang berfokus pada perencanaan, operasi, dan evaluasi kinerja. Mitigasi pada penelitian ini dibatasi hingga tahap perencanaan, sehingga klausa SNI ISO/IEC 27001:2013 yang digunakan adalah klausa 4, 5, dan 6. Kerangka kerja OCTAVE Allegro digunakan dalam penilaian resiko. OCTAVE adalah seperangkat alat, teknik dan metode untuk penilaian dan perencanaan keamanan sistem informasi berbasis risiko. Metode OCTAVE merupakan singkatan dari *Operationally, Critical, Threat, Asset, Vulnerability, and Evaluation* yang digunakan untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Metode OCTAVE melakukan penilaian risiko berdasarkan tiga prinsip dasar, yaitu [9]:
    a. Kerahasiaan adalah proses mengamankan dan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang orang. Informasi ini biasanya berkaitan dengan data pribadi dan bersifat rahasia.
    b. Integritas, adalah memastikan seluruh data tersedia secara utuh dan lengkap.
    c. Availability, berusaha membuat data dapat diakses kapan saja, tanpa penundaan, dan tersedia secara utuh tanpa cacat.

OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE Allegro adalah sebuah metode penilaian risiko yang berfokus pada aset informasi. OCTAVE Allegro terdiri dari delapan langkah yang dibagi menjadi empat tahapan sebagai berikut :



Gambar 2. Phases and Stages of OCTAVE Allegro

Gambar diatas menjelaskan fase pada kerangka kerja Octave Allegro diantaranya :

a. *Establish Drivers*. Fase pertama dalam OCTAVE Allegro adalah menetapkan tolok ukur atau kriteria yang digunakan oleh perguruan tinggi untuk menilai dampak risiko terhadap misi dan tujuan bisnis.
b. *Profile Assets*. Tahap kedua adalah menentukan profil asset informasi, dimana aset-aset yang menjadi focus dalam penilaian risiko diprofilkan. Untuk mengembangkan profil aset informasi dilakukan pengelompokan terhadap aset utama dan aset pendukung pada perguruan tinggi.
c. *Identify Threats*. Pada fase ini ancaman terhadap aset informasi diidentifikasi dan dikumpulkan melalui proses yang terstruktur.
d. *Identify and Mitigate Risk*. Risiko diidentifikasi dan dianalisis berdasarkan ancaman informasi, dan strategi mitigasi dikembangkan untuk mengatasinya risiko-risiko ini.

5. Berdasarkan hasil penilaian dan pengamanan resiko maka dirancang dokumen SMPI yang terdiri dari ruang lingkup SMPI, Kebijakan SMPI, dan *Statement of Applicability* (SoA) untuk diimplementasikan di Perguruan Tinggi X[10].

ISO/IEC 27001 menjadi standar yang paling populer dan banyak digunakan. ISO/IEC 27001 digunakan dengan presentase 27% dibanding framework lainnya, yaitu COBIT (26%), ITIL (8%), BS7799 (18%), dan PCIDSS (21%). ISO/IEC 27001 dapat digunakan pada semua jenis organisasi, karena standar yang fleksibel, dan dapat disesuaikan dengan kebutuhan dan kondisi organisasi[11].

3. Hasil dan Pembahasan

ISO 27001 adalah standar internasional untuk sistem manajemen pengamanan informasi (SMPI) yang mencakup berbagai persyaratan dan kontrol untuk memastikan keamanan informasi dalam suatu organisasi. Terdapat 11 klausul pada ISO 27001. Hasil dan pembahasan dari 3 klausa yang digunakan pada penelitian ini adalah sebagai berikut[12] :

Klausa 4: Konteks Organisasi

Klausa ini menuntut Perguruan Tinggi X untuk memahami konteks eksternal dan internal yang dapat mempengaruhi keamanan informasi. Perguruan Tinggi X harus memahami persyaratan dan ekspektasi pemangku kepentingan terkait dengan keamanan informasi. Berdasarkan hasil wawancara dan observasi berikut merupakan konteks eksternal dan internal yang teridentifikasi dapat mempengaruhi keamanan informasi di Perguruan Tinggi X :

Konteks Eksternal

1. Perguruan Tinggi X sebagai salah satu lembaga penyelenggara pendidikan tinggi yang memanfaatkan TIK harus menerapkan standar SNI ISO/IEC 27001 dalam melakukan pengamanan informasi sesuai Permenkominfo Nomor 4 Tahun 2016 mengenai Sistem Manajemen Pengamanan Informasi (SMPI) pada pasal 7.
2. Perguruan Tinggi X harus dapat mengatasi setiap ancaman siber yang mungkin terjadi seperti serangan DDoS pada sistem pembelajaran elektronik, sistem penyimpanan dokumen daring, dan serangan malware pada beberapa website program studi yang telah terjadi sebelumnya.

Konteks Internal

1. Perguruan Tinggi X harus memiliki kebijakan keamanan informasi yang ketat dan prosedur operasi standar untuk menangani data akademik.
2. Perguruan Tinggi X memiliki tim IT yang terlatih untuk menangani insiden keamanan dan memastikan kepatuhan terhadap kebijakan internal. Tim IT mengidentifikasi setiap aset yang dibutuhkan untuk mengelola data akademik yaitu informasi, personel, prosedur, data, perangkat lunak, perangkat keras, dan teknologi jaringan yang digunakan.

Klausa 5 : Kepemimpinan

Klausa 5 dari ISO 27001 berfokus pada kepemimpinan. Klausa 5 mencakup komitmen dari manajemen puncak untuk mendukung sistem manajemen pengamanan informasi (SMPI). Berikut adalah beberapa langkah konkret bagaimana kepemimpinan dapat diterapkan dalam SMPI Perguruan Tinggi X sesuai dengan persyaratan Klausa 5:

1. Manajemen puncak menetapkan tujuan keamanan informasi yang jelas dan terukur, seperti pengurangan insiden serangan siber sebesar 15% dalam satu tahun, dan memasukkan tujuan ini dalam rencana strategi perguruan tinggi.
2. Manajemen puncak menunjukkan komitmennya dengan mengalokasikan anggaran yang memadai untuk keamanan informasi, termasuk pembelian perangkat lunak keamanan, pelatihan karyawan, dan penambahan staf keamanan informasi.
3. Manajemen puncak mendirikan tim keamanan informasi sehingga memastikan peran, tanggung jawab, dan wewenang yang jelas untuk sistem manajemen keamanan informasi data akademik. Struktur Tim pengelola SMPI di Perguruan Tinggi X yaitu :
   a) Pimpinan (ITC Advisor)
   b) Pengendali SMPI (Kepala PTI)
   c) Pemimpin SMPI (Kabag dan Kasubag PTI)
   d) Tim Penerapan SMPI (Subbag Operasional, Pengembangan, dan Pengelolaan Informasi)

Kepemimpinan Perguruan Tinggi X memastikan bahwa semua kebijakan dan tindakan yang diambil selaras dengan regulasi eksternal dan mendukung struktur tim pengelola SMPI internal dalam mengimplementasikan sistem manajemen pengamanan informasi akademik.

Klausa 6 : Perencanaan

Klausa 6 dari ISO 27001 mengharuskan organisasi untuk merencanakan tindakan yang diperlukan untuk mengatasi risiko dan peluang terkait keamanan informasi. Implementasi Klausa 6 mencakup identifikasi risiko, penilaian risiko, pengendalian risiko, dan perencanaan tujuan keamanan informasi. Kerangka kerja manajemen resiko keamanan informasi (MRKI) yang digunakan untuk menilai risiko keamanan informasi pada penelitian ini adalah metode OCTAVE Allegro. Berikut adalah hasil penilaian resiko berdasarkan tahapan pada kerangka kerja OCTAVE Allegro :

Langkah 1. Tetapkan Kriteria Pengukuran Risiko

Pada tahap awal OCTAVE Allegro dilakukan wawancara dengan seluruh manajemen yang terkait dengan data akademik, yaitu : Kepala IT, Kepala Biro Bagian Akademik, Kepala Biro Keuangan, dan staf yang terkait dengan data akademik. Hasil wawancara diguna dalam menetapkan tolok ukur yang akan digunakan oleh Perguruan Tinggi X untuk menilai dampak risiko berdasarkan misi dan tujuan bisnis Perguruan Tinggi. Dari hasil wawancara, salah satu kriteria pengukuran risiko di Perguruan Tinggi X dapat dilihat pada Tabel 1 berikut:

Tabel 1: Contoh Kriteria Pengukuran Risiko

Allegro Worksheet 1	**KRITERIA PENGUKURAN RISIKO – REPUTASI DAN KEPERCAYAAN PELANGGAN**		
Area Dampak	**Rendah**	**Sedang**	**Tinggi**
Reputasi	Reputasi sedikit terganggu, dan tidak diperlukan biaya atau upaya untuk memulihkan reputasi	Reputasi rusak, dan diperlukan upaya untuk melakukan pemulihkan reputasi	Reputasi rusak permanen atau idak dapat diperbaiki
Kepercayaan Konsumen (Mahasiswa, Dosen, dan Staff)	Pengurangan penerimaan mahasiswa baru kurang dari 1%	Pengurangan penerimaan mahasiswa baru antara 5% hingga 10%	Pengurangan penerimaan mahasiswa baru lebih dari 50%
...	...	...	...

Sumber: Hasil Penelitian (2024)

Prioritaskan area dampak berdasarkan kriteria pengukuran risiko. Urutkan dari yang paling penting. Berdasarkan wilayah dampak paling penting terhadap Perguruan Tinggi, maka dapat dilihat prioritas wilayah dampak pada Tabel 2 berikut:

Tabel 2: Prioritas Wilayah Dampak

Allegro Worksheet 7	**PRIORITASISASI AREA DAMPAK**
Prioritas	**AREA DAMPAK**
5	Reputasi
4	Produktifitas Operasional
3	Keuangan
2	Keamanan Pengguna
1	Denda dan Hukuman

Sumber: Hasil Penelitian (2024)

Langkah 2. Mengembangan Profil Aset Informasi

Untuk mengembangkan profil aset informasi, hal pertama yang perlu dilakukan adalah mengidentifikasi kumpulan aset utama dan aset pendukung di Perguruan Tinggi. Informasi akademik merupakan aset informasi utama bagi perguruan tinggi, dimana aset informasi ini paling sering digunakan dalam proses kerja operasional dan memberikan kontribusi sebagai tolak ukur pencapaian tujuan Perguruan Tinggi. Aset informasi akademik diprofilkan menggunakan Lembar Kerja 8 Oktaf Allegro seperti Tabel 3

Tabel 3: Profil Aset Informasi– Informasi Akademik

Allegro Worksheet 8	**PROFIL ASET INFORMASI KRITIS**	
(1) Aset Kritis	**(2) Alasan Pemilihan**	**(3) Deskripsi**
Informasi Akademik	Sebagai pedoman dalam mengelola proses bisnis akademik dimulai dari Pendaftaran, keuangan mahasiswa baru, pelaksanaan pembelajaran, penelitian, dan PKM hingga penanganan mahasiswa yang lulus dari perguruan tinggi yang merupakan bisnis inti perguruan tinggi. Informasi akademik juga digunakan untuk pelaporan administrasi akademik perguruan tinggi.	Informasi Aakademik dikelola pada sistem berbasis komputer yang terhubung ke internet yang bisa menerima, mengirim, menyimpan, memproses dan menyajikan data dan informasi terkait proses bisnis akademik. Aset data/informasi akademik terdiri dari data keuangan yang termasuk data tagihan biaya kuliah dan data riwayat pembayaran, data mahasiswa yang meliputi data pribadi, studi rencana, hasil belajar, kehadiran, transkrip, data jadwal perkuliahan termasuk jadwal perkuliahan dan kurikulum. Data penelitian, dan data PKM.
(4) Pemilik Aset Informasi		
Biro Administrasi Akademik, Biro Keuangan, Pusat Teknologi Informasi (IT), Dosen, Mahasiswa		
(5) Persyaratan Keamanan		
Kerahasiaan (*Confidentiality*)	Hanya personel yang berwenang yang dapat melihatnya aset informasi akademik. Akses terhadap informasi akademik dibatasi berdasarkan pengguna tertentu dari Biro Akademik, Biro Keuangan, ITC dan pengguna yang telah ditentukan oleh sistem	
Integritas (*Integrity*)	Hanya personel berwenang yang dapat membuat data baru dan atau melakukan perubahan pada data, sehingga proses pengumpulan, pengolahan dan penyajian informasi untuk pengambilan keputusan dapat dipertanggungjawabkan.	
Ketersediaan (*Availability*)	Informasi harus tersedia sesuai dengan kebutuhan dan otoritas masing-masing pengguna kapan saja diperlukan, khususnya pada saat jam bekerja ketika proses bisnis akademik berjalan.	
(6) Persyaratan Keamanan Paling Penting		
Availability		

Sumber: Hasil Penelitian (2024)

Langkah 3 - Mengindentifikasi kontainer aset informasi

Kontainer aset informasi adalah tempat di mana aset informasi disimpan, diangkut, diproses, atau di mana aset informasi "hidup". Kontainer aset diklasifikasikan menjadi tiga kategori, yaitu: Teknis (mencakup perangkat keras, perangkat lunak, sistem aplikasi, server, dan jaringan),fisik (mencakup item seperti folder file tempat informasi disimpan), dan pengguna (mencakup pihak internal dan pihak eksternal yang terlibat dengan aset informasi). Dalam penelitian ini teridentifikasi 20 kontainer aset informasi, salah satunya dapat dilihat pada Tabel 4:

Tabel 4: Peta Lingkungan Risiko Aset Informasi (Teknis)

Allegro Worksheet 9a	PETA LINGKUNGAN RISIKO ASET INFORMASI (TEKNIS)	
	INTERNAL	
	DESKRIPSI KONTAINER	PEMILIK
1	Aplikasi web sistem informasi akademik merupakan tempat untuk data tagihan, pembayaran biaya kuliah dan data akademik yang terdiri dari database server dan aplikasi/web.	Biro Akademik, Biro Keuangan , dan IT.
2	Perangkat lunak berbasis web untuk kegiatan belajar mengajar dengan konsep pembelajaran elektronik atau e-learning, memiliki fitur untuk mengelola materi dan tugas matakuliah.	Biro Akademik dan IT
3	Perangkat server tempat semua transaksi diproses dan disimpan. internal perguruan tinggi	IT

Sumber: Hasil Penelitian (2024)

Langkah 4: Mengidentifikasi area yang menjadi perhatian

Identifikasi Area perhatian menjelaskan deskripsi rinci tentang kondisi atau situasi dunia nyata yang mungkin mempengaruhi aset informasi di perguruan tinggi. Berdasarkan kontainer aset informasi penting yang diidentifikasi sebelumnya, ditemukan 23 area perhatian. Tabel 5 adalah beberapa bidang yang menjadi perhatian yang teridentifikasi di perguruan tinggi X :

Tabel 5. *Area of Concern*

No Area of Concern (AC)	*Area of Concern*
1	Terdapat bug pada aplikasi web sistem informasi akademik sehingga data bisa diakses dan atau diubah oleh pihak yang tidak berkepentingan. Selain itu bug juga bisa menyebabkan terganggunya layanan akademik atau proses bisnis.
2	Server aplikasi web sistem informasi akademik dan perangkat lunak *e-learning down* sehingga layanan tidak dapat diakses atau terganggu.
3	Serangan *Denial-of-service* (DoS) terhadap perangkat lunak *elearning* oleh peretas yang dapat merender layanan *elearning* sehingga tidak dapat digunakan

Sumber: Hasil Penelitian (2024)

Langkah 5 : Mengidentifikasi Skenario Ancaman

Identifikasi skenario ancaman dilakukan berdasarkan Peta Lingkungan Aset Informasi yang dibuat pada Langkah 3 (Lembar Kerja 9a) sebagai panduan. Lembar Kerja Risiko Aset Informasi dibuat untuk menggambarkan properti skenario dari setiap area perhatian (*area of concern)* secara rinci. Tabel 6 merupakan salah satu contoh lembar kerja risiko aset informasi untuk *area of concern nomor* 1.

Tabel 6. Lembar Kerja Risiko Aset Informasi

	Allegro Worksheet 10	LEMBAR KERJA RISIKO ASET INFORMASI			
Threat	Aset Informasi	Informasi Akademik			
	Area of Concern	Terdapat bug pada aplikasi web sistem informasi akademik sehingga data bisa diakses dan atau diubah oleh pihak yang tidak berkepentingan. Selain itu bug juga bisa menyebabkan terganggunya layanan akademik atau proses bisnis.			
	Aktor (*Actor*)	*Hacker* (Peretas).			
	Cara (*Means*)	Menggunakan Scanning toolkit, kemudian melakukan serangan injeksi.			
	Motif (*Motive*)	Hiburan, Ekonomi			
	Hasil (*Outcome*)	Penyingkapan	Modifikasi	Penghancuran	Gangguan
	Persyaratan Keamanan	Aplikasi seharusnya dilindungi dari injeksi			

Sumber: Hasil Penelitian (2024)

Lembar kerja resiko aset informasi diatas menjelaskan bahwa aset informasi akademik memiliki wilayah perhatian (*area of concern*) adalah *bug* pada aplikasi web sistem informasi akademik sehingga data bisa diakses dan atau diubah oleh pihak yang tidak berkepentingan. Aktor yang menjadi pelaku pada skenario ancaman ini adalah *hacker* dengan menggunakan *Scanning toolkit*, kemudian melakukan serangan injeksi. Motif dalam menjalankan skenario ancaman ini ada hiburan atau motif ekonomi. Skenario ancaman ini dapat menyebabkan modifikasi data oleh pihak yang tidak berwenang, penghancuran data, dan terganggunya layanan akademik atau proses bisnis.

Langkah 6 : Mengidentifikasi Resiko

Pada langkah ini dilakukan identifikasi terhadap dampak dan konsekuensi yang diterima perguruan tinggi X. Identifikasi terhadap dampak dan konsekuensi resiko dilakukan berdasarkan setiap skenario ancaman yang didokumentasikan pada lembar kerja risiko aset informasi pada langkah sebelumnya. Tabel 8 menunjukan dampak yang diterima Perguruan Tinggi X untuk setiap skenario ancaman yang diidentifikasi pada tahapan sebelumnya :

Tabel 7. Identifikasi Resiko

No	Skenario Ancaman	Konsekuensi
1	Terdapat bug pada aplikasi web sistem informasi akademik sehingga data bisa diakses dan atau diubah oleh pihak yang tidak berkepentingan. Selain itu bug juga bisa menyebabkan terganggunya layanan akademik atau proses bisnis.	Penyelenggaraan layanan akademik dan/atau *e-learning* terganggu atau bahkan terhenti. Bug di situs web aplikasi bisa menjadi pintu untuk meretas sistem lain yang dapat menyebabkan kerugian finansial dan penurunan nilai reputasi Perguruan Tinggi X.
2	Server aplikasi web sistem informasi akademik dan perangkat lunak e-learning down sehingga layanan tidak dapat diakses atau terganggu.	Proses belajar mengajar akan terganggu. Penambahan jam kerja bagi pegawai IT meningkat tergantung kerusakan yang dialami oleh server.
3	Serangan *Denial-of-service* (DoS) terhadap perangkat lunak elearning oleh peretas yang dapat merender layanan elearning sehingga tidak dapat digunakan	Layanan *e-learning* lumpuh yang menyebabkan penurunan produktivitas dan reputasi Perguruan Tinggi X..

Sumber: Hasil Penelitian (2024)

Langkah 7 : Analisis Resiko

Mengacu pada kriteria pengukuran risiko yang dibuat pada Langkah 1, klasifikasikan konsekuensi dari setiap ancaman terhadap Perguruan Tinggi sesuai dengan kriteria rendah, sedang, dan tinggi.

Tabel 8. Analisis Resiko

Area Perhatian *(Area of Concern)*	Konsekuensi	Area dampak *(Impact Area)*	*Ranking*	Nilai Dampak *(Impact Value)*	*Score*
AC. 1	1	Reputasi	1	Rendah(1)	1
		Produktifitas Operasional	2	Rendah(1)	2
		Keuangan	3	Rendah(1)	3
		Keamanan Pengguna	4	Menengah(2)	8
		Denda dan Hukuman	5	Menengah(2)	10
				Total Skor	**24**
AC. 2	2	Reputasi	1	Rendah(1)	1
		Produktifitas Operasional	2	Menengah(2)	4
		Keuangan	3	Rendah(1)	3
		Keamanan Pengguna	4	Tinggi(3)	12
		Denda dan Hukuman	5	Tinggi(3)	15
				Total Skor	**35**
AC. 3	**3**	Reputasi	1	Rendah(1)	1
		Produktifitas Operasional	2	Menengah(2)	4
		Keuangan	3	Rendah(1)	3
		Keamanan Pengguna	4	Menengah(2)	8
		Denda dan Hukuman	5	Tinggi(3)	15
				Total Skor	**31**

Sumber: Hasil Penelitian (2024)

Langkah 8 : Pemilihan Pendekatan Mitigasi

Pada langkah ini dilakukan pemilihan pendekatan mitigasi yaitu pertimbangan untuk menerima risiko, menguranginya, atau menundanya berdasarkan beberapa faktor yang berhubungan dengan kondisi di Perguruan Tinggi X. Kegiatan pertama adalah memilah setiap risiko yang teridentifikasi berdasarkan skor risikonya. Mengkategorikan risiko berdasarkan skor risiko relatif dapat membantu dalam pengambilan keputusan mengenai status mitigasinya. Pengkategorian skor risiko relatif dapat dilihat pada Tabel 9 :

Tabel 9. Matrik Skor Resiko Relatif

MATRIK SKOR RESIKO RELATIF

	SKOR RESIKO		
SKOR RELATIF	40 – 45	16-39	0-15
POOL	POOL 1	POOL 2	POOL 3
PENDEKATAN MITIGASI	Mitigasi	Mitigasi atau Ditunda	Diterima

Sumber: Hasil Penelitian (2024)

Tindakan mitigasi terhadap kontainer aset dengan pendekatan tertentu sebagai solusi terhadap risiko. Mitigasi risiko yang dilakukan bisa terdiri dari pengendalian administratif, teknis dan fisik. Hasil akhir perhitungan pemilihan pendekatan mitigasi dapat dilihat pada Tabel 10 :

Tabel 10. Pendekatan Mitigasi

Area of Concern	Skor Resiko Relatif	Pool	Pendekatan Mitigasi
AC. 1	24	POOL 2	Mitigasi atau Ditunda
AC. 2	35	POOL 1	Mitigasi
AC. 3	31	POOL 1	Mitigasi

Sumber: Hasil Penelitian (2024)

Perancangan Dokumen SMPI

Mengacu pada seluruh kegiatan analisis manajemen pengamanan informasi berdasarkan integrasi SNI ISO/IEC 27001:2013 dan OCTAVE Allegro, maka diharuskan ada nya perancangan dokumen SMPI sebagai hasil dari pelaksanaan klausul 4 sampai dengan klausul 6 SNI ISO/IEC 27001:2013.

Dokumen yang dirancang yaitu dokumen level manajemen yaitu

1) Dokumen ruang lingkup SMPI : dokumen ini bertujuan menjelaskan ruang lingkup dan batasan penerapan SMPI di TI Perguruan Tinggi X, berisi komitmen manajemen dalam mendukung dan menerapkan SMPI, ruang lingkup terkait bisnis proses di departemen IT, penjelasan tentang tim pengelola SMPI IT, lokasi dan topologi jaringan yang dikelola IT.
2) Dokumen kebijakan SMPI : dokumen ini bertujuan menunjang tujuan bisnis dengan memastikan confidentiality, integrity, dan availability dari setiap aset informasi yang penting bagi PTI.
3) Dokumen SoA (*Statement of Applicability*) : berisi daftar Annex A SNI ISO/IEC 27001:2013 dengan penambahan status penerapan saat ini, alasan penerapan atau tidak diterapkan.

Penilaian risiko dilakukan pada tahap klausul 6 (Perencanaan) SNI ISO/IEC 27001:2013 dengan melakukan kegiatan pada langkah-langkah OCTAVE Allegro sehingga dihasilkan 23 skenario risiko (area perhatian) dari 1 aset kritis yaitu data/informasi akademik yang dikelola IT Perguruan Tinggi X. Hasil penilaian risiko pengelolaan data/informasi akademik di IT Perguruan Tinggi X menunjukan risiko tertinggi terjadi pada proses pemutakhiran data, dengan empat kategori risiko tinggi (skor risiko relatif: 41, 34,39, 41) dan lima kategori risiko sedang (skor risiko relatif : 36, 30, 35, 32, 30).

4. Kesimpulan

Berdasarkan hasil penilaian resiko yang dilakukan pada penelitian ini terhadap informasi akademik perguruan tinggi x ditemukan 10 risiko dengan kategori rendah, 5 risiko kategori sedang, dan 4 risiko kategori tinggi, dengan jumlah kendali keamanan informasi sebanyak 47 rekomendasi pengendalian yang mengacu pada Annex A SNI ISO/IEC 27001:2013. Dihasilkan rangkaian dokumen SMPI tingkat 1 (Kebijakan & standar) yang digunakan untuk mengatur kebijakan dan standar mitigasi dari setiap kategori resiko. Dokumen tersebut berupa Dokumen Ruang Lingkup SMPI pada klausul 4 (Kontek Organisasi), Dokumen Kebijakan SMPI pada klausul 5 (Kepemimpinan), dan Dokumen SoA pada klausul 6 (Perencanaan). Saran perbaikan penelitian atau untuk penelitian selanjutnya adalah sebagai berikut: 1) Rekomendasi pengendalian dari hasil penelitian dapat diterapkan di IT , mengingat IT belum memiliki perencanaa sistem manajemen pengamanan informasi berbasis manajemen risiko. 2) IT disarankan melakukan proses manajemen resiko keamanan informasi secara berkala sehingga ketika terjadinya perubahan pada organisasi maka resiko yang ada dapat diidentifikasi sehingga bisa ditangani dan diantisipasi secara tepat dan cepat. 3) Perencanaan

SMPI pada penelitian ini dapat dilanjutkan ke tahap selanjutnya yaitu implementasi bagi IT maupun peneliti atau kalangan akademik untuk penelitian selanjutnya.

Referensi

[1] P. M. Endraswari, N. Tou, and U. F. Vista, "Penggunaan Teknologi Informasi dalam Meningkatkan Mutu Kerja di Lingkungan Taman Kanak-Kanak Kecamatan Paguyangan," *J. Abdimas BSI J. Pengabdi. Kpd. Masy.*, vol. 6, no. 2, pp. 173–181, 2023.

[2] U. Aryanti, M. T. Anwar, and T. Rahmawati, "Information Security Risk Management Using OCTAVE Allegro Method at University," *Int. J. Ethno-Sciences Educ. Res.*, vol. 3, no. 4, pp. 137–145, 2023.

[3] P. Kementrian Riset, Teknologi, "Peraturan Kementrian Riset, Teknologi, dan Pendidikan No. 61 Tahun 2016." [Online]. Available: https://peraturan.bpk.go.id/Home/Download/133228/Permenristekdikti%0A Nomor 61 Tahun 2016.pdf

[4] Kementrian Komunikasi dan Informatika, *Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi", Kemenkominfo [Online].* Online, 2016. [Online]. Available: https://jdih.kominfo.go.id/produk_hukum/unduh/id/532/t/peraturan+m%0Aenteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+%0A11+april+2016

[5] BSN, "Badan Standardisasi Nasional, 'BSN dukung PPATK dalam Penerapan SNI ISO/IEC 27001:2013.'" [Online]. Available: https://bsn.go.id/main/berita/detail/11183/bsn-dukung-ppatk-dalam%02penerapan-sni-isoiec-27001201

[6] A. Rizky, A. Setyawan, A. Albert, K. Kraugusteeliana, and M. R. A. Pramudya, "Penilaian Resiko Teknologi Informasi dan Kemanan Informasi Menggunakan Framework NIST SP 800-30 (Studi Kasus: E-Learning Universitas Pembangunan Nasional Veteran Jakarta)," in *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya*, 2021, pp. 449–455.

[7] A. Pakarbudi, D. T. Piay, D. Nurmadewi, and A. Rachman, "Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi," *JURIKOM (Jurnal Ris. Komputer)*, vol. 10, no. 2, pp. 488–496, 2023.

[8] T. Tutik, N. Mutiah, and I. Rusi, "ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001: 2013 (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Sambas)," *Coding J. Komput. dan Apl.*, vol. 10, no. 02, pp. 249–261, 2022.

[9] M. Sukri and I. Riadi, "Risk Management Analysison Administration System Using Octave Allegro Framework," *Int. J. Comput. Appl.*, vol. 975, p. 8887, 2021.

[10] H. Jauhary, G. E. Pratiwi, A. Z. Salim, and F. Fitroh, "Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi: Literatur Review," *Media J. Inform.*, vol. 14, no. 1, pp. 43–49, 2022.

[11] I. D. Sánchez-García, J. Mejía, and T. San Feliu Gilabert, "Cybersecurity risk assessment: a systematic mapping review, proposal, and validation," *Appl. Sci.*, vol. 13, no. 1, p. 395, 2022.

[12] iso, "ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en