ANALISIS MANAJEMEN KEAMANAN SISTEM INFORMASI MENGGUNAKAN STANDAR ISO/IEC 27001 (STUDI KASUS : Universitas Teknologi Digital Indonesia (UTDI))

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

Oleh :

NOVAL ENGGAR OKTAVIAN

221011400671

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang sangat pesat telah membawa perubahan besar dalam sistem pengelolaan data di berbagai sektor, termasuk dunia pendidikan tinggi. Perguruan tinggi kini sangat bergantung pada sistem informasi digital untuk mengelola kegiatan akademik, administrasi, dan keuangan. Salah satu sistem utama yang digunakan adalah Sistem Informasi Akademik (SIAKAD) yang berfungsi untuk mengatur proses pendaftaran mahasiswa, penyimpanan nilai, jadwal kuliah, serta laporan akademik secara terintegrasi.

Namun, peningkatan ketergantungan terhadap sistem digital juga diikuti dengan meningkatnya ancaman terhadap keamanan informasi. Kasus kebocoran data mahasiswa, serangan malware, serta penyalahgunaan akun pengguna menjadi isu yang sering dihadapi oleh institusi pendidikan. Kondisi ini menunjukkan bahwa keamanan informasi merupakan aspek penting yang harus dijaga agar data yang bersifat rahasia, sensitif, dan strategis tetap terlindungi dari ancaman internal maupun eksternal.

Universitas Teknologi Digital Indonesia (UTDI) sebagai perguruan tinggi yang berbasis teknologi informasi juga menghadapi tantangan serupa. Sistem akademik digital yang dikelola oleh Pusat Teknologi Informasi dan Data (PTID) UTDI menyimpan berbagai aset penting, mulai dari data mahasiswa, dosen, nilai, hingga keuangan kampus. Seluruh data ini memiliki nilai tinggi dan sangat berpotensi menjadi target ancaman siber jika tidak dilindungi dengan baik.

Untuk itu, diperlukan penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional ISO/IEC 27001, yang menyediakan kerangka kerja sistematis untuk melindungi kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Dengan penerapan ISO/IEC 27001, universitas dapat mengidentifikasi risiko keamanan, menerapkan kontrol mitigasi, serta membangun budaya keamanan informasi yang berkelanjutan.

Melalui analisis dan simulasi penerapan ISO/IEC 27001 pada UTDI, diharapkan dapat diperoleh gambaran mengenai sejauh mana kesiapan universitas dalam

mengimplementasikan sistem manajemen keamanan informasi yang sesuai dengan standar **internacional**

1.2.Identifikasi Masalah

Berdasarkan latar belakang di atas, maka dapat diidentifikasi beberapa masalah yang dihadapi Universitas Teknologi Digital Indonesia (UTDI) terkait keamanan informasi, yaitu:

1. Belum adanya penerapan formal terhadap **standar keamanan informasi ISO/IEC 27001** di lingkungan universitas.
2. Pengelolaan aset informasi belum sepenuhnya terdokumentasi dan diklasifikasikan berdasarkan tingkat kerahasiaan.
3. Sistem pengendalian akses masih terbatas, belum menerapkan **role-based access control (RBAC)** secara menyeluruh.
4. Tidak ada audit berkala terhadap aktivitas pengguna dan keamanan jaringan kampus.
5. Kesadaran staf dan mahasiswa terhadap keamanan siber masih rendah, sehingga rentan terhadap *phishing* atau penyalahgunaan akun.
6. Proses **backup data** belum dilakukan secara terjadwal dan tidak memiliki lokasi cadangan (*off-site*).

1.2 Rumusan Masalah

Dari identifikasi masalah di atas, maka rumusan masalah dalam penelitian dan analisis ini adalah sebagai berikut:

1. Bagaimana konteks organisasi dan pengelolaan keamanan informasi di Universitas Teknologi Digital Indonesia (UTDI)?
2. Apa saja aset informasi dan risiko keamanan yang terdapat pada sistem akademik UTDI?
3. Bagaimana hasil analisis risiko berdasarkan standar ISO/IEC 27001 dapat digunakan untuk merancang sistem manajemen keamanan informasi (SMKI) di universitas?
4. Kontrol keamanan apa yang paling relevan diterapkan untuk mengurangi risiko keamanan informasi di lingkungan akademik UTDI?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

1. Menganalisis penerapan prinsip dan struktur ISO/IEC 27001 pada sistem akademik di Universitas Teknologi Digital Indonesia.
2. Mengidentifikasi aset informasi utama serta potensi risiko yang dapat mengancam keamanan data akademik.
3. Melakukan penilaian risiko keamanan informasi dengan metode kualitatif (impact × likelihood).
4. Menyusun rancangan awal Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan hasil analisis risiko.
5. Memberikan rekomendasi kontrol mitigasi yang relevan dengan Annex A ISO/IEC 27001:2013 agar universitas dapat meningkatkan tingkat keamanan informasinya.

BAB II

ORGANISASI

2.1 Profil Organisasi

Universitas Teknologi Digital Indonesia (UTDI) merupakan perguruan tinggi fiktif yang bergerak di bidang pendidikan tinggi berbasis teknologi informasi dan komunikasi. UTDI berdiri pada tahun 2012 di bawah naungan Yayasan Cerdas Nusantara, dengan tujuan untuk mencetak sumber daya manusia yang unggul, inovatif, dan berdaya saing global dalam era transformasi digital.

Visi utama UTDI adalah:

"Menjadi universitas unggulan nasional berbasis teknologi digital yang berorientasi pada riset dan inovasi berkelanjutan."

Untuk mencapai visi tersebut, UTDI mengemban misi sebagai berikut:

1. Menyelenggarakan pendidikan tinggi berbasis teknologi informasi dan komunikasi.
2. Mengembangkan penelitian dan inovasi dalam bidang teknologi digital.
3. Melakukan pengabdian masyarakat berbasis teknologi tepat guna.
4. Membangun tata kelola universitas yang transparan, akuntabel, dan berlandaskan keamanan informasi.

UTDI memiliki lima fakultas utama, yaitu:

1. Fakultas Teknologi Informasi
2. Fakultas Ekonomi dan Bisnis
3. Fakultas Teknik Industri
4. Fakultas Ilmu Komunikasi dan Desain
5. Fakultas Hukum dan Sosial Humaniora

Jumlah mahasiswa aktif di UTDI mencapai sekitar 8.000 orang, dengan tenaga pengajar dan staf sebanyak 400 orang. Seluruh kegiatan akademik dan administrasi universitas didukung oleh sistem digital terintegrasi bernama Sistem Informasi Akademik Digital (SIAKAD-D). Sistem ini mencakup berbagai layanan seperti pendaftaran mahasiswa baru,

pengisian KRS, input nilai, pembayaran kuliah, serta pengelolaan data dosen dan kepegawaian.

Dalam menjalankan fungsinya, universitas ini memiliki beberapa unit strategis, di antaranya:

- Pusat Teknologi Informasi dan Data (PTID): unit yang bertanggung jawab atas infrastruktur jaringan, server, keamanan data, dan pengembangan sistem informasi.
- Biro Administrasi Akademik (BAA): mengelola data mahasiswa, nilai, jadwal, dan kegiatan akademik lainnya.
- Biro Keuangan dan SDM: menangani pengelolaan keuangan, penggajian, serta data kepegawaian.
- Unit Penjaminan Mutu dan Audit Internal (UPMAI): melakukan audit berkala terhadap sistem akademik, keuangan, dan keamanan informasi.

Struktur organisasi UTDI bersifat hierarkis dan fungsional, yang dipimpin oleh Rektor, dengan tiga Wakil Rektor yang masing-masing membawahi bidang akademik, keuangan dan SDM, serta riset dan kerja sama. Struktur ini memastikan adanya pembagian tanggung jawab yang jelas dan koordinasi yang efektif dalam pengelolaan sistem informasi dan data akademik.

Sebagai universitas berbasis teknologi digital, UTDI memandang keamanan informasi sebagai aspek strategis dalam menjaga kelancaran operasional dan reputasi institusi. Aset-aset informasi seperti data mahasiswa, dosen, keuangan, serta infrastruktur jaringan merupakan bagian penting yang harus dilindungi dari ancaman internal maupun eksternal. Oleh karena itu, UTDI berkomitmen untuk mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) dengan mengacu pada standar internasional ISO/IEC 27001:2013.

Ruang lingkup penerapan SMKI di UTDI difokuskan pada Pusat Teknologi Informasi dan Data (PTID) yang mengelola sistem SIAKAD-D, server universitas, dan jaringan data akademik. Dengan penerapan SMKI ini, universitas diharapkan mampu memastikan aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari seluruh informasi akademik dan administrasi.

2.2 Struktur Organisasi

Struktur organisasi Universitas Teknologi Digital Indonesia (UTDI) dirancang dengan pendekatan hierarkis dan fungsional, yang memungkinkan setiap unit memiliki tanggung jawab dan wewenang yang jelas. Tujuannya adalah untuk menciptakan tata kelola yang efektif, efisien, dan selaras dengan prinsip good university governance serta mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2013.

Struktur organisasi UTDI terdiri atas unsur pimpinan universitas, unsur pelaksana akademik, serta unit penunjang dan pengawasan internal. Berikut uraian struktur dan peran masing-masing bagian:

1. Rektor

   Rektor merupakan pimpinan tertinggi universitas yang memiliki tanggung jawab penuh terhadap arah kebijakan akademik, administrasi, keuangan, serta pengembangan sistem informasi universitas.
   Rektor juga berperan sebagai penanggung jawab utama dalam penerapan kebijakan keamanan informasi dan memastikan seluruh kebijakan universitas sejalan dengan standar ISO/IEC 27001.

2. Wakil Rektor I (Bidang Akademik dan Kemahasiswaan)

   Wakil Rektor I bertugas mengkoordinasikan kegiatan akademik, proses belajar mengajar, dan pelayanan mahasiswa.
   Unit ini bekerja sama dengan Biro Administrasi Akademik (BAA) dalam mengelola data akademik dan memastikan sistem informasi akademik (SIAKAD-D) berfungsi dengan baik dan aman.

3. Wakil Rektor II (Bidang Keuangan dan Sumber Daya Manusia)

   Wakil Rektor II bertanggung jawab terhadap pengelolaan anggaran, akuntansi, keuangan, dan administrasi pegawai.
   Dalam konteks keamanan informasi, bidang ini berperan dalam melindungi data keuangan dan data kepegawaian, termasuk sistem pembayaran digital dan database staf universitas.

4. Wakil Rektor III (Bidang Riset, Inovasi, dan Kerja Sama)

Wakil Rektor III mengelola kegiatan penelitian, publikasi ilmiah, pengabdian kepada masyarakat, dan kerja sama institusional.
Unit ini juga terlibat dalam pengelolaan data riset digital dan repository akademik, sehingga perlu menjamin keamanan dan integritas data penelitian universitas.

5. Pusat Teknologi Informasi dan Data (PTID)

PTID merupakan unit teknis utama yang bertanggung jawab atas seluruh infrastruktur teknologi informasi, termasuk jaringan kampus, server, sistem informasi akademik, dan keamanan data.
Peran PTID sangat penting dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI), karena mengelola aset utama berupa:

- Server akademik dan server cadangan (backup)
- Akses jaringan dan sistem login SIAKAD
- Manajemen akun pengguna (user access management)
- Audit keamanan, enkripsi, dan kebijakan backup data

PTID juga bertanggung jawab langsung kepada Rektor melalui koordinasi dengan Wakil Rektor I.

6. Biro Administrasi Akademik (BAA)

BAA merupakan unit pelaksana administrasi akademik yang menangani seluruh kegiatan operasional akademik seperti registrasi mahasiswa, pengisian KRS, input nilai, serta penerbitan transkrip.
Unit ini menjadi pengguna utama sistem informasi akademik, sehingga harus memiliki kesadaran tinggi terhadap kebijakan keamanan data dan akses informasi.

7. Biro Keuangan dan SDM

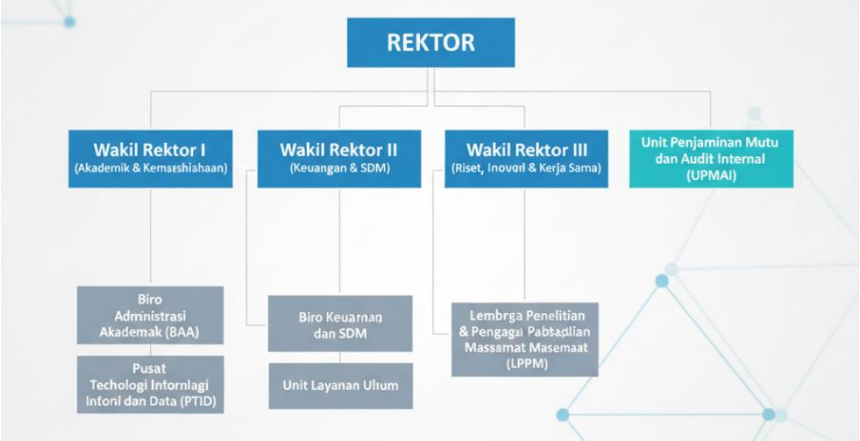
Biro ini menangani pengelolaan keuangan, pembayaran kuliah, gaji dosen, serta data personal pegawai.
Karena menangani data sensitif, biro ini wajib menerapkan kontrol keamanan data sesuai prinsip ISO 27001 seperti confidentiality (kerahasiaan) dan integrity (integritas data).

8. Unit Penjaminan Mutu dan Audit Internal (UPMAI)

UPMAI memiliki fungsi pengawasan dan evaluasi terhadap pelaksanaan kegiatan akademik, administrasi, serta penerapan keamanan informasi.
Unit ini juga melakukan audit internal terhadap pelaksanaan SMKI untuk memastikan kepatuhan terhadap standar ISO/IEC 27001 dan kebijakan universitas.

9. Fakultas dan Program Studi

Masing-masing fakultas memiliki tanggung jawab dalam melaksanakan kegiatan akademik di tingkat program studi.
Dosen dan tenaga kependidikan menggunakan SIAKAD-D untuk melakukan input nilai, pemantauan mahasiswa, dan pelaporan kegiatan akademik.
Fakultas juga menjadi pengguna langsung dari sistem informasi yang perlu dijaga keamanannya.



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	Dampak terhadap Keamanan Informasi
Internal	Kurangnya kebijakan keamanan informasi yang formal di tingkat universitas	Risiko inkonsistensi dalam pengelolaan data dan akses informasi
Internal	Minimnya pelatihan keamanan siber bagi staf dan mahasiswa	Potensi *phishing* atau penyalahgunaan kredensial
Internal	Backup data hanya dilakukan secara manual dan tidak rutin	Risiko kehilangan data akibat kerusakan atau serangan
Eksternal	Ancaman serangan siber (hacker, ransomware) terhadap server universitas	Gangguan layanan akademik dan potensi kebocoran data
Eksternal	Ketergantungan pada jaringan internet untuk seluruh sistem akademik	Keterlambatan akses dan gangguan operasional bila terjadi downtime
Eksternal	Regulasi pemerintah terkait perlindungan data pribadi (UU PDP)	Universitas wajib menyesuaikan dengan standar perlindungan data nasional

3.2.1 Pihak-Pihak Berkepentingan dan Kebutuhan Keamanan Informasi

Stakeholder	Kebutuhan Keamanan Informasi
Rektor dan Pimpinan	Data strategis universitas harus akurat, terlindungi, dan tersedia kapan pun diperlukan.
Pusat Teknologi Informasi & Data (PTID)	Sistem keamanan jaringan dan backup data berjalan efektif dan dapat diaudit.

Stakeholder	Kebutuhan Keamanan Informasi
Biro Akademik	Akses terhadap data mahasiswa dan nilai harus aman dan sesuai wewenang.
Dosen dan Staf	Kemudahan akses ke sistem akademik tanpa mengorbankan keamanan data.
Mahasiswa	Perlindungan data pribadi dan akses aman ke portal akademik.
Pemerintah dan BAN-PT	Kepatuhan terhadap regulasi keamanan informasi dan audit sistem informasi akademik.

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 akibat akses tidak sah	Tidak ada kontrol berbasis peran (RBAC)	5	4	**20 (Tinggi)**	Terapkan enkripsi database dan kebijakan hak akses.
2	Server akademik	Serangan malware/ransomware	Tidak ada IDS/IPS aktif	5	3	**15 (Tinggi)**	Instal IDS/IPS dan backup harian terenkripsi.
3	Sistem login SIAKAD-D	Penyalahgunaan akun pengguna	Tidak ada rotasi password dan audit log	4	4	**16 (Tinggi)**	Terapkan 2FA dan audit log periodik.

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
4	Dokumen akademik digital	Perubahan atau penghapusan data	Tidak ada enkripsi file server	3	3	**9 (Sedang)**	Gunakan enkripsi dan sistem versioning dokumen.
5	Infrastruktur jaringan	Serangan DDoS dan sniffing	Firewall belum dikonfigurasi optimal	5	2	**10 (Sedang)**	Konfigurasi ulang firewall dan segmentasi jaringan.
6	Email staf dan dosen	Phishing dan social engineering	Tidak ada pelatihan kesadaran keamanan	4	4	**16 (Tinggi)**	Pelatihan awareness dan filter anti-phishing.
7	Data keuangan mahasiswa	Manipulasi data pembayaran	Tidak ada audit transaksi otomatis	4	3	**12 (Sedang)**	Terapkan sistem audit digital dan validasi dua arah.
8	Server cadangan (backup)	Kehilangan data karena kerusakan fisik	Tidak ada backup off-site	4	2	**8 (Sedang)**	Terapkan backup ke lokasi berbeda dan replikasi otomatis.

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
9	Akun administrator IT	Penyalahgunaan hak istimewa	Tidak ada kontrol pengawasan hak akses	5	3	**15 (Tinggi)**	Audit hak akses dan prinsip least privilege.
10	Aplikasi mobile akademik	Penyadapan data login	Koneksi belum menggunakan SSL/TLS	4	3	**12 (Sedang)**	Gunakan SSL/TLS dan enkripsi komunikasi end-to-end.