ANALISIS MANAJEMEN KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN STANDAR ISO/IEC 27001 (STUDI KASUS : UNIVERSITAS CENDEKIA NUSANTARA (UCN)

"Sebagai salah satu syarat untuk memenuhi tugas UTS dan UAS mata kuliah Keamanan Komputer"

Oleh :

Kayla Nurhikmah

221011403051

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mendorong perguruan tinggi untuk memanfaatkan sistem informasi akademik (SIAKAD) sebagai sarana pengelolaan data mahasiswa, dosen, dan proses administrasi akademik. Dengan meningkatnya ketergantungan pada sistem digital, muncul pula berbagai ancaman terhadap keamanan informasi seperti kebocoran data, serangan siber, dan kesalahan akses pengguna.

Keamanan sistem informasi menjadi hal yang krusial agar data akademik tetap rahasia (confidentiality), terjaga keutuhannya (integrity), dan tersedia kapan pun diperlukan (availability).

Standar ISO/IEC 27001:2013 merupakan pedoman internasional yang digunakan untuk membangun Sistem Manajemen Keamanan Informasi (SMKI) melalui pendekatan berbasis risiko. Standar ini mencakup kebijakan, prosedur, dan kontrol keamanan yang dirancang untuk menjaga seluruh aset informasi organisasi.

Laporan ini menganalisis penerapan ISO/IEC 27001 pada Universitas Cendekia Nusantara (UCN) sebagai simulasi implementasi SMKI pada lingkungan akademik. Penelitian mengacu pada konsep dan metode yang digunakan oleh Tuga (2019) yang menilai tingkat kematangan keamanan sistem informasi berdasarkan kontrol ISO 27001 pada sektor pendidikan.

1.2 Identifikasi Masalah

Seiring meningkatnya penggunaan sistem digital di lingkungan pendidikan, Universitas Cendekia Nusantara (UCN) menghadapi tantangan dalam menjaga keamanan data akademik yang tersimpan pada Sistem Informasi Akademik (SIAKAD). Sistem ini mengelola berbagai informasi penting seperti data pribadi mahasiswa, nilai, jadwal kuliah, serta laporan keuangan kampus.

Namun, masih terdapat sejumlah permasalahan yang diidentifikasi dalam pengelolaan keamanan informasi, antara lain:

1. Belum adanya penerapan standar keamanan informasi yang baku seperti ISO/IEC 27001 dalam sistem akademik kampus.
2. Pengelolaan aset informasi belum sepenuhnya terdokumentasi dan diklasifikasikan sesuai tingkat kerahasiaan.
3. Akses terhadap data akademik masih terbuka bagi beberapa pihak tanpa sistem kontrol berbasis peran (role-based access control).
4. Kesadaran staf terhadap ancaman keamanan informasi seperti phishing, malware, atau kebocoran data masih rendah.
5. Tidak adanya mekanisme evaluasi berkala terhadap efektivitas kebijakan keamanan informasi dan sistem backup data.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan prinsip dan struktur ISO/IEC 27001:2013 dalam sistem informasi akademik di Universitas Cendekia Nusantara?
2. Risiko keamanan informasi apa saja yang terdapat pada pengelolaan data akademik di SIAKAD UCN?
3. Bagaimana tingkat kematangan kontrol keamanan informasi di lingkungan universitas berdasarkan standar ISO/IEC 27001?
4. Langkah mitigasi apa yang perlu diterapkan untuk meningkatkan keamanan informasi sesuai dengan kontrol ISO/IEC 27001?

1.4 Tujuan Penelitian

Tujuan dari penelitian dan analisis ini adalah untuk:

1. Menganalisis tingkat penerapan manajemen keamanan informasi di Universitas Cendekia Nusantara berdasarkan standar ISO/IEC 27001:2013.
2. Mengidentifikasi aset informasi utama, potensi ancaman, dan kerentanan yang terdapat dalam sistem akademik kampus.
3. Menilai tingkat kematangan keamanan informasi melalui area kontrol utama ISO/IEC 27001.
4. Menyusun rekomendasi langkah mitigasi dan kebijakan keamanan yang dapat diterapkan oleh universitas untuk meningkatkan perlindungan data akademik.

BAB II

ORGANISASI

2.1 Profil Organisasi

Universitas Cendekia Nusantara (UCN) merupakan perguruan tinggi swasta fiktif yang bergerak di bidang pendidikan teknologi dan sains terapan. UCN berdiri sejak tahun 2010 di bawah naungan Yayasan Cendekia Bangsa, dan berkomitmen untuk menjadi universitas unggul dalam bidang teknologi informasi, bisnis digital, dan manajemen modern.

Sebagai lembaga pendidikan tinggi, UCN memiliki visi “Menjadi universitas inovatif dan berdaya saing global melalui penerapan teknologi informasi dalam pendidikan dan penelitian.” Misi UCN meliputi penyelenggaraan pendidikan berkualitas, penelitian terapan di bidang teknologi digital, serta pengabdian kepada masyarakat berbasis inovasi teknologi.

alam operasionalnya, UCN memiliki 5 fakultas utama, yaitu:

1. Fakultas Teknologi Informasi dan Komputer
2. Fakultas Ekonomi dan Bisnis
3. Fakultas Teknik Industri
4. Fakultas Ilmu Pendidikan
5. Fakultas Hukum dan Komunikasi

Jumlah mahasiswa aktif saat ini mencapai sekitar 7.500 orang, dengan tenaga pengajar dan staf sebanyak 350 orang. Untuk mendukung kegiatan akademik dan administrasi, UCN menerapkan sistem berbasis digital yang terintegrasi, salah satunya melalui Sistem Informasi Akademik (SIAKAD UCN). Sistem ini digunakan untuk proses pendaftaran mahasiswa baru, pengisian Kartu Rencana Studi (KRS), penilaian dosen, pengelolaan keuangan, serta distribusi informasi akademik secara daring.

1. Struktur organisasi UCN terdiri dari Rektor, tiga Wakil Rektor, serta beberapa unit pendukung seperti:
2. Pusat Teknologi Informasi dan Data (PTID) yang bertanggung jawab terhadap infrastruktur jaringan, server, dan keamanan data digital.
3. Biro Administrasi Akademik (BAA) yang mengelola kegiatan akademik dan data mahasiswa.

4. Biro Keuangan dan SDM, yang mengelola keuangan kampus dan sistem kepegawaian.

Sebagai institusi pendidikan modern, UCN menyadari pentingnya keamanan informasi akademik sebagai bagian dari keberlangsungan layanan dan kepercayaan publik. Data mahasiswa, dosen, dan staf merupakan aset penting yang harus dijaga dari ancaman penyalahgunaan dan kebocoran. Oleh karena itu, UCN berupaya menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional ISO/IEC 27001:2013.

Ruang lingkup penerapan SMKI di Universitas Cendekia Nusantara berfokus pada Pusat Teknologi Informasi dan Data (PTID) yang mengelola server, sistem jaringan kampus, database akademik, serta aplikasi SIAKAD. Dengan adanya sistem manajemen keamanan informasi yang terstruktur, diharapkan UCN dapat menjaga kerahasiaan, integritas, dan ketersediaan data akademik, serta memenuhi persyaratan kepatuhan terhadap regulasi perlindungan data di Indonesia.

2.2 Struktur Organisasi

Struktur organisasi Universitas Cendekia Nusantara (UCN) dirancang untuk mendukung tata kelola perguruan tinggi yang efektif, transparan, dan akuntabel, terutama dalam pengelolaan sistem informasi akademik. Struktur ini dibangun secara hirarkis dan fungsional, di mana setiap unit memiliki tanggung jawab serta wewenang sesuai bidang kerjanya.

Secara umum, struktur organisasi UCN terdiri dari unsur pimpinan, unsur pelaksana akademik, serta unit pendukung operasional dan teknologi informasi. Berikut penjelasan tiap bagian:

1. Rektor

   Rektor merupakan pimpinan tertinggi universitas yang bertanggung jawab atas keseluruhan kegiatan akademik dan non-akademik. Rektor memiliki kewenangan dalam menentukan arah kebijakan universitas, termasuk dalam hal keamanan informasi dan tata kelola teknologi digital.
2. Wakil Rektor I (Bidang Akademik dan Kemahasiswaan)

Bertugas mengawasi seluruh kegiatan akademik, kurikulum, dan layanan mahasiswa. Wakil Rektor I bekerja sama dengan Pusat Teknologi Informasi dan Data (PTID) dalam menjamin keandalan Sistem Informasi Akademik (SIAKAD).

3. Wakil Rektor II (Bidang Administrasi, Keuangan, dan SDM)
   Memiliki tanggung jawab terhadap keuangan universitas, administrasi pegawai, serta kebijakan pengelolaan aset, termasuk keamanan data keuangan yang terintegrasi dengan sistem akademik digital.
4. Wakil Rektor III (Bidang Riset, Inovasi, dan Kerja Sama)
   Mengelola kegiatan penelitian, pengabdian masyarakat, dan hubungan kerja sama dengan lembaga lain. Unit ini turut menggunakan data akademik dan publikasi dosen yang disimpan dalam sistem informasi universitas, sehingga juga menjadi pengguna penting dari sistem keamanan informasi.
5. Pusat Teknologi Informasi dan Data (PTID)
   Merupakan unit utama yang menangani infrastruktur TI, jaringan kampus, keamanan data, dan pengembangan sistem informasi. PTID bertanggung jawab langsung kepada Rektor melalui koordinasi dengan Wakil Rektor I.
   Fungsi utama PTID antara lain:
   - Menjamin ketersediaan dan keandalan sistem SIAKAD.
   - Melakukan pengelolaan akun pengguna (dosen, mahasiswa, staf).
   - Melaksanakan kebijakan keamanan informasi sesuai standar ISO/IEC 27001.
   - Menjalankan backup dan pemeliharaan server secara berkala.
6. Biro Administrasi Akademik (BAA)
   Bertugas dalam pengelolaan seluruh data akademik mahasiswa, mulai dari pendaftaran, Kartu Rencana Studi (KRS), nilai, hingga kelulusan. Unit ini menjadi pengguna utama SIAKAD dan bekerja sama erat dengan PTID untuk menjaga keamanan dan integritas data akademik.
7. Biro Keuangan dan Sumber Daya Manusia (BKSDM)
   Menangani transaksi keuangan mahasiswa dan dosen, serta data gaji, beasiswa, dan anggaran universitas. Keamanan informasi pada biro ini juga menjadi bagian dari sistem keamanan terintegrasi karena terkait dengan data sensitif.
8. Fakultas dan Program Studi

Setiap fakultas dan program studi bertanggung jawab dalam pelaksanaan kegiatan akademik di tingkat jurusan. Dosen dan tenaga kependidikan menggunakan sistem SIAKAD untuk input nilai, bimbingan, dan pemantauan mahasiswa.

9. Unit Penjaminan Mutu dan Audit Internal (UPMAI)

   Berfungsi mengawasi pelaksanaan kebijakan universitas, termasuk kepatuhan terhadap standar keamanan informasi dan manajemen risiko. Unit ini juga bertugas melakukan audit internal terhadap pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI).

2.3 Aset Informasi Penting

Sebagai institusi pendidikan tinggi yang menerapkan sistem akademik berbasis teknologi informasi, **Universitas Cendekia Nusantara (UCN)** memiliki berbagai aset informasi yang berperan penting dalam mendukung kegiatan operasional dan pelayanan akademik. Aset-aset ini tidak hanya berupa perangkat keras (hardware) dan perangkat lunak (software), tetapi juga meliputi data, sumber daya manusia, serta kebijakan internal yang berkaitan dengan pengelolaan informasi.

1. Data pribadi mahasiswa dan dosen.
2. Data nilai dan keuangan mahasiswa.
3. Server database akademik.
4. Jaringan kampus dan sistem autentikasi pengguna.
5. Dokumen digital akademik dan arsip nilai.

BAB III

ANALISA DAN PERANCANGAN

3.1 Analisis Konteks Organisasi

3.1.1 Isu Internal dan Eksternal yang Mempengaruhi Keamanan Informasi

Jenis Isu	Deskripsi Isu
Internal	SIAKAD digunakan oleh seluruh mahasiswa dan dosen, meningkatkan risiko akses tidak sah. Belum semua staf memahami pentingnya kebijakan keamanan data. nfrastruktur TI masih bergantung pada server lokal tanpa sistem cadangan lokasi kedua.
Eksternal	Ancaman siber seperti *phishing*, *ransomware*, dan kebocoran data mahasiswa meningkat. Regulasi pemerintah tentang Perlindungan Data Pribadi (UU PDP) mulai diberlakukan. Reputasi kampus bergantung pada kepercayaan publik terhadap keamanan data akademik.

3.2.1 Pihak-Pihak Berkepentingan dan Kebutuhan Keamanan Informasi

Stakeholder	Kebutuhan terhadap Keamanan Informasi
Mahasiswa	Keamanan data pribadi dan akses aman ke sistem nilai.
Dosen & Staf Akademik	Sistem yang stabil, terlindungi dari gangguan, dan memiliki kontrol akses jelas.
Manajemen Universitas (Rektorat)	Kepatuhan terhadap regulasi pemerintah dan perlindungan reputasi kampus.

Divisi PTID (TI Kampus)	Infrastruktur yang aman, log aktivitas pengguna, serta sistem backup otomatis.
Pemerintah & Regulator (Kemendikbud, LLDIKTI)	Kepatuhan terhadap kebijakan perlindungan data pendidikan tinggi.

3.2 Penilaian Risiko Keamanan Informasi

NO	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
1	Data mahasiswa (biodata, nilai, keuangan)	Kebocoran data atau pencurian informasi pribadi	Akses data belum dibatasi berdasarkan peran pengguna	5	4	**20 (Tinggi)**	Terapkan enkripsi database dan kontrol akses berbasis peran (RBAC).
2	Server database akademik	Serangan malware atau ransomware	Tidak adanya sistem deteksi intrusi (IDS/IPS) aktif	5	3	**15 (Tinggi)**	Instalasi IDS/IPS, backup harian terenkripsi, dan antivirus server.
3	Sistem login SIAKAD	Penyalahgunaan akun pengguna (dosen/mahasiswa)	Tidak ada kebijakan rotasi password dan audit login	4	4	**16 (Tinggi)**	Terapkan autentikasi dua faktor (2FA) dan kebijakan rotasi password.
4	Dokumen akademik (KHS, transkrip, laporan)	Akses tanpa izin atau perubahan data	Penyimpanan file tidak terenkripsi dan tanpa log aktivitas	3	3	**9 (Sedang)**	Gunakan enkripsi file server dan sistem audit log pengguna.

NO	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
5	Infrastruktur jaringan kampus	Serangan DDoS dan penyusupan jaringan	Firewall dan konfigurasi router belum optimal	5	2	**10 (Sedang)**	Konfigurasi ulang firewall, aktifkan sistem anti-DDoS, dan segmentasi jaringan.
6	Email staf dan dosen	Phishing dan serangan social engineering	Kurangnya pelatihan kesadaran keamanan informasi	4	4	**16 (Tinggi)**	Lakukan pelatihan keamanan siber rutin dan gunakan filter anti-phishing.
7	Data keuangan mahasiswa	Manipulasi data pembayaran atau tagihan	Tidak ada sistem audit transaksi otomatis	4	3	**12 (Sedang)**	Implementasikan audit trail dan sistem validasi transaksi digital.
8	Backup server lokal	Kehilangan data akibat kerusakan perangkat	Tidak ada backup di lokasi berbeda (off-site)	4	2	**8 (Sedang)**	Terapkan sistem backup otomatis ke server cadangan di lokasi berbeda.
9	Akun administrator sistem	Penyalahgunaan hak akses istimewa	Tidak ada audit akses berkala	5	3	**15 (Tinggi)**	Audit hak akses secara periodik dan terapkan prinsip least privilege.

NO	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
10	Aplikasi mobile SIAKAD	Penyadapan data saat login	Komunikasi aplikasi belum menggunakan SSL/TLS	4	3	**12 (Sedang)**	Terapkan SSL/TLS dan enkripsi komunikasi end-to-end.

3.3 Pemilihan dan Perancangan Kontrol Keamanan

Berdasarkan hasil analisis risiko pada Sistem Informasi Akademik Universitas Cendekia Nusantara (UCN), dipilih sejumlah kontrol keamanan dari Annex A ISO/IEC 27001 yang relevan untuk melindungi aset informasi akademik seperti data mahasiswa, dosen, nilai, dan jadwal perkuliahan.

No	Kode Kontrol	Nama Kontrol	Alasan Pemilihan	Rancangan Penerapan di UCN
1	A.5.1	Kebijakan Keamanan Informasi	Sebagai dasar pengelolaan keamanan informasi akademik	Menyusun kebijakan keamanan informasi yang berlaku untuk seluruh civitas akademika
2	A.5.15	Kontrol Akses	Mencegah akses tidak sah ke sistem akademik	Penerapan hak akses berbasis peran (admin, dosen, mahasiswa)
3	A.6.3	Kesadaran dan Pelatihan Keamanan	Faktor manusia berpotensi menimbulkan insiden keamanan	Pelatihan keamanan informasi bagi dosen, staf, dan mahasiswa
4	A.6.7	Proses Disiplin Keamanan	Menangani pelanggaran keamanan informasi	Pemberlakuan sanksi sesuai peraturan akademik dan institusi
5	A.7.4	Keamanan Fisik dan Lingkungan	Melindungi server dan perangkat jaringan	Pembatasan akses ruang server dan pemasangan CCTV
6	A.8.1	Perangkat Pengguna	Penggunaan laptop pribadi berisiko terhadap kebocoran data	Kebijakan penggunaan perangkat dan antivirus wajib
7	A.8.9	Manajemen Konfigurasi	Kesalahan konfigurasi dapat menimbulkan celah keamanan	Penerapan prosedur perubahan konfigurasi sistem
8	A.8.12	Pencegahan	Data akademik bersifat	Enkripsi data dan pembatasan

No	Kode Kontrol	Nama Kontrol	Alasan Pemilihan	Rancangan Penerapan di UCN
		Kebocoran Data	rahasia	media penyimpanan eksternal
9	A.8.15	Logging dan Monitoring	Mendeteksi aktivitas mencurigakan	Pencatatan log aktivitas pengguna sistem
10	A.8.16	Manajemen Insiden Keamanan	Menjamin respons cepat saat terjadi insiden	Penyusunan prosedur penanganan insiden keamanan

3.4 Kebijakan Keamanan Informasi

Universitas Cendekia Nusantara (UCN) berkomitmen untuk melindungi seluruh informasi akademik dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Kebijakan ini menjadi pedoman dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) sesuai ISO/IEC 27001.

3.4.1 Tujuan Keamanan

Tujuan keamanan informasi UCN adalah:

1. Melindungi data akademik dari akses tidak sah
2. Menjamin keakuratan dan keutuhan data akademik
3. Menjamin ketersediaan sistem akademik selama jam operasional
4. Mengurangi risiko kebocoran data
5. Meningkatkan kesadaran keamanan informasi pengguna
6. Menyediakan mekanisme penanganan insiden keamanan
7. Mendukung kepatuhan terhadap standar ISO/IEC 27001

3.5 Rencana Implementasi SMKI

No	Tahapan	Kegiatan
1	Penentuan Ruang Lingkup	Menentukan cakupan SMKI pada sistem akademik
2	Identifikasi Aset	Data akademik, server, jaringan
3	Analisis Risiko	Identifikasi ancaman dan dampak
4	Pemilihan Kontrol	Menyesuaikan Annex A ISO 27001
5	Penyusunan Dokumen	Kebijakan dan prosedur SMKI
6	Implementasi	Penerapan kontrol keamanan

No	Tahapan	Kegiatan
7	Pelatihan	Sosialisasi kepada pengguna
8	Monitoring	Evaluasi dan audit internal
9	Perbaikan	Peningkatan berkelanjutan

BAB IV

PENUTUP

4.1 Kesimpulan

- Sistem Informasi Akademik UCN memiliki peran penting dalam mendukung kegiatan akademik.
- Analisis menunjukkan masih terdapat risiko keamanan informasi yang perlu dikelola secara sistematis.
- Beberapa kontrol keamanan telah diterapkan, namun belum terintegrasi dalam SMKI yang terdokumentasi.
- Rancangan SMKI berdasarkan ISO/IEC 27001 dapat menjadi solusi untuk meningkatkan keamanan informasi akademik.
- UCN berada pada tahap awal dalam penerapan manajemen keamanan informasi berbasis standar internasional.

4.2 Rekomendasi

- Membentuk tim atau penanggung jawab keamanan informasi
- Menyusun dan menerapkan dokumen SMKI secara formal
- Melakukan analisis risiko secara berkala
- Mengadakan pelatihan keamanan informasi rutin
- Melakukan audit internal keamanan informasi
- Menerapkan siklus **Plan–Do–Check–Act (PDCA)**
- Mempersiapkan institusi menuju sertifikasi ISO/IEC 27001

DAFTAR PUSTAKA

A. Z. Maingak, C. Candiwan, dan L. D. Harsono, “Information Security Assessment Using ISO/IEC 27001:2013 Standard on Government Institution,” *TRIKONOMIKA*, vol. 17, no. 1, pp. 28–37, 2018, doi: 10.23969/trikonomika.v17i1.1138.

M. N. H. Siregar dan M. Mardiah, “Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001,” *J. Ilmu Komputer dan Teknik Informatika*, vol. 1, no. 2, pp. 58–64, Jul. 2025, doi: 10.64803/juikti.v1i2.52.

F. Fitroh, M. R. Seputra, G. Ramadhan, T. N. H. Hersyaf, dan A. N. Rokhman, “Pentingnya Implementasi ISO 27001 dalam Manajemen Keamanan: Sistematika Review,” *Prosiding Semnastek*, 2024.

J. Jevelin dan A. Faza, “Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification,” *J. Information Systems and Informatics*, vol. 5, no. 4, 2025, doi: 10.51519/journalisi.v5i4.572.