Analisis Manajemen Risiko Keamanan Informasi pada Sistem Informasi Akademik Universitas XYZ Menggunakan Metode OCTAVE-S

Oleh :

Septya Kurnia Azzahra

227006516065

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

2025

BAB I
PENDAHULUAN

1.1 Latar Belakang

Digitalisasi telah menjadi pilar penting dalam operasional perguruan tinggi, khususnya dalam mendukung efisiensi layanan akademik. Salah satu sistem utama yang banyak diandalkan adalah Sistem Informasi Akademik (SIA**)**, yang digunakan untuk menangani proses seperti pendaftaran, pengelolaan nilai, KRS, dan data riwayat studi mahasiswa. Sistem ini memberikan kemudahan akses dan pengolahan informasi, namun juga membawa risiko yang cukup besar apabila tidak disertai dengan perlindungan data yang kuat.

Data yang tersimpan dalam SIA meliputi informasi penting dan sensitif, mulai dari identitas pribadi hingga rekam jejak akademik. Risiko keamanan dapat muncul jika sistem tidak memiliki kontrol akses yang baik, konfigurasi server terbuka, atau prosedur pengamanan yang lemah. Beberapa temuan menunjukkan bahwa masih banyak SIAKAD di lingkungan kampus yang memiliki celah seperti ini, sehingga membuka kemungkinan eksploitasi melalui teknik pemetaan sistem *footprinting* maupun pemindaian kerentanan *vulnerability scanning* (Hardiansyah et al., 2024).

Kondisi tersebut mencerminkan pentingnya implementasi sistem manajemen risiko yang tidak hanya menitikberatkan pada solusi teknis, tetapi juga melibatkan aspek organisasi, kesadaran pengguna, dan pengelolaan aset informasi secara menyeluruh. Salah satu pendekatan yang dianggap sesuai dengan kebutuhan institusi skala menengah seperti universitas adalah OCTAVE-S, sebuah kerangka kerja yang dirancang untuk mengidentifikasi aset kritikal, menilai kerentanan, dan merancang mitigasi risiko berdasarkan ancaman nyata yang dihadapi oleh organisasi.

Berdasarkan latar tersebut, judul **"Analisis Manajemen Risiko Keamanan Informasi pada Sistem Informasi Akademik Universitas XYZ Menggunakan Metode OCTAVE-S"** dipilih untuk menelaah sejauh mana sistem akademik digital mampu menghadapi tantangan keamanan informasi,

serta bagaimana metode OCTAVE-S dapat digunakan untuk menyusun strategi perlindungan yang sesuai dan berkelanjutan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan sebelumnya, maka identifikasi masalah dalam penelitian ini adalah sebagai berikut

1. Sistem informasi akademik masih memiliki kelemahan dalam aspek keamanan, khususnya pada pengendalian akses dan konfigurasi sistem yang rentan.
2. Belum diterapkannya manajemen risiko yang menyeluruh membuat institusi tidak siap dalam menghadapi potensi ancaman terhadap informasi digital.
3. Rendahnya tingkat kesadaran dari pengguna sistem terhadap praktik keamanan informasi menyebabkan meningkatnya potensi kelalaian dan kebocoran data.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengevaluasi keamanan informasi pada system informasi akademik Universitas XYZ dengan menggunakan pendekatan OCTAVE-S. Melalui penerapan metode ini, diharapkan dapat dilakukan identifikasi aset informasi yang kritikal, penilaian terhadap risiko dan kerentanannya, serta penyusunan strategi mitigasi yang sesuai dengan kondisi dan kebutuhan institusi.

1.4 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan ruang lingkup yang dibutuhkan, beberapa batasan ditetapkan sebagai berikut :

1. Penelitian hanya berfokus pada keamanan informasi yang terdapat dalam Sistem Informasi Akademik (SIA) di Universitas XYZ
2. Pembahasan meliputi identifikasi aset informasi yang dianggap penting, potensi ancaman dari sisi digital, dan celah sistem yang mungkin disalahgunakan oleh pihak tidak bertanggung jawab

3. Sistem lain seperti keuangan, kepegawaian, maupun layanan non-akademik tidak termasuk dalam lingkup pembahasan
4. Penelitian menggunakan metode OCTAVE-S yang lebih menekankan pada evaluasi risiko berdasarkan situasi dan kondisi internal kampus

1.5 Kontribusi Penelitian

Penelitian ini diharapkan bisa memberi manfaat langsung bagi perguruan tinggi, khususnya dalam memperkuat sistem keamanan informasi yang digunakan dalam kegiatan akademik. Hasil dari penelitian ini dapat dijadikan sebagai bahan pertimbangan untuk menyusun kebijakan atau langkah-langkah pengamanan data yang lebih terarah dan sesuai kebutuhan kampus.

Selain itu, dari sisi akademik, penelitian ini juga menambah referensi tentang penerapan metode OCTAVE-S di bidang pendidikan, yang selama ini lebih sering digunakan di sektor industri atau bisnis. Temuan dan pendekatan dalam penelitian ini bisa dijadikan acuan oleh institusi lain yang memiliki kebutuhan serupa dalam mengelola risiko keamanan informasi.

BAB II
TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Sistem Informasi Akademik

Sistem Informasi Akademik (SIA) merupakan sistem terkomputerisasi yang dirancang untuk memfasilitasi pengelolaan proses akademik di perguruan tinggi, seperti registrasi mahasiswa, pengisian KRS, penyimpanan nilai, serta pelaporan akademik. SIA mendukung efektivitas penyelenggaraan pendidikan dengan menyediakan data dan informasi yang akurat dan real-time. Namun, sistem ini juga menyimpan data sensitif seperti informasi pribadi mahasiswa dan dosen, sehingga menimbulkan tantangan dalam aspek keamanan informasi. Oleh karena itu, penting bagi perguruan tinggi untuk menerapkan sistem pengamanan yang memadai pada SIA (Nur Fadhila et al., 2025).

2.1.2 Keamanan Informasi

Keamanan informasi adalah seperangkat kebijakan dan kontrol teknis yang dirancang untuk melindungi informasi dari berbagai ancaman yang dapat mengakibatkan gangguan terhadap kelangsungan organisasi. Tiga komponen utama yang menjadi prinsip dasar keamanan informasi adalah *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), dan *Availability* (ketersediaan), yang dikenal dengan istilah CIA Triad. Dalam lingkungan pendidikan, penerapan prinsip-prinsip ini harus dilaksanakan dengan cermat karena kegagalan menjaga satu saja dari ketiganya dapat menyebabkan kerugian yang signifikan, baik dari sisi hukum, kepercayaan publik, maupun reputasi institusi (Rachmadhani et al., 2024).

2.1.3 Manajemen Risiko Informasi

Manajemen risiko informasi merupakan proses yang dilakukan secara sistematis untuk mengenali, menilai, dan mengendalikan risiko yang berpotensi mengganggu keamanan informasi dalam organisasi. Proses ini mencakup identifikasi aset informasi kritis, analisis ancaman, pengukuran

dampak, serta pemilihan kontrol mitigasi yang sesuai. Tujuannya adalah untuk meminimalkan kemungkinan kerugian akibat ancaman terhadap sistem informasi. Dalam konteks sistem informasi akademik, pendekatan ini menjadi semakin penting karena perguruan tinggi mengelola data besar yang bersifat rahasia dan operasional (Pakarbudi et al., 2023).

2.2 Landasan Teori

2.2.1 Teori Sistem Sosio-Teknis

Teori sistem sosio-teknis (*socio-technical systems theory*) menekankan bahwa setiap sistem informasi terdiri dari dua subsistem utama: aspek teknis (teknologi, infrastruktur) dan aspek sosial (pengguna, kebijakan, budaya organisasi). Keamanan sistem informasi tidak dapat ditangani hanya dari sisi teknis saja, melainkan juga membutuhkan pemahaman terhadap interaksi sosial yang terjadi di dalam organisasi. Dalam konteks ini, risiko tidak hanya muncul dari serangan eksternal, tetapi juga dari kelalaian atau kesalahan pengguna internal. Oleh karena itu, integrasi antara pendekatan teknis dan kebijakan organisasi menjadi sangat penting untuk mencapai perlindungan informasi yang (Fachrunisa Lubis et al., 2024).

2.2.2 Teori Pengelolaan Keamanan Informasi

Teori pengelolaan keamanan informasi berangkat dari pemahaman bahwa sistem informasi harus dikelola sebagai bagian dari aset strategis organisasi. Organisasi perlu menerapkan kebijakan, standar operasional, audit, serta peningkatan kapasitas sumber daya manusia untuk mendukung keamanan informasi secara berkelanjutan. Salah satu kerangka kerja yang dapat digunakan untuk mendukung pengelolaan ini adalah ISO 27001, serta metode penilaian risiko seperti OCTAVE-S atau OCTAVE Allegro. Teori ini memperkuat argumen bahwa manajemen risiko informasi harus menjadi bagian dari strategi organisasi, bukan hanya tanggung jawab unit teknologi informasi (Febriyono & Heaven Happyna Putra, 2023).

2.3 Penelitian Terdahulu

No	Peneliti	Tahun	Judul	Metode	Temuan
1	Zahra Nur Fadhila , Ilham	2025	PENERAPAN OCTAVE ALLEGRO DALAM MANAJEMEN RISIKO SISTEM INFORMASI PADA UNIVERSITAS ISLAM XYZ	OCTAVE ALLEGRO	Terdapat 7 risiko utama, termasuk kebocoran data dan pemalsuan. Strategi mitigasi disusun aset-basis.
2	Mirga Maulana Rachmadhani, Aprisa Rian Histiarini, Siti Nur Kayatun, Mohammad Arief Nur Wahyudien, Asih Ahistasari	2024	Analisis Manajemen Risiko Aset pada Biro Administrasi Akademikdan Kemahasiswaan Universitas Muhammadiyah Sorong	ISO 31010:2019	Teridentifikasi 17 risiko. Penekanan pada proses penilaian risiko untuk melindungi aset BAAK.
3	Adib Pakarbudi , Dea Tiara Piay , Dita Nurmadewi , Andy Rachman	2023	Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi	Octave Allegro dan Fmea	OCTAVE dinilai lebih partisipatif dan cocok untuk sektor pendidikan.

4	Ayuni Fachrunisa Lubis, Diana Nadha, Megawati	2024	ANALISA MANAJEMEN RISIKO IT DENGAN MENGGUNAKAN METODE OCTAVE-S UNTUK MENINGKATKAN KEAMANAN SISTEM DI PTIPD UNIVERSITAS XYZ	OCTAVE-S	Ancaman internal mendominasi. Disarankan peningkatan kontrol administratif dan kesadaran pengguna.
5	Febriyono, Heaven Happyna Putra	2023	Evaluasi Sistem Manajemen Keamanan Informasi menggunakan Metode OCTAVE-S berdasarkan Standar Kontrol ISO 27001 (Studi Kasus: UPT TIK Institut Teknologi Kalimantan)	*OCTAVE-S berdasarkan Standar Kontrol ISO 27001*	Evaluasi menunjukkan lemahnya dokumentasi dan kontrol. ISO memperkuat mitigasi teknis dan kebijakan.

2.4 Kajian Pustaka

Dalam era digitalisasi layanan pendidikan tinggi, sistem informasi akademik (SIA) menjadi elemen sentral dalam pengelolaan data mahasiswa, proses perkuliahan, hingga administrasi akademik. Kerentanan terhadap gangguan sistem, kesalahan input data, hingga potensi kebocoran informasi pribadi mahasiswa menuntut dilakukannya manajemen risiko yang efektif. Fadhilah dan Ilham (2025) menyatakan bahwa sistem informasi akademik sangat rentan terhadap ancaman yang bersifat teknis maupun non-teknis, sehingga diperlukan pendekatan manajemen risiko yang tidak hanya berbasis teknologi, tetapi juga melibatkan peran organisasi.

Salah satu pendekatan yang banyak digunakan adalah metode OCTAVE-S. Metode ini menekankan pada pentingnya identifikasi dan

evaluasi risiko berdasarkan aset informasi yang dimiliki organisasi. Dibandingkan dengan metode teknis seperti FMEA, OCTAVE lebih bersifat partisipatif dan menyesuaikan dengan konteks organisasi, sehingga cocok diterapkan di sektor pendidikan yang umumnya memiliki keterbatasan SDM di bidang keamanan informasi (Pakarbudi et al., 2023). Penelitian oleh Lubis dan Nadha (2024) menunjukkan bahwa risiko terbesar di sistem informasi institusi pendidikan justru berasal dari dalam organisasi, seperti penggunaan akun bersama dan lemahnya kebijakan penggunaan perangkat pribadi. Temuan tersebut mempertegas bahwa keamanan informasi tidak hanya dipengaruhi oleh teknologi, tetapi juga perilaku dan kebijakan internal.

Integrasi antara metode OCTAVE dan standar keamanan seperti ISO 27001 juga menjadi praktik yang banyak dianalisis. Ciptaningtyas dan Ghozali (2024) menilai bahwa penggunaan standar internasional membantu memetakan risiko secara lebih sistematis dan memberikan arahan pengendalian yang terukur. Dalam studi mereka, kelemahan ditemukan pada dokumentasi kebijakan keamanan, kontrol teknis yang tidak seragam, serta minimnya pelatihan pengguna sistem. Dengan penguatan kerangka ISO, hasil analisis OCTAVE-S menjadi lebih konkret dan dapat diimplementasikan dengan pendekatan kontrol standar.

Selain pendekatan berbasis ISO 27001, ISO 31010:2019 juga dapat digunakan untuk menilai risiko di unit akademik non-teknis seperti Biro Administrasi Akademik dan Kemahasiswaan (BAAK). Rachmadhani dan Histiarini (2024) dalam penelitiannya berhasil mengidentifikasi 17 risiko yang mungkin terjadi dalam proses layanan BAAK. Penelitian ini menunjukkan bahwa manajemen risiko tidak terbatas pada sistem informasi utama, tetapi juga perlu diterapkan pada unit-unit administratif yang menyimpan dan memproses data sensitif mahasiswa.

Berbagai studi tersebut menggarisbawahi pentingnya pemilihan metode manajemen risiko yang relevan dengan karakteristik institusi pendidikan. OCTAVE-S terbukti efektif karena mampu mengakomodasi

sudut pandang organisasi dan memprioritaskan aset-aset penting dalam proses penilaian risiko. Ditambah dengan standar ISO, baik 27001 maupun 31010, hasil penilaian risiko dapat dihubungkan dengan praktik pengelolaan keamanan informasi yang terstandarisasi.

DAFTAR PUSTAKA

Fachrunisa Lubis, A., Nadha, D., & Sains dan Teknologi, F. (2024). ANALISA MANAJEMEN RISIKO IT DENGAN MENGGUNAKAN METODE OCTAVE-S UNTUK MENINGKATKAN KEAMANAN SISTEM DI PTIPD UNIVERSITAS XYZ. *Journal Informatics NIVEDITA* |, *01*(1).

Febriyono, & Heaven Happyna Putra. (2023). *Evaluasi Sistem Manajemen Keamanan Informasi menggunakan Metode OCTAVE-S berdasarkan Standar Kontrol ISO 27001 (Studi Kasus: UPT TIK Institut Teknologi Kalimantan)*.

Hardiansyah, A., Eka Septiana, idah, & Rahmalia Eka Putri, M. (2024). *ANALISIS KEAMANAN WEBSITE SIAKAD UNTIRTA MENGGUNAKAN TEKNIK FOOT PRINTING DAN VULNERABILITY SCANNING* (Vol. 4, Issue 1).

Nur Fadhila, Z., Sistem Informasi, I., Sains dan Teknologi, F., Islam Negeri Sunan Ampel Jl Ahmad Yani No, U., Wonosari, J., & Wonocolo, K. (2025). PENERAPAN OCTAVE ALLEGRO DALAM MANAJEMEN RISIKO SISTEM INFORMASI PADA UNIVERSITAS ISLAM XYZ. In *Jurnal Mahasiswa Teknik Informatika)* (Vol. 9, Issue 2).

Pakarbudi, A., Piay, D. T., Nurmadewi, D., & Rachman, A. (2023). Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi. *JURIKOM (Jurnal Riset Komputer)*, *10*(2), 488. https://doi.org/10.30865/jurikom.v10i2.5950

Rachmadhani, M. M., Histiarini, A. R., Kayatun, S. N., Wahyudien, M. A. N., & Ahistasari, A. (2024). Analisis Manajemen Risiko Aset pada Biro Administrasi Akademik dan Kemahasiswaan Universitas Muhammadiyah Sorong. *JISI: Jurnal Integrasi Sistem Industri*, *11*(2), 171–182. https://doi.org/10.24853/jisi.11.2.171-182