

Analisis Penilaian Resiko Keamanan Sistem Informasi Akademik

Security Risk Assessment Analysis Academic Information System

Dwi Yana Ayu Andini¹, Citra Anisa²

^{1,2}Universitas Aisyah Pringsewu, Indonesia

Article Info	ABSTRAK
Kata Kunci: <i>ISO 27002, Octave Allegro, Penilaian Resiko</i>	Sistem Informasi Akademik (SIKAD) dibuat untuk memudahkan penyebaran informasi akademik pada institusi perguruan tinggi. Universitas Aisyah Pringsewu (UAP) saat ini belum menerapkan penilaian resiko terhadap Sistem Informasi Akademik (SIKAD). Hal ini menyebabkan potensi terjadinya resiko keamanan seperti kebocoran data, informasi, dan gangguan teknis yang mempengaruhi proses bisnis dalam Universitas Aisyah Pringsewu (UAP). Penilaian resiko pada SIKAD Universitas Aisyah Pringsewu menggunakan metode Octave Allegro dan ISO 27002. Pada metode Octave Allegro terdapat 8 tahapan yang hasilnya disesuaikan dengan klausul ISO 27002 yang berkaitan. Hasil dari perhitungan nilai ancaman metode Octave Allegro didapatkan bahwa lingkungan terimbas yang memiliki skor tertinggi adalah keandalan dan pengguna yaitu 38. Selanjutnya hasil control keamanan informasi diterapkan dalam klausul ISO 27002 pada setiap area perhatian. Mengacu pada pendekatan mitigasi, kebijakan keamanan Sistem Informasi Akademik (SIKAD) yang direkomendasikan terdiri dari Panduan Keamanan Informasi SIKAD, Instruksi Kerja SIKAD, Prosedur Keamanan SIKAD, Formulir Keamanan SIKAD. Penelitian ini masih memiliki kekurangan, yaitu keterbatasan data yang diperoleh dari pengguna Sistem Informasi Akademik (SIKAD) khususnya mahasiswa. Penelitian ini masih memiliki kekurangan, yaitu keterbatasan data yang diperoleh dari pengguna SIKAD khususnya mahasiswa.
Keywords: <i>Risk Assessment Octave Allegro ISO 27002</i>	ABSTRACT The Academic Information System (SIKAD) was created to facilitate the dissemination of academic information at higher education institutions. Aisyah Pringsewu University (UAP) currently has not implemented a risk assessment of the Academic Information System (SIKAD). This causes potential security risks such as leakage of data, information, and technical disturbances that affect business processes within Aisyah Pringsewu University (UAP). The risk assessment at SIKAD Aisyah Pringsewu University uses the Octave Allegro method and ISO 27002. In the Octave Allegro method there are 8 stages, the results of which are adjusted to the relevant ISO 27002 clause. The results of the calculation of the threat value of the Octave Allegro method found that the affected environment had the highest score for reliability and users, namely 38. Furthermore, the results of information security controls are applied in the ISO 27002 clause in each area of concern. Referring to the mitigation approach, the recommended Academic Information System (SIKAD) security policy consists of SIKAD Information Security Guidelines, SIKAD Work Instructions, SIKAD Security Procedures, SIKAD Security Forms. This research still has shortcomings, namely the limitations of data obtained from users of the Academic Information System (SIKAD), especially students. This study still has shortcomings, namely the limited data obtained from SIKAD users, especially students. SIKAD Security Procedure, SIKAD Security Form. This study still has shortcomings, namely the limitations of data obtained from users of the Academic Information System (SIKAD), especially students. This study still has shortcomings, namely the limited data obtained from SIKAD users, especially students. SIKAD Security Procedure, SIKAD Security Form.
	This is an open access article under the CC BY-SA license. 

Penulis Korespondensi:

Dwi Yana Ayu Andini,
Program Studi Rekayasa Perangkat Lunak,
Universitas Aisyah Pringsewu, Indonesia
Email: dwiandini983@aisyahuniversity.ac.id

1 PENDAHULUAN

Pemanfaatan Teknologi Informasi (TI) saat ini sudah menjadi bagian penting dan diperlukan hampir diseluruh kalangan bisnis dan berlaku juga untuk sebuah institusi perguruan tinggi. Sistem Informasi Akademik (SIKAD) dibuat untuk memudahkan penyebaran informasi akademik pada institusi tersebut. Seperti halnya sistem informasi lainnya, Sistem Informasi Akademik (SIKAD) perlu adanya penilaian resiko untuk menjamin keamanan informasi dan data yang terkandung dalam sistem tersebut.

Saat ini, masih banyak institusi pendidikan yang belum menerapkan penilaian resiko terhadap Sistem Informasi Akademik (SIKAD). Penyebab utamanya adalah kurangnya kesadaran institusi perguruan tinggi tentang resiko yang akan muncul apabila tidak dilakukannya penilaian resiko. Sebagai contoh resiko yang muncul adalah kebocoran data, informasi, dan adanya gangguan teknis yang mempengaruhi proses bisnis dalam institusi perguruan tinggi.

Pengamatan ini menghasilkan kesimpulan awal, bahwa institusi perguruan tinggi belum menerapkan penilaian resiko pada keamanan Sistem Informasi Akademik (SIKAD) secara optimal. Oleh sebab itu, diperlukan adanya penialain resiko keamanan dengan menggunakan metode OCTAVE Allegro dan ISO 27002. OCTAVE Allegro memiliki kemampuan untuk menampilkan hasil yang kuat dari penilaian resiko dengan dalam waktu yang relatif singkat dan sumber daya yang sedikit, bahkan dapat dilakukan oleh institusi perguruan tinggi yang tidak memiliki keahlian dalam penilaian resiko [1]. Dalam ISO 27002 untuk menerapkan kebijakan keamanan diperlukan standar keamanan informasi [2]. Hasil dari penelitian ini dapat menjadi acuan institusi perguruan tinggi dalam penilaian resiko keamanan Sistem Informasi Akademik (SIKAD).

2 METODE PENELITIAN (10 PT)

Penilaian resiko keamanan informasi Sistem Akademik (SIKAD) di Universitas Aisyah Pringsewu (UAP) dilakukan dengan metode Octave Allgero dan ISO 27002. Teknik pengumpulan data pada penelitian ini menggunakan data kualitatif. Data kualitatif yang dimaksud adalah data yang berasal dari hasil wawancara dan diskusi dengan Kepala ICT, Kepala Unit Akademik dan Kemahasiswaan Universitas Aisyah Pringsewu (UAP).

Langkah 1 – Menetapkan Kriteria Pengukuran Resiko

Pada langkah ini membangun organizational drivers yang digunakan untuk mengevaluasi dampak resiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting.

Langkah 2 – Mengembangkan Profil Aset Informasi

Mengumpulkan Informasi yang terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi, kedua dilakukan penilaian risiko terstruktur pada aset yang kritis. Tiga dan empat mengumpulkan informasi mengenai informasi aset yang penting, kelima membuat dokumentasi alasan pemilihan aset informasi tersebut. Keenam membuat deskripsi aset informasi kritis kemudian mengidentifikasi. Aktivitas tujuh mengisi kebutuhan keamanan untuk confidentiality, integrity dan availability. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Langkah 3 – Mengidentifikasi Wadah dari Aset Informasi

Dalam langkah tiga ini hanya ada satu aktivitas, perhatikan tiga poin penting yang terkait dengan keamanan dan konsep dari wadah aset informasi, yaitu cara aset informasi dilindungi, tingkat perlindungan atau pengamanan aset informasi dan kerentanan serta ancaman terhadap wadah dari aset informasi.

Langkah 4 – Mengidentifikasi Area Perhatian

Aktivitas pada langkah empat ini yaitu diawali dengan pengembangan profil resiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin dapat mengancam aset informasi. Dengan berpedoman pada dokumen Information Asset Risk Environment Maps dan Information Asset Risk Worksheet maka dapat dicatat area yang diperhatikan (area of concern). Berpedoman pada dokumen Information Asset Risk Worksheet lakukan review dari kontainer untuk membuat Area of Concern dan mendokumentasikannya.

Langkah 5 – Mengidentifikasi Skenario Ancaman

Aktivitas pada langkah lima ini yang pertama yaitu melakukan identifikasi skenario ancaman tambahan. pada aktivitas ini dapat menggunakan Appendix C – Threat Scenarios Questionnaires. Aktivitas kedua melengkapi Information Asset Risk.

Langkah 6 – Mengidentifikasi Resiko

Aktivitas pada langkah enam adalah menentukan threat scenario yang telah didokumentasikan di Information Asset Risk Worksheet yang dapat memberikan dampak bagi institusi.

Langkah 7 – Menganalisis Resiko

Aktivitas pada langkah ini harus dilakukan dengan mengacu pada dokumentasi yang terdapat pada Information Asset Risk Worksheet. Aktivitas pertama dimulai dengan melakukan review risk measurement criteria dilanjutkan dengan aktivitas kedua

yaitu menghitung nilai resiko relatif yang dapat digunakan untuk menganalisis resiko dan memutuskan strategi terbaik dalam menghadapi resiko yang muncul.

Langkah 8 – Memilih Pendekatan Mitigasi

Aktivitas pertama pada langkah delapan yaitu mengurutkan setiap resiko yang telah diidentifikasi berdasarkan nilai resikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi resiko tersebut. Aktivitas kedua adalah melakukan pendekatan mitigasi untuk setiap resiko dengan berpedoman pada kondisi yang unik di institusi tersebut [8].

3 HASIL DAN ANALISIS (10 PT)

3.1. Gambaran Umum Sistem Informasi Akademik di Universitas Aisyah Pringsewu (UAP)

Universitas Aisyah Pringsewu (UAP) mulai membangun Sistem Informasi Akademik (SIKAD) pada tahun 2014 [9]. Pengembangan SIKAD ini dimulai dari pengembangan perangkat lunak yang mencakup bidang akademik di Universitas Aisyah Pringsewu (UAP). Serta perangkat keras pendukung seperti, komputer server, komputer klien, dan jaringan komputer. Selanjutnya dilakukan pelatihan untuk para calon pengguna Sistem Informasi Akademik (SIKAD) yaitu dosen, mahasiswa, dan pengelola sistem.

Sebelum memulai penilaian resiko dan menetapkan kontrol keamanan, peneliti terlebih dahulu menghubungi orang-orang yang terkait dengan SIKAD Universitas Aisyah Pringsewu, yaitu Kepala ICT, dan Kepala Unit Akademik dan Kemahasiswaan [10].

3.2. Penilaian Resiko Menggunakan Metode Octave

Langkah 1

Menentukan criteria pengukuran resiko dengan cara mewawancarai narasumber.

Tabel 1. Keandalan dan pengguna

Rendah	Sedang	Tinggi
Penurunan ringan dalam keandalan	Kerusakan dan penurunan keandalan yang perlu perbaikan	Penurunan yang parah dalam keandalan yang tidak dapat diperbaiki
Penurunan ringan dalam kehilangan pengguna	Banyak kehilangan pengguna	Banyak kehilangan pengguna yang mengakibatkan hilangnya kepercayaan pengguna

Tabel 2. Skala prioritas lingkungan yang terimbas

Prioritas	Lingkungan yang Terimbas
5	Keandalan dan Pengguna
4	Keuangan
3	Produktifitas
2	Keamanan dan Kesehatan
1	Denda dan Pinalti

Langkah 2

Menentukan profile aset informasi terpenting. Dimulai dengan identifikasi aset, penilaian resiko pada aset, mengumpulkan informasi tentang aset, dan mengidentifikasi kebutuhan keamanan yang paling penting untuk melindungi aset. Dari pertimbangan diatas, aset informasi yang dikategorikan sebagai aset terpenting adalah database SIKAD.

Tabel 3. Profil aset informasi database

Alasan Pemilihan	Penjelasan
Seluruh data dan informasi berada pada database SIKAD.	Data SIKAD yang disimpan saling berhubungan dan saling berkaitan untuk menghasilkan informasi.
Pengelola	Kepala Unit Akademik dan Kemahasiswaan

Persyaratan Keamanan	Kerahasiaan	Kerahasiaan harus dijaga, karena itu perlu adanya pembatasan akses oleh pengguna yang memiliki hak akses khusus.
	Integritas	Integritas data terganggu akan menghambat sistem.
	Ketersediaan	Data harus selalu tersedia untuk pengguna.

Langkah 3

Mengidentifikasi wadah dari aset informasi melalui tiga poin penting dalam keamanan dan konsep aset informasi yaitu bagaimana cara aset dilindungi, tingkat perlindungan dan kerentanan wadah aset informasi dari setiap ancaman.

Tabel 4. Lingkungan resiko aset informasi database SIAKAD

Pemetaan Lingkungan Resiko Aset Informasi	
Internal	
Deskripsi Wadah	Pemilik
Server database cenderung untuk kebutuhan pengguna dimana dapat menyimpan banyak data dari para pengguna yang disimpan di tiap pengguna untuk mencegah pencurian data	UAP, Kepala ICT, dan Kepala Unit Akademik dan Kemahasiswaan.
Eksternal	
Kepala ICT, dan Kepala Unit Akademik dan Kemahasiswaan	UAP

Langkah 4

Mengidentifikasi area yang perlu diperhatikan. Dengan meninjau setiap wadah untuk menentukan area yang berpotensi menjadi perhatian.

Tabel 5. Database area

No	Area Perhatian
1	Pemberitahuan akses masuk oleh Kepala Unit Akademik dan Kemahasiswaan
2	Ancaman <i>Sniffing</i>
3	Database mengalami error saat maintenance sistem
4	Staff atau hacker yang terhubung kedalam jaringan computer melakukan kegiatan sniffing

Langkah 5

Mengidentifikasi skenario ancaman. Hal ini dilakukan untuk mengidentifikasi setiap ancaman yang mungkin terjadi.

Tabel 6. Properti ancaman – database SIAKAD

Area Perhatian	Properti Ancaman	
Pemberitahuan akses masuk oleh Kepala Unit Akademik dan Kemahasiswaan	Aktor	Ka. Unit Akademik & Kemahasiswaan
	Cara	Data login dapat bocor ke staff atau pihak yang tidak memiliki wewenang
	Motif	Pihak tidak berwenang dapat mengakses, mengubah, menambah, atau menghapus data dalam database sistem. Baik disengaja atau tidak
	Hasil	Penyingkapan, modifikasi, perusakan
	Persyaratan Keamanan	Kebijakan yang mengatur akses pribadi yang masuk kedalam sistem

Langkah 6

Mengidentifikasi Resiko dan menentukan skenario ancaman yang telah didokumentasikan yang dapat mempengaruhi institusi.

Tabel 7. Perhitungan nilai ancaman lingkungan yang terimbas

Lingkungan yang Terimbas	Prioritas	Rendah	Sedang	Tinggi
Keandalan dan Pengguna	5	5	10	20
Keuangan	4	4	8	12
Produktifitas	3	3	6	9
Keamanan dan Kesehatan	2	2	4	6
Denda dan Pinalti	1	1	2	3

Langkah 7

Menganalisis resiko berdasarkan perhitungan nilai ancaman.

Tabel 8. Perhitungan area

Lingkungan yang Terimbas	Nilai	Skor
Keandalan dan Pengguna	Tinggi	20
Keuangan	Sedang	8
Produktifitas	Rendah	3
Keamanan dan Kesehatan	Rendah	1
Denda dan Pinalti	Sedang	6

Langkah 8

Memilah semua resiko yang teridentifikasi berdasar nilai, untuk pengambilan keputusan menggunakan pendekatan mitigasi dengan mnegikuti kondisi dalam institusi.

Tabel 9. Matrik resiko

Skor Resiko		
Pool 1	Pool 2	Pool 3
36-50	19-35	0-18

Tabel 10. Matrik resiko relatif

Matrik Resiko Relatif			
Pool	1	2	3
Pendekatan Mitigasi	Mengurangi	Menunda	Menerima

3.3 Kontrol Keamanan ISO 27002

Setelah didapatkan hasil berdasarkan pendekatan mitigasi resiko selama fase Octave langkah selanjutnya adalah penyesuaian dengan klausul ISO 27002 yang terdiri dari.

Tabel 11. Matrik resiko relatif

Klausul	Sasaran
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan
11	Kontrol Akses
12	Akuisisi sistem informasi pengembangan dan pemeliharaan

3.4 Penerapan Kontrol Keamanan ISO 27002

ISO 27002 tidak mengharuskan organisasi untuk mengikuti bentuk control tertentu. Hal ini memungkinkan organisasi untuk menerapkan control yang sesuai kebutuhan dengan memperhatikan hasil penilaian resiko yang telah dilakukan.

Tabel 11. Matrik resiko relatif

Klausul 11 Kontrol Akses	
Kontrol	Sasaran
11.2.	Manajemen hak istimewa
11.3.	Manajemen kata sandi pengguna
11.4.	Peninjauan hak akses pengguna

3.5 Rekomendasi Kebijakan Keamanan SIAKAD

Penelitian ini menggunakan metode kualitatif, dimana hasil penelitian sesuai dengan metode Octave Allegro. Selanjutnya hasil control keamanan informasi diterapkan dalam klausul ISO 27002 pada setiap area perhatian. Mengacu pada pendekatan mitigasi, kebijakan keamanan Sistem Informasi Akademik (SIAKAD) yang direkomendasikan terdiri dari:

1. Panduan Keamanan Informasi SIAKAD,
2. Instruksi Kerja SIAKAD,
3. Prosedur Keamanan SIAKAD,
4. Formulir Keamanan SIAKAD.

4 KESIMPULAN

Penelitian ini menghasilkan kesimpulan sebagai berikut:

1. Metode Octave Allegro dapat diterapkan untuk menjamin ketersediaan informasi secara berkelanjutan di Universitas Aisyah Pringsewu (UAP) dalam mencapai visi dan misi.
2. Penilaian resiko dapat menggambarkan tentang ancaman terhadap aset yang penting dan mengambil tindakan pencegahan ancaman yang mungkin terjadi.
3. Klausul ISO 27002 yang berhubungan dengan penilaian resiko adalah keamanan sumber daya manusia, keamanan fisik dan lingkungan, control akses, dan Akuisisi sistem informasi pengembangan dan pemeliharaan.

UCAPAN TERIMA KASIH

Penelitian ini dapat dilaksanakan dengan baik berkat bantuan dari beberapa pihak, untuk itu peneliti mengucapkan terimakasih kepada Universitas Aisyah Pringsewu, Kepala ICT, Kepala Unit Akademik dan Kemahasiswaan yang telah memberikan kesempatan dan kerjasama yang baik dalam penelitian ini.

REFERENSI (10 PT)

Ahmad, S., 2019. Deteksi Penilaian Resiko Pada e-Learning SMK Bina Prestasi AMI Balikpapan Dengan Metode Octave Allegro. Jurnal Sistem Informasi 2 (2), 69-77.

Altry, D.P., Iketut, A.P., Iputu, A E., 2018. Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. Jurnal Ilmiah Merpati 6 (3), 148.

Arif, F.R., Awalludiyah, A., Eman, S., 2020. Analisis Manajemen Risiko Dan Keamanan Aset Menggunakan Metode Actave-S. Jurnal Of Information Technology and Computer Science 3 (2), 298-310.

Asriyanik, Prajoko., 2018. Manajemen Keamanan Informasi pada Sistem Informasi Akademik Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIK) Universitas Muhammadiyah Sukabumi (UMMI). Jurnal Teknik Informatika dan Sistem Infor-masi 4 (2), 315-325.

Aulia, Z., Endang, L.R., Pacu, P., 2020. Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya. Journal of Information System 6 (1). 40-47.

Deni, A.J., R, T.D., Hendrik., 2013. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. Fakultas Hukum UII, 37-42.

- Fadzri, A.A., Suprpto., Andi, R.P., 2019. Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001(Studi Kasus Bidang IT Kepolisian Daerah Banten). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 3(2), 1701–1707.
- Fernando, R.D., Nelmiawati., Maya, A.R., 2017. Mana-jemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OC-TAVE. Jurnal Integrasi 9 (1), 35.
- Ijacs, 1967. Angewandte Chemie International Edition, 6(11), 951–952.
- Joshua, J.L., Ayu, K.P., 2015. Analisis Manajemen Risiko Untuk Evaluasi Aset Menggunakan Metode Octave Allegro. Expert-Jurnal Manajemen Sistem Informasi Dan Teknologi 5 (1), 28-30.
- Kholifah., Reza, A.P., Fathiyah, N., 2021. Analisis Penilaian Risiko Terhadap Penggunaan Sistem Informasi Akademik Pada Universitas Muhammadiyah Palembang Menggunakan Metode Octave Allegro. Journal of Computer and Information Systems Ampera 2 (1), 28-42.
- Muhammad, T.J., Mokhamad, H., Toto, S., 2018. Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017, 1–6.
- Nurhafifah, M., Ika, N.I., Anita, M., 2017. Analisis Manajemen Risiko Keamanan Data Sistem Informasi. Jurnal Resti 1 (1), 19–25.
- Raihan, R.A., Rahadian, B., 2021. Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik. Journal of Emerging Information System and Business Intelligence 2 (2), 17-23.
- Raniyah, A.L., Dedy, S., 2020. Risk analysis of insan university system using iso27001. Jurnal Technology Acceptance Model 11 (2), 100-104.