**LAPORAN TAHAP 1–3**

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

**(Studi Kasus: PT. Panca Citra Sukses)**



Disusun Oleh:

Marchelina Annisa Assabrina

221011403197

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

# DAFTAR ISI

[DAFTAR ISI 2](#_Toc211784422)

[**1. PENDAHULUAN** 3](#_Toc211784423)

[1.1. Latar Belakang 3](#_Toc211784424)

[1.2. Batasan Masalah 4](#_Toc211784425)

[1.3. Tujuan 5](#_Toc211784426)

[1.4. Manfaat 5](#_Toc211784427)

[**2. ANALISI DAN HASIL** 5](#_Toc211784428)

[2.1 Tahap 1 – Pemilihan Organisasi Dan Ruang Lingkup Smki 5](#_Toc211784429)

[2.2 Tahap 2 – Analisis Konteks Organisasi 8](#_Toc211784430)

[2.3 Tahap 3 – Penilaian Risiko Keamanan Informasi 10](#_Toc211784431)

[**3. KESIMPULAN** 10](#_Toc211784432)

[DAFTAR PUSTAKA 12](#_Toc211784433)

## **PENDAHULUAN**

## **Latar Belakang**

Keamanan informasi telah menjadi pilar kritikal dalam menjamin kelangsungan operasional dan keunggulan kompetitif organisasi di era digital, di mana data merupakan aset yang tak ternilai. Peningkatan pesat dalam volume data dan kompleksitas ancaman siber menuntut perusahaan untuk tidak hanya bereaksi, tetapi juga proaktif dalam mengelola risiko keamanan. PT Panca Citra Sukses, sebagai entitas bisnis yang beroperasi dalam lanskap digital ini, menyadari betul pentingnya kerahasiaan, integritas, dan ketersediaan (K-I-K) data untuk menjaga kepercayaan pelanggan dan mematuhi regulasi yang berlaku. Oleh karena itu, penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur dan berdasarkan standar internasional menjadi suatu keharusan. Dokumen ini bertujuan untuk menyajikan simulasi penerapan awal ISO/IEC 27001:2022, standar global terkemuka untuk SMKI, dalam konteks operasional PT Panca Citra Sukses, berfokus pada tahapan fundamental yang krusial.

Penerapan ISO/IEC 27001:2022 memerlukan pendekatan sistematis untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi secara berkelanjutan, sebagaimana panduan dari ISO/IEC 27005:2018 tentang manajemen risiko. Langkah awal yang disimulasikan dalam laporan ini adalah identifikasi aset informasi PT Panca Citra Sukses. Tahapan ini sangat mendasar karena aset informasi seperti basis data pelanggan, desain produk, infrastruktur TI, dan informasi keuangan merupakan objek yang harus dilindungi. Penggunaan alat bantu seperti Eramba Community Edition, sebuah Open Source ISMS Tool, dapat memfasilitasi pendokumentasian dan kategorisasi aset-aset ini secara efisien, yang kemudian menjadi dasar yang kuat untuk analisis risiko yang akurat.

Setelah aset informasi teridentifikasi dan diklasifikasikan, tahapan selanjutnya yang disimulasikan adalah analisis risiko. Analisis ini esensial untuk memahami potensi kerugian yang mungkin timbul dari berbagai ancaman, mempertimbangkan kerentanan yang ada, dan menentukan tingkat risiko inheren. Simulasi ini mengadopsi prinsip-prinsip yang diuraikan dalam NIST Special Publication 800-30 Revision 1, yang memberikan panduan komprehensif untuk melakukan penilaian risiko, serta memanfaatkan templat penilaian risiko seperti yang disediakan oleh ISMS.online untuk memastikan konsistensi dan kelengkapan. Keluaran dari analisis risiko ini adalah penentuan risiko-risiko utama yang dihadapi PT Panca Citra Sukses. Berdasarkan identifikasi risiko, langkah terakhir yang diuraikan dalam pendahuluan ini adalah penentuan tindakan mitigasi awal. Tindakan ini merupakan respons terhadap risiko, bertujuan untuk mengurangi kemungkinan (probabilitas) atau dampak (konsekuensi) dari ancaman yang teridentifikasi. Dalam konteks laporan ini, fokus diberikan pada penentuan respons awal yang paling mendesak dan relevan untuk meningkatkan posisi keamanan informasi perusahaan secara cepat dan terukur.

## **Batasan Masalah**

Agar laporan ini fokus dan terarah, batasan masalah yang ditetapkan adalah:

1. Studi hanya dilakukan pada satu organisasi sebagai objek analisis, tidak mencakup seluruh organisasi di sektor lain.
2. Analisis konteks organisasi difokuskan pada aspek yang berhubungan langsung dengan keamanan informasi, tanpa membahas semua aspek operasional organisasi secara keseluruhan.
3. Penilaian risiko keamanan informasi hanya mencakup identifikasi dan evaluasi risiko serta rekomendasi pengendalian sesuai ISO/IEC 27001, tanpa melakukan implementasi penuh SMKI di organisasi.

## **Tujuan**

Tujuan dari laporan ini adalah untuk:

1. Memilih organisasi yang tepat sebagai objek studi untuk penerapan SMKI berdasarkan karakteristik dan kebutuhan keamanan informasi.
2. Menganalisis konteks internal dan eksternal organisasi untuk memahami faktor-faktor yang memengaruhi keamanan informasi.
3. Menilai risiko keamanan informasi guna mengidentifikasi ancaman dan menentukan langkah pengendalian sesuai ISO/IEC 27001.

## **Manfaat**

Berdasarkan tujuan laporan ini, manfaat yang diperoleh antara lain:

1. Membantu organisasi memahami konteks internal dan eksternal yang memengaruhi keamanan informasi sehingga dapat mengambil kebijakan yang tepat.
2. Menyediakan dasar dalam mengidentifikasi risiko keamanan informasi dan merancang langkah pengendalian yang sesuai dengan standar ISO/IEC 27001.
3. Meningkatkan kesadaran dan kesiapan organisasi dalam mengelola risiko keamanan informasi secara sistematis.

## **ANALISI DAN HASIL**

## **Tahap 1 – Pemilihan Organisasi Dan Ruang Lingkup Smki**

1. Profil Singkat Perusahaan

|  |  |  |
| --- | --- | --- |
| Nama Perusahaan | : | PT. Panca Citra Sukses |
| Bidang Usaha | : | Distribusi produk bahan bangunan |
| Tahun Berdiri | : | 2011 |
| Lokasi | : | BSD, Pagedangan |
| Gudang Cabang | : | Cisuka, Parung, dan Rangkas |

1. Visi dan Misi Perusahaan

Visi:

Menjadi pilihan utama pelanggan dan principal sebagai perusahaan distribusi bahan bangunan lokal dan internasional yang terpercaya, inovatif, dan berdaya saing tinggi.

Misi:

1. Melakukan inovasi berkelanjutan dalam budaya kerja dan layanan.
2. Mengembangkan SDM yang kompeten di bidang administrasi, logistik, dan penjualan.
3. Meningkatkan sarana dan prasarana guna menunjang efisiensi dan produktivitas.
4. Menyesuaikan sistem operasional dengan perkembangan teknologi.
5. Struktur Organisasi Singkat
6. CEO (Chief Executive Officer)

Berperan sebagai pengambil keputusan strategis dan pengawasan umum.

1. Divisi Operasional
2. Supervisor Sales
3. Admin Logistik
4. Kepala Gudang
5. Divisi Finance & Accounting
6. Account Receivable (AR)
7. Account Payable (AP)
8. Layanan Utama
9. Distribusi bahan bangunan dan kebutuhan industri
10. Pengelolaan stok dan logistik
11. Pengelolaan penagihan (piutang dan pembayaran)
12. Aset Informasi Penting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Jenis Aset Informasi** | **Deskripsi** | **Lokasi Penyimpanan** | **Kepemilikan** |
| 1 | Data Transaksi Pelanggan | Data pembelian dan pengiriman produk | Server internal & cloud | Finance & Sales |
| 2 | Data Stok Barang | Catatan inventori di tiap gudang | Sistem ERP & Ms. Excel | Logistik |
| 3 | Dokumen Keuangan | Data AP/AR, faktur, bukti transfer | Komputer Finance | Finance |
| 4 | Data Karyawan | Informasi pribadi dan gaji | File HR internal | HRD |
| 5 | Email dan Surat Menyurat | Komunikasi dengan pelanggan/vendor | Gmail korporat | Semua divisi |

Tabel 1 Aset Informasi Penting Perusahaan

1. Ruang Lingkup SMKI

Penerapan Sistem Manajemen Keamanan Informasi difokuskan pada Divisi Operasional dan Administrasi (Logistik, Sales, dan Finance & Accounting) yang mengelola:

1. Data transaksi penjualan dan pembelian.
2. Informasi pelanggan dan vendor.
3. Dokumen keuangan (invoice, faktur, bukti pembayaran).
4. Sistem administrasi berbasis komputer (Excel, email, sistem internal).

Hasil analisis terhadap konteks dan profil PT. Panca Citra Sukses menunjukkan ketergantungan operasional yang tinggi pada aset informasi tersebar, sehingga memvalidasi penetapan ruang lingkup SMKI yang difokuskan pada Divisi Operasional dan Administrasi, guna menjamin kerahasiaan data finansial dan integritas data logistik sebagai dukungan utama terhadap pencapaian tujuan strategis perusahaan.

## **Tahap 2 – Analisis Konteks Organisasi**

1. Isu Internal dan Eksternal

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Jenis Isu** | **Deskripsi** | **Dampak terhadap Keamanan Informasi** |
| 1 | Internal | Pengelolaan data keuangan masih manual pada beberapa bagian | Potensi human error dan kehilangan data |
| 2 | Belum adanya kebijakan keamanan informasi formal | Tidak ada standar penanganan insiden |
| 3 | Eksternal | Ancaman serangan siber dari luar (phishing/email) | Kebocoran data pelanggan |
| 4 | Ketergantungan pada koneksi internet untuk sistem ERP | Gangguan layanan jika terjadi downtime |
| 5 | Regulasi perlindungan data pribadi (UU PDP) | Risiko sanksi hukum jika tidak patuh |

Tabel 2 Isu Internal dan Eksternal

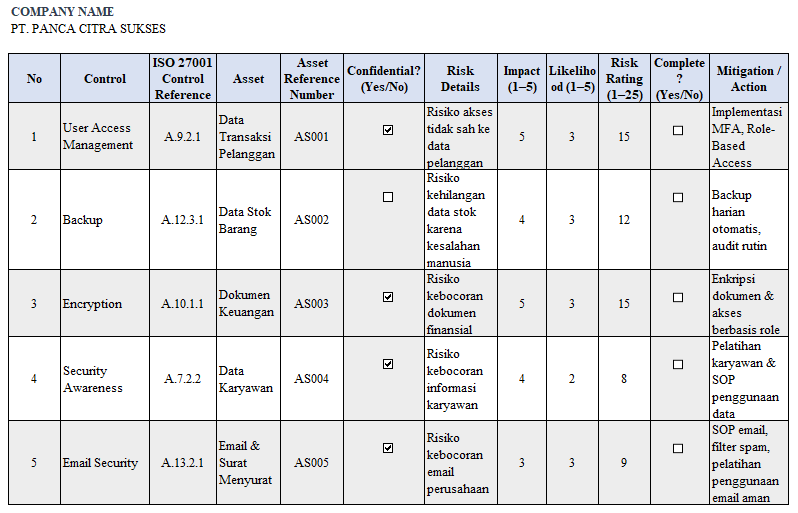
1. Pihak Berkepentingan (Stakeholder) dan Kebutuhan

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Pihak Berkepentingan** | **Kebutuhan Keamanan Informasi** | **Kepentingan** |
| 1 | Manajemen | Data laporan dan transaksi yang akurat, aman, dan selalu tersedia. | Pengambilan keputusan strategis. |
| 2 | Sales & Admin | Akses cepat ke data pelanggan tanpa gangguan sistem. | Operasional harian dan pelayanan pelanggan. |
| 3 | Pelanggan | Keamanan data pribadi dan transaksi. | Kepercayaan dan loyalitas pelanggan. |
| 4 | Vendor / Principal | Integritas dan kerahasiaan data order dan pembayaran. | Hubungan bisnis jangka panjang. |
| 5 | Bagian Finance | Kerahasiaan laporan keuangan dan dokumen tagihan. | Akurasi transaksi dan audit internal. |
| 6 | Regulator | Kepatuhan terhadap aturan perlindungan data. | Legalitas dan sertifikasi. |

Tabel 3 Pihak Berkepentingan

Analisis konteks organisasi menunjukkan bahwa kelemahan internal pada pengelolaan manual dan ketiadaan kebijakan keamanan formal secara kritis meningkatkan risiko kebocoran data pelanggan dan dokumen keuangan, yang diperburuk oleh ancaman eksternal pada serangan siber dan kepatuhan UU PDP. Oleh karena itu, hasilnya adalah prioritas mutlak untuk segera mengimplementasikan kontrol teknis yang kuat seperti MFA dan Enkripsi, serta menyusun kebijakan keamanan formal untuk memenuhi tuntutan Kerahasiaan, Integritas, dan Ketersediaan dari seluruh pihak berkepentingan (Manajemen, Pelanggan, dan Regulator).

## Tahap 3 – Penilaian Risiko Keamanan Informasi



Gambar 1 Tabel Penilaian Risiko Keamanan Informasi

🔹 Menggunakan Template Excel ISO 27001 Risk Assessment

Analisis dan hasil tahap ini menunjukkan bahwa dua risiko utama terkait keamanan informasi yaitu Akses Tidak Sah terhadap Data Pelanggan dan Kebocoran Dokumen Keuangan yang dikelompokkan dalam kategori kritis (Peringkat 15) berdasarkan metodologi Impact x Likelihood. Hasilnya adalah penetapan Rencana Perlakuan Risiko yang jelas, yang memprioritaskan penerapan kontrol mitigasi yang kuat, seperti Multi-Factor Authentication (MFA) dan Enkripsi Dokumen, yang harus segera diimplementasikan untuk menurunkan tingkat risiko ini ke batas yang dapat diterima.

## **KESIMPULAN**

**Simulasi penerapan SMKI ISO/IEC 27001:2022 pada PT. Panca Citra Sukses menegaskan bahwa keamanan informasi sangat penting untuk melindungi aset kritikal seperti data transaksi pelanggan, stok barang, dokumen keuangan, dan data karyawan. Pada Tahap 1 (Pemilihan Organisasi dan Ruang Lingkup SMKI), fokus pada penerapan yang ditetapkan pada Divisi Operasional dan Administrasi yang langsung mengelola aset informasi penting. Tahap 2 (Analisis Konteks Organisasi) mengidentifikasi isu internal, seperti kesalahan manusia dan belum adanya kebijakan formal, serta ancaman eksternal, termasuk serangan siber dan kepatuhan terhadap regulasi perlindungan data, sekaligus mempertimbangkan kebutuhan stakeholder terkait keamanan informasi. Tahap 3 (Penilaian Risiko) menunjukkan risiko utama terhadap aset yang harus diantisipasi, sehingga disarankan tindakan mitigasi awal untuk mengurangi kemungkinan dan dampak ancaman. Jadi, secara keseluruhan simulasi ini menekankan pentingnya pendekatan sistematis dalam mengelola risiko keamanan informasi, membangun dasar kebijakan dan prosedur sesuai standar ISO/IEC 27001, serta meningkatkan kesiapan organisasi dalam menjaga kepercayaan pelanggan dan kepatuhan regulasi.**

# DAFTAR PUSTAKA

Eramba Community Edition. (2024). Eramba Community Edition: Open Source ISMS Tool.

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2018). ISO/IEC 27005:2018: Information security risk management.

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

ISMS.online. (2023). ISO 27001 risk assessment template.

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (Special Publication 800-30 Revision 1). U.S. Department of Commerce.

Panca Citra Sukses. (n.d.). Panca Citra Sukses. Diakses pada 19 Oktober 2025, dari https://pancacitrasukses.co.id/