**ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001   
( STUDI KASUS pada Rumah Sakit Umum Daerah (RSUD) Kota Semarang )**



Disusun Oleh :

Muhammad Satrio Wibowo [221011403165]  
Yoga Fikriansyah. P [221011400694]

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS KOMPUTER  
UNIVERSITAS PAMULANG  
2025**

**BAB I**

**PENDAHULUAN**

**1.1 Latar Belakang**

Keamanan informasi telah menjadi prioritas utama bagi organisasi di era digital. Ancaman siber seperti pencurian data, malware, phishing, dan kebocoran sistem dapat menyebabkan kerugian finansial maupun reputasi. Oleh karena itu, organisasi perlu menerapkan sistem yang sistematis dan terdokumentasi untuk melindungi aset informasinya.

ISO/IEC 27001 merupakan standar internasional yang memberikan kerangka kerja dalam membangun **Sistem Manajemen Keamanan Informasi (SMKI)**. Standar ini membantu organisasi dalam mengidentifikasi, mengelola, dan meminimalkan risiko terhadap informasi yang dimilikinya. Melalui penerapan ISO 27001, organisasi dapat menunjukkan komitmen terhadap keamanan informasi kepada pihak internal dan eksternal.

Dalam laporan ini, dilakukan simulasi penerapan ISO/IEC 27001 pada **PT Semarang Digital Solusi**, sebuah startup di bidang teknologi informasi, untuk memahami bagaimana proses analisis risiko dan implementasi kontrol dilakukan secara sistematis.

**1.2 Rumusan Masalah**

1. Bagaimana konteks organisasi PT Semarang Digital Solusi dalam penerapan SMKI berdasarkan ISO 27001?
2. Apa saja risiko utama terhadap keamanan informasi yang ada di divisi IT perusahaan tersebut?
3. Bagaimana langkah mitigasi yang dapat diterapkan untuk mengurangi tingkat risiko tersebut?

**1.3 Tujuan Penelitian**

1. Menganalisis konteks organisasi dan kebutuhan keamanan informasi.
2. Mengidentifikasi risiko keamanan informasi berdasarkan aset yang dimiliki.
3. Menentukan kontrol keamanan yang relevan sesuai Annex A ISO/IEC 27001:2022.
4. Menyusun rancangan awal dokumen SMKI sebagai dasar implementasi lebih lanjut.

**1.4 Manfaat Penelitian**

* Memberikan pemahaman kepada mahasiswa mengenai penerapan ISO/IEC 27001.
* Menjadi referensi bagi organisasi yang ingin membangun sistem keamanan informasi.
* Membantu dalam pengambilan keputusan strategis terkait keamanan data dan aset digital.

**1.5 Metodologi Penelitian**

Metode yang digunakan meliputi:

* **Studi literatur** terhadap ISO/IEC 27001 dan referensi akademik.
* **Analisis kualitatif** untuk menilai risiko berdasarkan dampak dan kemungkinan.
* **Simulasi organisasi fiktif** untuk memodelkan penerapan SMKI tahap awal.

**BAB II**

**TAHAP 1: PEMILIHAN ORGANISASI**

**2.1 Profil Organisasi**

**Nama Organisasi:** PT Semarang Digital Solusi  
**Jenis Usaha:** Startup Teknologi Informasi  
**Alamat:** Jl. Imam Bonjol No. 120, Semarang  
**Struktur Organisasi:**

* Direktur Utama
* Kepala Divisi IT
* Kepala Keuangan
* Kepala Pemasaran
* Tim Developer & Support

**Layanan Utama:**

1. Pengembangan aplikasi berbasis web dan mobile.
2. Layanan cloud hosting untuk UMKM.
3. Pengelolaan sistem informasi pelanggan.

**Aset Informasi Utama:**

* Database pelanggan dan proyek.
* Source code aplikasi internal dan klien.
* Server cloud dan sistem penyimpanan internal.
* Akun admin sistem dan perangkat jaringan.

**2.2 Ruang Lingkup SMKI**

Ruang lingkup implementasi SMKI difokuskan pada **Divisi Teknologi Informasi (IT Department)**.  
Lingkup ini mencakup:

* Pengelolaan server dan database pelanggan.
* Proteksi source code dan sistem internal.
* Manajemen hak akses pengguna.
* Pemantauan keamanan jaringan dan perangkat keras.

**ANALISIS KONTEKS ORGANISASI**

1. **2.1 Profil Organisasi**

**Nama Organisasi:** PT. Semarang Digital Teknologi (SDT)  
**Bidang Usaha:** Pengembangan perangkat lunak, hosting server, dan solusi digital marketing.  
**Struktur Organisasi Singkat:**

* Direktur Utama
* Divisi Teknologi Informasi (TI)
* Divisi Keuangan dan Administrasi
* Divisi Pemasaran dan Layanan Klien
* Divisi Keamanan dan Infrastruktur

**Layanan Utama:**

* Pembuatan website dan aplikasi mobile
* Pengelolaan cloud server dan hosting
* Jasa keamanan siber (cybersecurity services)
* Konsultasi transformasi digital

**Aset Informasi Penting:**

* Database klien (informasi pengguna, kontrak, proyek)
* Source code aplikasi
* Server produksi dan backup
* Dokumen keuangan
* Data pegawai dan akses login sistem internal

1. **2.2 Ruang Lingkup SMKI**

SMKI difokuskan pada **Divisi Teknologi Informasi dan Keamanan**, mencakup:

* Pengelolaan data pelanggan, server, dan sistem informasi internal.
* Perlindungan terhadap data digital yang disimpan di cloud serta backup lokal.
* Pemantauan keamanan jaringan dan akses sistem.

1. **2.3 Analisis Isu Internal dan Eksternal**

|  |  |  |
| --- | --- | --- |
| **Kategori** | **Isu Utama** | **Dampak terhadap Keamanan Informasi** |
| Internal | Kurangnya pelatihan staf terkait keamanan siber | Potensi human error dan pelanggaran prosedur |
| Internal | Penggunaan sistem open-source tanpa kontrol patch | Meningkatkan risiko eksploitasi celah keamanan |
| Eksternal | Ancaman serangan phishing dan malware | Gangguan layanan dan kebocoran data klien |
| Eksternal | Perubahan regulasi pemerintah (UU PDP, ISO 27001:2022 update) | Perlu penyesuaian kebijakan keamanan |
| Eksternal | Kompetisi pasar digital tinggi | Tekanan operasional dapat menurunkan fokus pada keamanan |

1. **2.4 Analisis SWOT**

|  |  |
| --- | --- |
| **Faktor** | **Deskripsi** |
| **Strengths** | Tim TI berpengalaman, server lokal dengan backup harian, dan sistem enkripsi aktif. |
| **Weaknesses** | Belum ada dokumen kebijakan keamanan formal dan kurangnya audit internal rutin. |
| **Opportunities** | Sertifikasi ISO 27001 dapat meningkatkan kepercayaan klien dan daya saing. |
| **Threats** | Ancaman siber meningkat, termasuk ransomware dan social engineering. |

1. **2.5 Pihak Berkepentingan dan Kebutuhan**

|  |  |
| --- | --- |
| **Pihak Berkepentingan** | **Kebutuhan terhadap Keamanan Informasi** |
| Manajemen | Kepastian kepatuhan regulasi dan perlindungan reputasi |
| Karyawan | Kejelasan tanggung jawab dan akses yang aman |
| Klien | Keamanan data dan privasi terjamin |
| Regulator | Penerapan kebijakan sesuai UU Perlindungan Data Pribadi |
| Vendor IT | Prosedur keamanan saat integrasi sistem pihak ketiga |

1. **2.6 Konteks Regulasi dan Kepatuhan**

PT. SDT wajib memperhatikan:

* **ISO/IEC 27001:2022** – Standar internasional SMKI
* **Undang-Undang No. 27 Tahun 2022** tentang Perlindungan Data Pribadi (UU PDP)
* **Peraturan Pemerintah No. 71 Tahun 2019** tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)
* Kebijakan keamanan jaringan internal dan kebijakan keamanan cloud dari vendor hosting