**ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001:2022 PADA PT. INOVASI TEKNOLOGI INDONESIA**



Disusun Oleh:  
Anugrah Ageng Prasetyo  
221011401510

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

Daftar isi

**BAB I   
PENDAHULUAN**

**1.1 Latar Belakang**

Dalam era digital yang ditandai dengan pesatnya perkembangan teknologi informasi, aset informasi telah menjadi tulang punggung bagi kelangsungan dan kesuksesan suatu organisasi, baik di sektor swasta maupun publik. Aset informasi ini tidak hanya terbatas pada data digital, tetapi juga mencakup perangkat keras, perangkat lunak, sumber daya manusia, dan bahkan reputasi organisasi. PT. Inovasi Teknologi Indonesia (PT. ITI), sebuah perusahaan fiktif yang bergerak di bidang pengembangan software dan konsultan TI, menyadari betul bahwa keamanan aset informasinya merupakan hal yang kritis.

PT. ITI menghadapi berbagai tantangan dan ancaman keamanan informasi yang kompleks. Beberapa insiden seperti upaya *phishing* terhadap karyawan, potensi kebocoran data kekayaan intelektual proyek, dan risiko serangan *ransomware* pada server pengembangan mulai mengkhawatirkan manajemen. Selain ancaman eksternal, kerentanan juga datang dari dalam, seperti kurangnya kesadaran keamanan (*human error*), kebijakan keamanan yang tidak terdokumentasi dengan baik, dan tidak adanya kerangka kerja manajemen keamanan yang terstruktur.

Ketergantungan yang tinggi pada sistem informasi untuk operasional sehari-hari, pengembangan produk, dan interaksi dengan klien menuntut PT. ITI untuk memiliki suatu sistem yang dapat mengelola, memantau, dan terus meningkatkan keamanan informasinya. Tanpa sistem yang terkelola, setiap insiden keamanan tidak hanya dapat mengakibatkan kerugian finansial yang signifikan tetapi juga merusak kepercayaan klien dan reputasi perusahaan yang telah dibangun bertahun-tahun.

ISO/IEC 27001:2022 merupakan standar internasional yang diakui secara global untuk Sistem Manajemen Keamanan Informasi (SMKI). Standar ini menyediakan kerangka kerja yang sistematis dan holistik untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan keamanan informasi dalam suatu organisasi. Dengan mengadopsi ISO/IEC 27001, organisasi dapat secara proaktif mengidentifikasi risiko, menerapkan kontrol yang tepat, dan membangun budaya keamanan informasi di semua tingkat organisasi.

Berdasarkan latar belakang inilah, makalah ini menganalisis kebutuhan dan merancang strategi untuk mengimplementasikan SMKI berdasarkan ISO/IEC 27001:2022 di PT. Inovasi Teknologi Indonesia. Implementasi ini diharapkan dapat menjadi solusi yang komprehensif untuk memitigasi risiko, melindungi aset informasi, dan memastikan keberlangsungan bisnis perusahaan.

**1.2 Tujuan**

Secara umum, makalah ini bertujuan untuk menganalisis dan merancang rencana implementasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001:2022 di PT. Inovasi Teknologi Indonesia.

Secara khusus, tujuan dari makalah ini adalah:

1. **Menganalisis Kebutuhan:** Mengidentifikasi dan menganalisis kondisi eksisting keamanan informasi di PT. ITI, termasuk aset, ancaman, kerentanan, dan risiko yang dihadapinya.
2. **Merancang Rencana Implementasi SMKI:** Menyusun langkah-langkah sistematis untuk menerapkan SMKI, mulai dari perencanaan, penetapan kebijakan, pelaksanaan kontrol, hingga persiapan untuk sertifikasi.
3. **Mengidentifikasi Kontrol Keamanan:** Memilih dan merancang kontrol keamanan dari Annex A ISO/IEC 27001:2022 yang relevan dengan konteks dan risiko bisnis PT. ITI.
4. **Membangun Kerangka Peningkatan Berkelanjutan:** Merancang mekanisme untuk pemantauan, pengukuran, tinjauan, dan peningkatan berkelanjutan (*Continual Improvement*) dari SMKI.

**1.3 Ruang Lingkup**

Agar analisis dan implementasi dalam makalah ini dapat terfokus dan terukur, ruang lingkup pembahasan dibatasi pada hal-hal berikut:

1. **Organisasi:** Kajian ini hanya berfokus pada PT. Inovasi Teknologi Indonesia, dengan mempertimbangkan struktur organisasi, proses bisnis, dan budaya perusahaan yang spesifik.
2. **Aset Informasi dalam Lingkup:** Implementasi SMKI tahap pertama akan difokuskan pada aset-aset informasi kritis yang mendukung layanan inti perusahaan, yaitu:
   * **Kode Sumber (*Source Code*) dan Dokumentasi Proyek:** Aset utama untuk pengembangan perangkat lunak.
   * **Data Pribadi Klien dan Karyawan:** Sesuai dengan kebutuhan compliance terhadap regulasi perlindungan data pribadi.
   * **Infrastruktur TI Kritis:** Server pengembangan, server produksi, dan jaringan internal (*local area network*).
   * **Hak Kekayaan Intelelektual (HKI) dan Rahasia Dagang.**
3. **Proses Bisnis yang Dicakup:** Ruang lingkup proses bisnis meliputi:
   * Pengembangan Perangkat Lunak (*Software Development Life Cycle*).
   * Manajemen Hubungan dengan Klien.
   * Manajemen Sumber Daya Manusia (rekrutmen, onboarding, dan offboarding).
   * Manajemen Infrastruktur Teknologi Informasi.
4. **Standar yang Digunakan:** Kerangka kerja yang digunakan secara eksklusif adalah ISO/IEC 27001:2022, termasuk persyaratan klausul utama (4-10) dan kontrol keamanan pada Annex A. Referensi terhadap standar lain seperti ISO/IEC 27002 hanya sebagai panduan pelengkap.
5. **Tahapan:** Makalah ini akan membahas siklus lengkap implementasi SMKI berdasarkan model PDCA (*Plan-Do-Check-Act*), mulai dari tahap perencanaan hingga persiapan audit sertifikasi, dengan penekanan pada tahap *Plan* (Perencanaan) dan *Do* (Penerapan).

Dengan pembatasan ruang lingkup ini, diharapkan implementasi SMKI dapat berjalan lebih terarah, efektif, dan mencapai tujuan yang telah ditetapkan.

**BAB II   
PROFIL ORGANISASI**

Sebelum menganalisis dan merancang implementasi SMKI, penting untuk memahami organisasi yang menjadi objek studi. Bab ini akan menguraikan profil PT. Inovasi Tekknologi Indonesia (PT. ITI), mulai dari gambaran umum hingga aset informasi kritisnya, yang akan menjadi dasar bagi seluruh proses implementasi SMKI.

**2.1 Gambaran Umum**

**PT. Inovasi Teknologi Indonesia (PT. ITI)** adalah sebuah perusahaan nasional yang bergerak di bidang layanan teknologi informasi, khususnya pengembangan perangkat lunak (*software development*) dan konsultasi TI. Berdiri sejak 2018, PT. ITI telah tumbuh menjadi perusahaan dengan lebih dari 100 karyawan dan portofolio klien dari berbagai sektor, seperti perbankan, ritel, dan manufaktur.

Perusahaan beroperasi dari kantor pusatnya di Jakarta dan memiliki beberapa tim pengembang yang tersebar. Model bisnis PT. ITI meliputi:

* **Pengembangan Aplikasi Kustom:** Membangun aplikasi web dan mobile sesuai kebutuhan spesifik klien.
* **Sistem Integrasi:** Mengintegrasikan berbagai sistem yang sudah ada dalam organisasi klien.
* **Konsultasi Transformasi Digital:** Membantu klien merancang strategi digital untuk meningkatkan efisiensi dan layanan.

Dengan kompleksitas proyek dan sensitivitas data yang ditangani, keamanan informasi bukan hanya menjadi kebutuhan teknis, tetapi juga nilai jual dan kepercayaan bagi klien.

**2.2 Visi dan Misi**

**Visi:**  
"Menjadi mitra terdepan dalam menyediakan solusi teknologi informasi yang inovatif dan andal untuk mendukung kesuksesan digital bisnis klien."

**Misi:**

1. Memberikan layanan pengembangan perangkat lunak berkualitas tinggi dengan menggunakan teknologi terkini.
2. Membangun kemitraan jangka panjang dengan klien melalui pemahaman mendalam terhadap kebutuhan bisnis mereka.
3. Menciptakan lingkungan kerja yang kolaboratif dan mendukung pengembangan kompetensi karyawan secara berkelanjutan.
4. Menjaga kepercayaan klien dengan menjunjung tinggi integritas, kerahasiaan, dan keamanan data.

Dari visi dan misi tersebut, poin ke-4 secara eksplisit menekankan komitmen perusahaan terhadap keamanan informasi, yang sejalan dengan tujuan penerapan SMKI.

**2.3 Struktur Organisasi Divisi Teknologi Informasi (Divisi IT)**

Divisi TI di PT. ITI memegang peran sentral tidak hanya sebagai pendukung operasional internal, tetapi juga sebagai tulang punggung layanan kepada klien. Struktur organisasinya dirancang untuk mendukung kedua fungsi tersebut.

**(Gambar: Bagan Struktur Organisasi Divisi TI PT. ITI)**

* **Kepala Divisi TI:** Bertanggung jawab atas strategi, anggaran, dan kinerja seluruh divisi TI.
* **Tim Infrastruktur dan Jaringan:**
  + Mengelola dan memelihara server, jaringan, dan pusat data.
  + Menangankan keamanan perimeter (firewall, IPS/IDS).
  + Melakukan backup dan pemulihan bencana (*disaster recovery*).
* **Tim Pengembangan Aplikasi (Software Development):**
  + Merancang, mengembangkan, dan menguji aplikasi untuk klien.
  + Mengelola *source code* dan versi aplikasi (menggunakan Git).
* **Tim Keamanan Siber & Kepatuhan (InfoSec & Compliance):**
  + ***(Bagian yang akan sangat terlibat dalam implementasi SMKI)***
  + Memantau ancaman keamanan dan menangani insiden.
  + Mengembangkan dan menegakkan kebijakan keamanan informasi.
  + Memastikan kepatuhan terhadap standar dan regulasi (seperti ISO 27001).
* **Tim Helpdesk & Dukungan Pengguna:** Memberikan dukungan TI kepada seluruh karyawan PT. ITI.

**2.4 Fungsi dan Tanggung Jawab Divisi IT**

Fungsi utama Divisi TI adalah memastikan bahwa teknologi informasi menjadi pemacu dan pendukung yang efektif bagi tercapainya tujuan bisnis PT. ITI. Tanggung jawabnya meliputi:

* **Perencanaan Strategis TI:** Menyusun roadmap teknologi yang selaras dengan rencana bisnis perusahaan.
* **Pengembangan dan Pemeliharaan Aplikasi:** Membangun dan menjaga kualitas aplikasi yang dikembangkan untuk klien.
* **Manajemen Infrastruktur:** Memastikan ketersediaan, kinerja, dan keandalan seluruh infrastruktur TI.
* **Keamanan Informasi:** Melindungi aset informasi PT. ITI dan klien dari ancaman internal dan eksternal.
* **Dukungan Operasional:** Memastikan kelancaran operasional TI sehari-hari bagi semua karyawan.
* **Manajemen Risiko TI:** Mengidentifikasi, menilai, dan memitigasi risiko yang terkait dengan TI.

**2.5 Layanan Utama Divisi IT**

Layanan yang diberikan oleh Divisi TI dapat dikategorikan menjadi dua: layanan internal dan layanan eksternal (untuk klien).

* **Layanan Internal:**
  + Manajemen Jaringan dan Email Perusahaan.
  + Aplikasi Manajemen Proyek Internal (seperti Jira).
  + Sistem Kehadiran dan Penggajian (*Payroll*).
  + Helpdesk Support.
* **Layanan Eksternal (Kepada Klien):**
  + Pengembangan Aplikasi Web dan Mobile.
  + Hosting dan Manajemen Server Aplikasi Klien.
  + Layanan Konsultasi Keamanan Aplikasi.
  + Pemeliharaan dan Dukungan Aplikasi (*Application Maintenance & Support*).

**2.6 Aset Informasi Penting**

Berdasarkan analisis awal, berikut adalah aset informasi kritis PT. ITI yang menjadi fokus utama dalam implementasi SMKI:

1. **Aset Informasi:**
   * **Kode Sumber (*Source Code*):** Merupakan inti kekayaan intelektual dan produk perusahaan.
   * **Data Pribadi Klien & Karyawan:** Termasuk informasi identitas, kontak, dan data finansial.
   * **Dokumentasi Desain & Proyek:** Berisi spesifikasi teknis dan bisnis yang detail.
   * **Rahasia Dagang & Strategi Bisnis:** Informasi internal perusahaan dan rencana strategis.
2. **Aset Perangkat Lunak:**
   * *Software Development Kits* (SDK) dan lisensi perangkat lunak.
   * Aplikasi Manajemen Proyek (Jira, Confluence).
   * Sistem Manajemen Basis Data (MySQL, PostgreSQL).
3. **Aset Perangkat Keras:**
   * Server Pengembangan dan Produksi.
   * *Network Attached Storage* (NAS) untuk backup.
   * Perangkat Jaringan (Firewall, Switch, Router).
4. **Aset Manusia:**
   * Para *Software Developer*, *System Analyst*, dan *Security Specialist* yang memiliki pengetahuan dan keahlian kunci.
5. **Aset Layanan:**
   * Koneksi Internet dan Layanan Cloud (jika digunakan).

**2.7 Budaya dan Nilai Organisasi**

Budaya organisasi PT. ITI dicirikan oleh nilai-nilai berikut:

* **Inovasi:** Mendorong karyawan untuk terus belajar dan menerapkan teknologi baru.
* **Kolaborasi:** Tim kerja dibentuk secara lintas fungsi untuk menyelesaikan proyek.
* **Kualitas:** Memiliki komitmen untuk memberikan hasil kerja yang terbaik kepada klien.
* **Keterbukaan (*Transparency*):** Komunikasi yang terbuka antar karyawan dan dengan klien.

Namun, dari perspektif keamanan informasi, budaya "keterbukaan" dan "inovasi" ini terkadang dapat menimbulkan risiko, seperti kecenderungan untuk mencoba tool baru tanpa assessment keamanan yang memadai atau berbagi informasi secara berlebihan. Oleh karena itu, implementasi SMKI tidak hanya tentang menerapkan kontrol teknis, tetapi juga tentang **membentuk "Budaya Keamanan Informasi"** yang dapat berjalan seiring dengan nilai-nilai inti perusahaan yang sudah ada. SMKI akan membantu menanamkan kesadaran bahwa menjaga keamanan informasi adalah bagian dari tanggung jawab setiap individu dalam berinovasi dan berkolaborasi.