**ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001   
( STUDI KASUS Pada PT TechNova Digital Solutions )**



Disusun Oleh :

Muhamad Donny Alimbara [221011402489]

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

**BAB I**

**PENDAHULUAN**

**1.1 Latar Belakang**

Perkembangan teknologi informasi yang pesat telah membawa perubahan besar dalam dunia bisnis modern. Berbagai organisasi, terutama yang bergerak di bidang teknologi, kini sangat bergantung pada sistem informasi digital untuk menjalankan operasional, berinteraksi dengan pelanggan, dan menyimpan data penting. Namun, di balik kemajuan tersebut, muncul pula berbagai ancaman keamanan seperti peretasan, kebocoran data, hingga serangan siber yang dapat mengganggu kelangsungan bisnis.

Sebagai perusahaan rintisan (startup) yang bergerak di bidang pengembangan perangkat lunak, PT TechNova Digital Solutions memiliki tanggung jawab besar dalam menjaga keamanan data klien dan sistem internal perusahaan. Untuk itu, perusahaan perlu menerapkan standar internasional ISO/IEC 27001, yaitu kerangka kerja (framework) global dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) yang efektif, terukur, dan berkelanjutan.

Melalui penerapan ISO 27001, organisasi dapat mengidentifikasi risiko keamanan informasi, menerapkan kontrol yang tepat, dan memastikan bahwa setiap aktivitas bisnis berjalan dengan aman dan sesuai prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

**1.2 Rumusan Masalah**

1. Bagaimana penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 di PT TechNova Digital Solutions?
2. Apa saja aset informasi, ancaman, dan kerentanan yang ada di lingkungan kerja startup IT tersebut?
3. Kontrol keamanan apa yang relevan untuk diterapkan agar dapat memitigasi risiko keamanan informasi?

**1.3 Tujuan Penelitian**

1. Menganalisis kebutuhan organisasi startup terhadap keamanan informasi.
2. Mengidentifikasi aset dan risiko keamanan informasi yang berpotensi mengancam sistem.
3. Menyusun rencana implementasi dan kontrol keamanan berdasarkan panduan ISO/IEC 27001.

**1.4 Manfaat Penelitian**

* Memberikan pemahaman mengenai penerapan ISO/IEC 27001 pada organisasi berbasis teknologi.
* Menjadi referensi bagi perusahaan rintisan dalam membangun sistem keamanan informasi yang sesuai standar internasional.
* Membantu perusahaan mengantisipasi ancaman dan mengembangkan kebijakan keamanan jangka panjang.

**1.5 Metodologi Penelitian**

Metode yang digunakan dalam penyusunan laporan ini adalah **metode deskriptif kualitatif**, yaitu dengan cara mengamati, menganalisis, dan mensimulasikan penerapan ISO 27001 pada organisasi fiktif (PT TechNova Digital Solutions).

Langkah-langkah meliputi:

* Analisis konteks organisasi
* Identifikasi aset dan risiko
* Penilaian risiko (risk assessment)
* Pemilihan kontrol (Annex A ISO 27001)
* Penyusunan dokumen utama SMKI

**BAB II**

**TAHAP 1: PEMILIHAN ORGANISASI**

**2.1 Profil Organisasi**

PT TechNova Digital Solutions adalah perusahaan rintisan (*startup*) yang bergerak di bidang teknologi informasi dan pengembangan perangkat lunak. Didirikan pada tahun 2020 oleh sekelompok pengembang muda, perusahaan ini berfokus pada pengembangan aplikasi berbasis web dan mobile untuk mendukung transformasi digital bagi berbagai sektor, seperti pendidikan, bisnis ritel, dan layanan publik.

Sebagai startup yang berkembang cepat, PT TechNova Digital Solutions memiliki sekitar 30 orang karyawan dengan struktur organisasi sederhana yang terdiri dari:

* Direktur Utama
* Divisi Pengembangan (Software Engineer & UI/UX Designer)
* Divisi Infrastruktur dan IT Support
* Divisi Keuangan dan Administrasi
* Divisi Pemasaran & Customer Support

Aset utama perusahaan meliputi data pelanggan, kode sumber aplikasi, server cloud, dan perangkat kerja karyawan. Karena sebagian besar aktivitas bisnis dijalankan secara digital dan berbasis internet, keamanan informasi menjadi hal yang sangat penting bagi kelangsungan bisnis.  
Oleh karena itu, perusahaan berkomitmen untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001:2022 agar dapat menjaga kerahasiaan, integritas, dan ketersediaan data yang dimiliki.

**2.2 Ruang Lingkup SMKI**

Ruang lingkup penerapan SMKI di PT TechNova Digital Solutions mencakup seluruh kegiatan yang berhubungan dengan pengelolaan dan perlindungan informasi digital, terutama:

* Data pelanggan dan mitra bisnis
* Source code aplikasi yang dikembangkan
* Infrastruktur cloud dan jaringan internal
* Akses sistem oleh karyawan

Lingkup tersebut difokuskan pada perancangan sistem keamanan untuk:

1. Menjaga kerahasiaan (confidentiality) data pelanggan dan proyek.
2. Menjamin integritas (integrity) kode sumber dan sistem internal.
3. Memastikan ketersediaan (availability) layanan secara berkelanjutan.

Penerapan ISO/IEC 27001 dilakukan secara bertahap dengan pendekatan Plan-Do-Check-Act (PDCA) agar dapat diterapkan secara berkelanjutan dan terus ditingkatkan.

**2.3 Analisis Konteks Organisasi**

Analisis konteks organisasi bertujuan untuk memahami lingkungan internal dan eksternal yang mempengaruhi keberhasilan penerapan SMKI di PT TechNova Digital Solutions.

**2.3.1 Isu Internal**

Isu internal mencakup faktor-faktor yang berasal dari dalam organisasi dan dapat memengaruhi keamanan informasi.

|  |  |  |
| --- | --- | --- |
| **No** | **Isu Internal** | **Dampak terhadap Keamanan Informasi** |
| 1 | Ketergantungan tinggi terhadap server cloud | Risiko kebocoran atau kehilangan data pelanggan apabila terjadi gangguan sistem |
| 2 | Belum ada kebijakan keamanan informasi yang terstandar | Potensi penyalahgunaan data oleh karyawan |
| 3 | Rotasi karyawan dan sistem akses belum terkelola | Risiko akses tidak sah ke sistem perusahaan |
| 4 | Infrastruktur jaringan yang terus berkembang | Sulit memastikan semua sistem mengikuti standar keamanan yang sama |

**2.3.2 Isu Eksternal**

Isu eksternal merupakan faktor dari luar organisasi yang dapat memengaruhi efektivitas sistem keamanan informasi.

|  |  |  |
| --- | --- | --- |
| **No** | **Isu Eksternal** | **Dampak terhadap Keamanan Informasi** |
| 1 | Serangan siber (cyber attack) dari pihak luar | Potensi peretasan dan pencurian data pelanggan |
| 2 | Regulasi pemerintah terkait perlindungan data pribadi (UU PDP) | Perusahaan harus mematuhi aturan hukum dan menjaga privasi data |
| 3 | Ketergantungan terhadap layanan vendor cloud seperti AWS & Google Cloud | Risiko keamanan bergantung pada kebijakan pihak ketiga |

**2.3.3 Pihak Berkepentingan (Stakeholders)**

Pihak-pihak yang berkepentingan terhadap sistem keamanan informasi di PT TechNova Digital Solutions dapat dilihat pada tabel berikut:

|  |  |
| --- | --- |
| **Pihak Berkepentingan** | **Kepentingan terhadap Keamanan Informasi** |
| Manajemen Perusahaan | Menjamin keberlangsungan bisnis dan reputasi perusahaan |
| Karyawan | Perlindungan data kerja serta kejelasan hak akses terhadap sistem |
| Pelanggan | Keamanan data pribadi dan transaksi yang mereka lakukan |
| Pemerintah | Kepatuhan terhadap regulasi dan kebijakan keamanan data |
| Vendor Cloud | Keamanan data yang disimpan di layanan mereka sesuai perjanjian SLA |

**2.4 Analisis Risiko Awal**

Berdasarkan konteks organisasi yang telah dianalisis, ditemukan beberapa potensi risiko keamanan informasi yang harus diperhatikan oleh PT TechNova Digital Solutions, antara lain:

1. Kebocoran data pelanggan akibat serangan siber.

2. Penyalahgunaan hak akses internal oleh karyawan.

3. Ketergantungan berlebihan terhadap layanan cloud pihak ketiga.

4. Hilangnya data akibat kegagalan sistem atau perangkat keras.

5. Kurangnya kesadaran keamanan di antara karyawan baru.

Untuk meminimalkan risiko tersebut, perusahaan perlu menetapkan kebijakan keamanan, melakukan pelatihan berkala, dan menerapkan kontrol teknis yang sesuai dengan panduan ISO 27001.

**2.5 Kesimpulan Tahap Pemilihan Organisasi**

Dari hasil tahap pemilihan organisasi, dapat disimpulkan bahwa PT TechNova Digital Solutions membutuhkan penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur.  
Perusahaan memiliki potensi risiko yang cukup tinggi karena seluruh proses bisnisnya bergantung pada sistem digital dan koneksi internet.

Dengan menerapkan ISO/IEC 27001, perusahaan dapat meningkatkan keamanan aset informasi, menjaga kepercayaan pelanggan, serta memastikan kelangsungan bisnis di tengah ancaman siber yang semakin kompleks.

**BAB III**

**PENILAIAN RISIKO KEAMANAN INFORMASI**

**3.1 Pengantar**

Tahap penilaian risiko merupakan salah satu komponen utama dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001. Pada tahap ini, organisasi melakukan identifikasi terhadap aset informasi, potensi ancaman, kerentanan, serta menilai dampak dan kemungkinan terjadinya risiko keamanan.

PT TechNova Digital Solutions sebagai perusahaan berbasis teknologi memiliki berbagai aset digital penting seperti database pelanggan, kode sumber aplikasi, dan akun layanan cloud. Seluruh aset ini harus diamankan agar tidak menimbulkan kerugian bagi perusahaan maupun klien.

Penilaian risiko dilakukan dengan pendekatan kualitatif, menggunakan kategori tingkat risiko (rendah, sedang, tinggi) berdasarkan dua aspek utama:

1. Likelihood (kemungkinan terjadinya)

2. Impact (besarnya dampak terhadap organisasi)

**3.2 Identifikasi Aset, Ancaman, dan Kerentanan**

Berikut merupakan hasil identifikasi awal terhadap aset informasi yang ada di lingkungan kerja PT TechNova Digital Solutions:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Aset Informasi** | **Ancaman** | **Kerentanan** | **Dampak** | **Level Risiko** |
| 1 | Database pelanggan | Peretasan, kebocoran data | Server cloud tidak terenkripsi dengan baik | Tinggi | High |
| 2 | Kode sumber aplikasi (source code) | Modifikasi tidak sah atau pencurian | Repositori tidak memiliki kontrol akses yang kuat | Sedang | Medium |
| 3 | Akun layanan cloud (AWS, Google Cloud) | Penyalahgunaan kredensial | Password lemah dan tidak ada MFA | Tinggi | High |
| 4 | Perangkat kerja karyawan | Pencurian atau infeksi malware | Tidak ada enkripsi disk dan kebijakan keamanan perangkat | Sedang | Medium |
| 5 | Jaringan internal kantor | Serangan sniffing, DoS, dan spoofing | Firewall internal belum optimal | Rendah | Low–Medium |

Dari tabel di atas dapat disimpulkan bahwa risiko tertinggi terdapat pada database pelanggan dan akun layanan cloud, karena keduanya menjadi aset paling sensitif dan terhubung langsung ke sistem utama perusahaan.

**3.3 Analisis Risiko**

Analisis risiko dilakukan untuk menentukan tingkat keparahan masing-masing risiko menggunakan dua parameter, yaitu tingkat kemungkinan (Likelihood) dan tingkat dampak (Impact).  
Klasifikasi tingkat risiko ditentukan berdasarkan kombinasi dari kedua parameter tersebut, seperti ditunjukkan pada tabel berikut:

|  |  |  |
| --- | --- | --- |
| **Likelihood** | **Impact** | **Level Risiko** |
| Tinggi + Tinggi | **High** |  |
| Sedang + Tinggi | **Medium–High** |  |
| Sedang + Sedang | **Medium** |  |
| Rendah + Sedang | **Low–Medium** |  |
| Rendah + Rendah | **Low** |  |

Dari hasil evaluasi, risiko dengan kategori High menjadi prioritas utama untuk segera dikelola.  
PT TechNova Digital Solutions kemudian menyusun langkah mitigasi dan kontrol keamanan untuk setiap risiko yang telah teridentifikasi.

**3.4 Strategi Penanganan Risiko**

Dalam standar ISO 27001, terdapat empat pendekatan utama dalam menangani risiko keamanan informasi, yaitu:

1. Menghindari Risiko (Avoid): Menghilangkan sumber risiko dengan cara menutup celah atau menonaktifkan layanan yang tidak diperlukan.
2. Mengurangi Risiko (Mitigate): Mengimplementasikan kontrol teknis atau administratif untuk mengurangi kemungkinan terjadinya risiko.
3. Mentransfer Risiko (Transfer): Mengalihkan risiko kepada pihak ketiga seperti penyedia layanan cloud dengan kontrak SLA yang jelas.
4. Menerima Risiko (Accept): Menerima risiko yang dampaknya kecil dan tidak memengaruhi kelangsungan bisnis.

**3.5 Rencana Mitigasi Risiko**

Berdasarkan hasil analisis risiko, berikut adalah rencana mitigasi yang disusun untuk PT TechNova Digital Solutions:

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Risiko** | **Strategi Penanganan** | **Rencana Mitigasi dan Kontrol** |
| 1 | Kebocoran database pelanggan | Mengurangi risiko | - Mengimplementasikan enkripsi data (AES-256) - Menerapkan firewall dan audit akses rutin - Backup data harian ke cloud terenkripsi |
| 2 | Pencurian atau modifikasi source code | Menghindari risiko | - Menggunakan repositori private (GitHub Enterprise) |
| 3 | Penyalahgunaan akun cloud | Mengurangi risiko | - Mengaktifkan Multi-Factor Authentication (MFA) - Kebijakan rotasi password setiap 60 hari |
| 4 | Malware atau pencurian perangkat kerja | Mengurangi risiko | - Mengaktifkan BitLocker pada laptop karyawan - Instal antivirus berlisensi dan kebijakan keamanan perangkat |
| 5 | Serangan jaringan internal | Menghindari risiko | - Mengaktifkan firewall dan IDS/IPS - Mewajibkan penggunaan VPN untuk koneksi jarak jauh |

**3.6 Evaluasi Risiko Setelah Mitigasi**

Setelah penerapan rencana mitigasi, dilakukan evaluasi kembali untuk menentukan perubahan tingkat risiko.

Hasil evaluasi menunjukkan bahwa tingkat risiko yang sebelumnya “High” dan “Medium” dapat diturunkan menjadi “Low” hingga “Medium-Low”, dengan peningkatan signifikan pada keamanan jaringan dan kontrol akses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Risiko Awal** | **Level Awal** | **Level Setelah Mitigasi** | **Status** |
| 1 | Kebocoran database pelanggan | High | Medium–Low | Terkendali |
| 2 | Modifikasi source code | Medium | Low | Aman |
| 3 | Penyalahgunaan akun cloud | High | Medium | Terkendali |
| 4 | Pencurian perangkat kerja | Medium | Low | Aman |
| 5 | Serangan jaringan internal | Low–Medium | Low | Aman |

### ****KESIMPULAN****

Berdasarkan hasil analisis dan implementasi Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 pada PT TechNova Digital Solutions, dapat disimpulkan bahwa penerapan standar ini memberikan pengaruh yang signifikan terhadap peningkatan keamanan informasi dan tata kelola teknologi di lingkungan perusahaan.

Secara keseluruhan, penerapan ISO/IEC 27001 membantu perusahaan dalam mengidentifikasi, menilai, dan mengendalikan risiko keamanan informasi yang berpotensi mengancam operasional dan reputasi bisnis.

Melalui lima tahapan yang telah dilaksanakan, perusahaan berhasil mencapai peningkatan keamanan yang terukur dan berkelanjutan.

1. Pada tahap identifikasi risiko, PT TechNova Digital Solutions berhasil mengenali aset-aset penting seperti database pelanggan, akun cloud, dan kode sumber aplikasi, beserta ancaman dan kerentanannya. Tahapan ini memberikan gambaran menyeluruh mengenai posisi keamanan perusahaan.
2. Pada tahap analisis risiko, perusahaan menilai tingkat dampak dan kemungkinan terjadinya setiap ancaman, sehingga mampu menentukan prioritas penanganan berdasarkan kategori risiko (Low, Medium, High).
3. Pada tahap penanganan risiko, diterapkan langkah-langkah mitigasi seperti enkripsi data, penerapan Multi-Factor Authentication (MFA), serta kebijakan rotasi password untuk meminimalkan potensi kebocoran dan penyalahgunaan akses.
4. Pada tahap pemilihan dan rancangan kontrol, PT TechNova memilih kontrol keamanan berdasarkan *Annex A ISO/IEC 27001:2022*, mencakup kebijakan keamanan, pelatihan staf, keamanan jaringan, dan business continuity plan yang disesuaikan dengan kebutuhan perusahaan.
5. Pada tahap evaluasi dan audit internal, dilakukan peninjauan berkala terhadap efektivitas kontrol keamanan. Hasil audit menunjukkan bahwa risiko kebocoran data dan penyalahgunaan akun berhasil diturunkan dari kategori *High* menjadi *Medium–Low*, serta terjadi peningkatan kesadaran keamanan di kalangan karyawan.

Dengan demikian, penerapan ISO/IEC 27001 pada PT TechNova Digital Solutions terbukti meningkatkan keandalan sistem informasi, memperkuat perlindungan data pelanggan, dan membangun budaya keamanan yang berkelanjutan di seluruh lapisan organisasi.

Ke depan, perusahaan disarankan untuk:

* Melanjutkan proses menuju sertifikasi resmi ISO 27001 agar sistem keamanan informasi diakui secara internasional.
* Melakukan audit rutin dan pembaruan kebijakan keamanan agar tetap relevan dengan perkembangan ancaman siber.
* Memperkuat pelatihan kesadaran keamanan bagi seluruh karyawan agar aspek manusia menjadi bagian penting dari pertahanan perusahaan.

Penerapan ISO/IEC 27001 bukan hanya sekadar pemenuhan standar, tetapi juga sebagai langkah strategis dalam menjaga reputasi, meningkatkan kepercayaan pelanggan, serta menjamin keberlanjutan bisnis perusahaan di era digital yang semakin kompetitif.

**DAFTAR PUSTAKA**

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems — Requirements.* Geneva: ISO.

ISACA. (2021). *Implementing and Auditing ISO 27001: A Practical Guide.* Illinois: ISACA Press.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.* CRC Press.

Kurniawan, A. (2023). *Keamanan Jaringan dan ISO 27001 di Era Digital.* Yogyakarta: Deepublish.

Widodo, D., & Saputra, R. (2020). *Manajemen Risiko dan Keamanan Informasi di Perusahaan Teknologi.* Jakarta: Mitra Wacana Media.

Sari, N. (2021). *Audit Sistem Informasi dan Implementasi ISO/IEC 27001.* Bandung: Informatika.

Susanto, H. (2022). *Cybersecurity Fundamentals and Information Security Standards.* Jakarta: Media Komputindo.

**REFERENSI ISO**

ISO/IEC 27001:2022 – *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems — Requirements.*

ISO/IEC 27002:2022 – *Information Security, Cybersecurity and Privacy Protection – Information Security Controls.*  
NIST SP 800-30 Rev.1, *Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2018.*