**Analisis dan Implementasi Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO/IEC 27001**

**Studi Kasus: Divisi Teknologi Informasi Universitas Pamulang   
(Aplikasi MyUnpam)**



**Oleh :**

**Reza Fahlevi (221011402441)**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PAMULANG**

**TANGERANG SELATAN**

**2025**

# DAFTAR ISI

[DAFTAR ISI 2](#_Toc212642112)

[PENDAHULUAN 3](#_Toc212642113)

[Tahap 1 Pemilihan Organisasi dan Ruang Lingkup SMKI 5](#_Toc212642114)

[1.1 Pemilihan Organisasi 5](#_Toc212642115)

[1.2 Ruang Lingkup SMKI 5](#_Toc212642116)

[1.2 Profil Singkat Universitas Pamulang 6](#_Toc212642117)

[1.2.1 Jenis Bisnis 6](#_Toc212642118)

[1.2.2 Struktur Organisasi Singkat 6](#_Toc212642119)

[1.2.3 Layanan Utama 7](#_Toc212642120)

[1.2.4 Data atau Aset Informasi Penting 7](#_Toc212642121)

[Tahap 2 Analisis Konteks Organisasi 9](#_Toc212642122)

[2.1 Isu Internal dan Eksternal 9](#_Toc212642123)

[2.2 Pihak Berkepentingan dan Kebutuhan 10](#_Toc212642124)

[Tahap 3 Penilaian Risiko Keamanan Informasi 11](#_Toc212642125)

[KESIMPULAN 13](#_Toc212642126)

# PENDAHULUAN

Dalam era digital saat ini, keamanan informasi menjadi aspek yang sangat krusial bagi setiap organisasi, termasuk lembaga pendidikan tinggi. Perguruan tinggi modern tidak hanya berfungsi sebagai pusat pendidikan, tetapi juga sebagai pengelola data akademik, keuangan, dan pribadi dari puluhan ribu mahasiswa, dosen, serta tenaga kependidikan. Oleh karena itu, penerapan sistem keamanan informasi yang efektif merupakan kebutuhan strategis untuk menjamin kelangsungan operasional dan menjaga kepercayaan publik.

Universitas Pamulang (UNPAM) sebagai salah satu universitas swasta terbesar di Indonesia telah mengimplementasikan berbagai layanan digital untuk menunjang kegiatan akademik, salah satunya adalah aplikasi MyUnpam. Aplikasi ini berfungsi sebagai platform terpadu untuk mengelola aktivitas akademik seperti pengisian Kartu Rencana Studi (KRS), pencatatan nilai, jadwal kuliah, serta proses administrasi mahasiswa. Namun, seiring meningkatnya ketergantungan terhadap sistem daring, muncul pula berbagai tantangan terkait keamanan, seperti potensi peretasan, kebocoran data pribadi, dan gangguan layanan akibat serangan siber.

Untuk menghadapi tantangan tersebut, diperlukan penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur dan sesuai dengan standar internasional ISO/IEC 27001 (Nurbojatmiko et al., 2025). Standar ini memberikan kerangka kerja yang komprehensif dalam mengidentifikasi aset informasi, menganalisis risiko, serta menetapkan kontrol keamanan yang tepat guna melindungi informasi organisasi.

Laporan ini disusun sebagai bagian dari simulasi penerapan ISO/IEC 27001 di Universitas Pamulang dengan fokus pada Divisi Teknologi Informasi dan keamanan aplikasi MyUnpam. Tujuan utama dari analisis ini adalah untuk:

1. Memahami k onteks organisasi dan faktor-faktor yang memengaruhi keamanan informasi.
2. Mengidentifikasi aset informasi utama beserta potensi ancaman dan kerentanannya.
3. Melakukan penilaian risiko dan menentukan prioritas mitigasi untuk meningkatkan keamanan sistem.

Melalui analisis ini diharapkan Universitas Pamulang dapat memperoleh gambaran menyeluruh mengenai kondisi keamanan informasinya saat ini dan memiliki dasar yang kuat untuk merancang kebijakan serta prosedur keamanan yang sejalan dengan prinsip-prinsip ISO/IEC 27001 (Fathurohman & Witjaksono, 2020).

# Tahap 1 Pemilihan Organisasi dan Ruang Lingkup SMKI

## 1.1 Pemilihan Organisasi

Organisasi yang dipilih dalam simulasi penerapan Sistem Manajemen Keamanan Informasi (SMKI) ini adalah Universitas Pamulang (UNPAM).

Universitas Pamulang dipilih karena merupakan salah satu perguruan tinggi swasta terbesar di Indonesia yang telah menerapkan sistem informasi akademik berbasis daring, yaitu aplikasi MyUnpam. Sistem ini menjadi tulang punggung dalam pengelolaan data mahasiswa dan kegiatan akademik sehari-hari. Dengan kompleksitas data dan tingginya tingkat penggunaan, aplikasi MyUnpam berpotensi menghadapi berbagai risiko keamanan informasi, sehingga penerapan SMKI menjadi sangat relevan (Nurbojatmiko et al., 2025; Paramita et al., 2022).

## 1.2 Ruang Lingkup SMKI

Ruang lingkup implementasi Sistem Manajemen Keamanan Informasi (SMKI) difokuskan pada Divisi Teknologi Informasi Universitas Pamulang, khususnya pada pengelolaan dan keamanan aplikasi MyUnpam.

Ruang lingkup ini mencakup seluruh proses yang berkaitan dengan penyimpanan, pemrosesan, dan pengelolaan data mahasiswa, dosen, serta staf administrasi melalui aplikasi tersebut. Fokus utama penerapan SMKI meliputi tiga aspek keamanan informasi, yaitu:

1. Kerahasiaan (Confidentiality): Melindungi data pribadi dan akademik pengguna dari akses tidak sah.
2. Integritas (Integrity): Menjamin keakuratan, keutuhan, dan keandalan data akademik di dalam sistem.
3. Ketersediaan (Availability): Menjaga agar layanan MyUnpam tetap beroperasi dan dapat diakses kapan pun dibutuhkan.

Ruang lingkup ini juga mempertimbangkan aspek kepatuhan terhadap regulasi nasional, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta prinsip keamanan informasi dalam standar ISO/IEC 27001:2022 (Fathurohman & Witjaksono, 2020; Nurbojatmiko et al., 2025).

## 1.2 Profil Singkat Universitas Pamulang

Universitas Pamulang (UNPAM) merupakan perguruan tinggi swasta yang berlokasi di Tangerang Selatan, Banten. UNPAM memiliki lebih dari 50.000 mahasiswa aktif dari berbagai fakultas seperti Ekonomi, Hukum, Teknik, Sastra, dan Ilmu Komputer. Dalam kegiatan akademiknya, UNPAM menggunakan aplikasi MyUnpam, sistem informasi akademik berbasis web dan mobile (Paramita et al., 2022).

### 1.2.1 Jenis Bisnis

Universitas Pamulang (UNPAM) merupakan lembaga pendidikan tinggi swasta yang berfokus pada penyelenggaraan pendidikan akademik di berbagai bidang ilmu. UNPAM berperan sebagai institusi pendidikan, penelitian, dan pengabdian kepada masyarakat.

Sebagai lembaga pendidikan, UNPAM memiliki tanggung jawab besar dalam menjaga keamanan data akademik, data pribadi mahasiswa dan dosen, serta informasi administratif lainnya yang menjadi aset penting universitas (Nurbojatmiko et al., 2025).

### 1.2.2 Struktur Organisasi Singkat

Struktur organisasi Universitas Pamulang secara umum terdiri dari:

1. Rektorat, yang memimpin seluruh kegiatan universitas dan pengambilan kebijakan strategis.
2. Wakil Rektor, yang membawahi bidang akademik, kemahasiswaan, keuangan, dan sumber daya manusia.
3. Dekan dan Fakultas, yang mengelola kegiatan akademik di tingkat program studi.
4. Biro Administrasi Akademik dan Kemahasiswaan (BAAK), yang bertanggung jawab atas pengelolaan data akademik.
5. Divisi Teknologi Informasi (TI), yang mengelola sistem informasi, jaringan, infrastruktur, serta keamanan sistem digital termasuk aplikasi MyUnpam.

Divisi Teknologi Informasi menjadi unit utama dalam lingkup SMKI, karena berperan langsung dalam pengembangan, pemeliharaan, dan pengamanan data di lingkungan sistem akademik (Fathurohman & Witjaksono, 2020).

### 1.2.3 Layanan Utama

Universitas Pamulang menyediakan berbagai layanan akademik dan administrasi berbasis teknologi, antara lain:

1. Sistem Informasi Akademik MyUnpam untuk mahasiswa dan dosen.
2. Portal e-learning untuk kegiatan perkuliahan daring.
3. Sistem informasi keuangan untuk pembayaran biaya kuliah.
4. Sistem kehadiran dan penilaian mahasiswa secara online.
5. Layanan surat dan dokumen akademik digital.

Layanan tersebut bergantung pada konektivitas jaringan, keandalan server, serta keamanan basis data yang dikelola oleh Divisi Teknologi Informasi.

### 1.2.4 Data atau Aset Informasi Penting

Beberapa data dan aset informasi penting yang menjadi objek perlindungan dalam ruang lingkup SMKI Universitas Pamulang meliputi:

1. Data pribadi mahasiswa dan dosen (nama, NIM/NIDN, alamat, kontak, dan data pribadi lainnya).
2. Data akademik (nilai, jadwal kuliah, KRS, presensi, hasil ujian).
3. Data keuangan (transaksi pembayaran kuliah, laporan keuangan mahasiswa).
4. Akun dan kredensial pengguna (username, password, hak akses).
5. Infrastruktur TI dan server MyUnpam yang menyimpan serta memproses seluruh data universitas.

Aset-aset informasi tersebut menjadi komponen krusial dalam operasional kampus, sehingga harus dilindungi dari ancaman kebocoran, kerusakan, maupun kehilangan data.

# Tahap 2 Analisis Konteks Organisasi

## 2.1 Isu Internal dan Eksternal

Tahap ini bertujuan untuk menganalisis kondisi internal dan eksternal organisasi yang memengaruhi keamanan informasi, serta mengidentifikasi pihak-pihak berkepentingan (stakeholder) yang terlibat.

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Jenis Isu** | **Deskripsi Isu** | **Dampak terhadap Keamanan Informasi** |
| 1 | Internal | Server dan jaringan dikelola lokal dengan kapasitas terbatas | Risiko downtime dan kehilangan data |
| 2 | Internal | Belum ada SOP penanganan insiden | Insiden siber sulit ditangani |
| 3 | Internal | Kurangnya pelatihan keamanan bagi staf IT | Human error meningkat |
| 4 | Eksternal | Peningkatan serangan siber terhadap kampus | Potensi peretasan MyUnpam |
| 5 | Eksternal | Regulasi UU PDP 2022 | Kewajiban kepatuhan terhadap hukum |
| 6 | Eksternal | Ketergantungan layanan cloud & internet | Gangguan operasional |

## 2.2 Pihak Berkepentingan dan Kebutuhan

|  |  |  |  |
| --- | --- | --- | --- |
| No | Pihak Berkepentingan | Kebutuhan terhadap Keamanan Informasi | Dampak Bila Tidak Terpenuhi |
| 1 | Mahasiswa | Data pribadi dan nilai aman | Kehilangan kepercayaan |
| 2 | Dosen | Akses aman untuk input nilai | Manipulasi data akademik |
| 3 | Staf IT | Pedoman keamanan sistem | Kesalahan konfigurasi |
| 4 | Pimpinan Universitas | Kepatuhan & reputasi lembaga | Risiko hukum |
| 5 | Regulator | Kepatuhan terhadap UU PDP | Sanksi administratif |

# Tahap 3 Penilaian Risiko Keamanan Informasi

Tahap ini melibatkan proses identifikasi, analisis, dan evaluasi risiko keamanan informasi berdasarkan ISO/IEC 27001 dan ISO/IEC 27005. Metode yang digunakan adalah pendekatan kualitatif menggunakan Risk Matrix Template.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Aset | Ancaman | Kerentanan | Dampak | Kemungkinan | Level Risiko | Tindakan Mitigasi |
| Server MyUnpam | Serangan DDoS | Bandwidth rendah, tanpa firewall | Tinggi | Sedang | Tinggi | Implementasi firewall & CDN |
| Database Mahasiswa | SQL Injection | Validasi input lemah | Tinggi | Tinggi | Sangat Tinggi | Audit kode & query parameter |
| Akun Admin | Pencurian password | Tidak ada MFA | Tinggi | Sedang | Tinggi | Terapkan MFA & kebijakan password kuat |
| Data Mahasiswa | Insider threat | Akses tanpa RBAC | Tinggi | Rendah | Sedang | Role-Based Access Control |
| Aplikasi Web | Malware / deface | Patch keamanan tidak rutin | Sedang | Sedang | Sedang | Patch & vulnerability scan berkala |
| Jaringan | Sniffing data | Tanpa enkripsi TLS | Tinggi | Sedang | Tinggi | Implementasi HTTPS & VPN internal |
| Backup Data | Kehilangan data | Tidak ada backup otomatis | Tinggi | Sedang | Tinggi | Backup otomatis harian |

Dari hasil analisis risiko di atas, dapat disimpulkan bahwa area dengan tingkat risiko tinggi perlu segera dilakukan tindakan mitigasi teknis dan administratif sesuai rekomendasi ISO/IEC 27001.

# KESIMPULAN

Berdasarkan hasil analisis dari tahap 1 hingga tahap 3, penerapan Sistem Manajemen Keamanan Informasi (SMKI) pada Universitas Pamulang (UNPAM), khususnya di Divisi Teknologi Informasi yang mengelola aplikasi MyUnpam, menunjukkan bahwa organisasi memiliki kebutuhan mendesak untuk membangun sistem keamanan informasi yang terstruktur dan berkelanjutan.

Tahap pertama (Pemilihan Organisasi) menunjukkan bahwa Universitas Pamulang memiliki lingkungan operasional yang kompleks dengan jumlah pengguna sistem yang sangat besar. Aplikasi MyUnpam sebagai sistem informasi akademik utama berperan penting dalam menjaga keberlangsungan kegiatan akademik, sehingga menjadi aset strategis yang harus dilindungi. Ruang lingkup SMKI difokuskan pada Divisi Teknologi Informasi yang bertanggung jawab atas keamanan data, sistem, dan infrastruktur digital universitas.

Tahap kedua (Analisis Konteks Organisasi) mengungkap bahwa terdapat berbagai isu internal seperti keterbatasan sumber daya TI, kurangnya pelatihan keamanan, dan belum adanya SOP penanganan insiden siber. Di sisi eksternal, UNPAM menghadapi ancaman dari meningkatnya serangan siber terhadap sektor pendidikan serta kewajiban kepatuhan terhadap regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Selain itu, analisis stakeholder memperlihatkan bahwa keamanan informasi tidak hanya berdampak pada aspek teknis, tetapi juga reputasi institusi dan kepercayaan publik.

Tahap ketiga (Penilaian Risiko Keamanan Informasi) menunjukkan bahwa terdapat sejumlah risiko dengan tingkat tinggi hingga sangat tinggi, terutama yang berkaitan dengan ancaman serangan siber, kebocoran data, dan kesalahan konfigurasi sistem. Risiko tertinggi ditemukan pada database mahasiswa (potensi SQL Injection), infrastruktur jaringan tanpa enkripsi, serta akses akun tanpa autentikasi ganda (MFA). Kondisi ini menunjukkan bahwa pengendalian keamanan yang ada saat ini masih perlu diperkuat, baik dari sisi teknis, kebijakan, maupun pelatihan sumber daya manusia.

Secara keseluruhan, hasil analisis tahap 1–3 menegaskan bahwa Universitas Pamulang perlu segera merancang kerangka kerja keamanan informasi berbasis ISO/IEC 27001, yang mencakup kebijakan, kontrol teknis, serta mekanisme pemantauan dan evaluasi risiko secara berkala. Langkah ini akan menjadi fondasi penting bagi peningkatan keamanan aplikasi MyUnpam dan perlindungan seluruh aset informasi universitas.

Tahapan berikutnya (Tahap 4–6) akan berfokus pada pemilihan kontrol keamanan dari Annex A ISO/IEC 27001, perancangan dokumen utama SMKI (kebijakan, tujuan, dan rencana implementasi), serta penyusunan rekomendasi tindak lanjut untuk mencapai tingkat kepatuhan terhadap standar internasional tersebut.

# DAFTAR PUSTAKA

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Nurbojatmiko, N., Karimiyah, M. S. K., Asnadi, N. M., & Anisyah, R. (2025). ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review. *Sinkron*, *9*(1), 484–492. https://doi.org/10.33395/sinkron.v9i1.14448

Paramita, S., Siregar, S. A., Damanik, R. A., & Dedi Irawan, M. (2022). Bulletin of Information Technology (BIT) Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374–379.