

**ANALISIS MANAJEMEN KEAMANAN SISTEM INFORMASI
MENGUNAKAN STANDAR ISO/IEC 27001 PADA PT SHOPEE
EXPRESS**



Disusun Oleh :
Raizka Hafidh Fadhilla
221011401906

**UNIVERSITAS PAMULANG
PROGRAM STUDY TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER**

Jl. Raya Puspiptek No. 46, Serpong, Kota Tangerang Selatan, Banten 15316.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, taufik, serta hidayah-Nya, sehingga penulis dapat menyelesaikan makalah dengan judul “Analisis Manajemen Keamanan Sistem Informasi Menggunakan Standar ISO/IEC 27001 pada PT Shopee Express” tepat pada waktunya. Makalah ini disusun untuk memenuhi salah satu tugas mata kuliah *Manajemen Keamanan Informasi* pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang.

Dalam penyusunan makalah ini, penulis berupaya memberikan gambaran menyeluruh mengenai penerapan sistem manajemen keamanan informasi berbasis standar internasional ISO/IEC 27001 pada perusahaan logistik digital. Penulis juga berusaha menganalisis pentingnya keamanan informasi dalam menunjang keberhasilan operasional serta menjaga kepercayaan pelanggan terhadap perusahaan.

Ucapan terima kasih penulis sampaikan kepada dosen pengampu yang telah memberikan bimbingan dan arahan selama proses penyusunan, serta kepada rekan-rekan mahasiswa yang turut memberikan masukan dan dukungan. Tidak lupa, penulis juga berterima kasih kepada pihak-pihak yang telah membantu dalam menyediakan data serta informasi yang diperlukan.

Penulis menyadari bahwa makalah ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan karya ilmiah ini di masa mendatang. Besar harapan penulis agar makalah ini dapat memberikan manfaat dan menambah wawasan pembaca, khususnya dalam memahami penerapan standar ISO/IEC 27001 di dunia industri logistik modern.

DAFTAR ISI

COVER.....	i
KATA PENGANTAR	ii
DAFTAR ISI.....	iii
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penulisan.....	2
1.4 Manfaat Penulisan	2
BAB II.....	4
2.1 Pengertian ISO/IEC 27001.....	4
2.2 Tujuan dan Manfaat ISO/IEC 27001	4
2.3 Prinsip Dasar Keamanan Informasi (CIA Triad)	5
2.4 Siklus PDCA (Plan–Do–Check–Act) dalam ISO/IEC 27001	6
2.5 Komponen Utama Sistem Manajemen Keamanan Informasi (SMKI)	7
2.6 Annex A ISO/IEC 27001:2022	7
2.7 Hubungan ISO/IEC 27001 dengan Standar Lain	8
BAB III	9
3.1 Profil Perusahaan.....	9
3.2 Analisis Konteks Organisasi	10
3.3 Identifikasi Aset Informasi.....	11
3.4 Analisis Risiko Keamanan Informasi.....	11
3.5 Penerapan Kontrol Keamanan Berdasarkan ISO/IEC 27001	12
3.6 Rencana Implementasi SMKI di PT Shopee Express	14
3.7 Tantangan dan Solusi Implementasi	15

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa perubahan besar dalam seluruh sektor bisnis, termasuk industri logistik. Proses pengiriman barang, pelacakan, dan manajemen data kini dilakukan secara digital menggunakan sistem informasi yang terhubung melalui jaringan internet. Transformasi digital ini menjadikan keamanan informasi sebagai aspek yang sangat penting, karena data yang dikelola bersifat sensitif dan bernilai tinggi.

Dalam konteks perusahaan logistik seperti PT Shopee Express, keamanan informasi tidak hanya mencakup perlindungan data pelanggan, tetapi juga mencakup keandalan sistem operasional, server, aplikasi pelacakan barang, dan jaringan komunikasi antar kantor cabang. Gangguan sekecil apa pun terhadap sistem informasi dapat berdampak pada keterlambatan pengiriman, kehilangan data, hingga menurunnya kepercayaan pelanggan terhadap layanan perusahaan.

Di era digital, ancaman terhadap informasi semakin kompleks. Serangan siber, pencurian data, penyalahgunaan akses oleh pihak internal, dan serangan malware menjadi risiko yang harus dikelola dengan baik. Berdasarkan survei yang dilakukan oleh Cybersecurity Ventures (2024), kerugian akibat kejahatan siber di sektor logistik global mencapai lebih dari 10 miliar dolar per tahun. Hal ini menunjukkan bahwa tanpa sistem manajemen keamanan informasi yang kuat, perusahaan akan rentan mengalami kerugian besar, baik secara finansial maupun reputasi.

Sebagai upaya untuk mengantisipasi risiko tersebut, diperlukan sebuah kerangka kerja yang mampu mengatur, mengontrol, dan mengevaluasi sistem keamanan informasi secara sistematis. Salah satu standar internasional yang diakui secara global untuk tujuan ini adalah ISO/IEC 27001. Standar ini memberikan pedoman dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) yang melibatkan kebijakan, prosedur, dan kontrol keamanan untuk melindungi data serta aset penting organisasi.

Penerapan ISO/IEC 27001 di PT Shopee Express sangat relevan mengingat perusahaan ini beroperasi secara digital dan melayani jutaan pelanggan di seluruh Indonesia. Dengan menerapkan SMKI berbasis ISO 27001, Shopee Express dapat memastikan bahwa semua informasi pelanggan, data transaksi, serta sistem operasional terlindungi dengan baik. Selain itu, penerapan ini juga dapat meningkatkan efisiensi internal, mengurangi potensi kesalahan manusia, serta membangun kepercayaan publik terhadap layanan pengiriman yang aman dan andal.

Pentingnya keamanan informasi juga terkait langsung dengan regulasi di Indonesia. Pemerintah melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa setiap organisasi yang mengelola data pribadi wajib menjaga kerahasiaan, integritas, dan ketersediaan data pengguna. Dengan demikian, penerapan ISO/IEC 27001 tidak hanya bersifat teknis, tetapi juga merupakan bentuk kepatuhan terhadap regulasi nasional.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apa yang dimaksud dengan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001?
2. Bagaimana penerapan ISO/IEC 27001 di PT Shopee Express dalam konteks operasional logistik digital?
3. Risiko keamanan informasi apa saja yang dihadapi oleh PT Shopee Express dan bagaimana cara mengelolanya?
4. Kontrol keamanan apa yang diterapkan berdasarkan Annex A ISO/IEC 27001 untuk mitigasi risiko?
5. Apa manfaat strategis yang diperoleh PT Shopee Express dari penerapan ISO 27001?

1.3 Tujuan Penulisan

1. Menjelaskan konsep dan prinsip dasar ISO/IEC 27001 serta kaitannya dengan sistem keamanan informasi.
2. Menganalisis penerapan SMKI di PT Shopee Express secara mendalam.
3. Mengidentifikasi risiko keamanan informasi dan aset penting yang perlu dilindungi.
4. Menentukan kontrol keamanan yang sesuai dengan Annex A ISO/IEC 27001:2022.
5. Memberikan rekomendasi strategis agar penerapan ISO 27001 di PT Shopee Express berjalan efektif dan berkelanjutan.

1.4 Manfaat Penulisan

Makalah ini diharapkan memberikan manfaat sebagai berikut:

Secara Akademik: Menjadi referensi pembelajaran mengenai penerapan standar keamanan informasi ISO/IEC 27001 di dunia industri logistik.

Secara Praktis: Memberikan gambaran bagi PT Shopee Express dalam membangun sistem keamanan informasi yang efektif dan efisien.

Secara Strategis: Meningkatkan kesadaran organisasi terhadap pentingnya perlindungan data pelanggan dan keamanan sistem digital.

Secara Regulatif: Menunjang kepatuhan terhadap peraturan pemerintah terkait perlindungan data pribadi dan keamanan siber nasional.

BAB II

KAJIAN TEORI

2.1 Pengertian ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional yang dirancang untuk membantu organisasi dalam menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (Information Security Management System / ISMS). Standar ini diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC).

ISO 27001 memberikan kerangka kerja sistematis untuk mengidentifikasi ancaman terhadap informasi, menilai tingkat risiko, dan menerapkan kontrol keamanan yang sesuai untuk melindungi informasi dari penyalahgunaan, kehilangan, atau kerusakan.

Standar ini bersifat fleksibel dan dapat diterapkan di berbagai jenis organisasi, baik sektor publik maupun swasta, termasuk perusahaan logistik seperti PT Shopee Express yang mengelola data pelanggan dalam jumlah besar. Tujuan utama ISO 27001 adalah memastikan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi—tiga aspek utama yang menjadi pondasi keamanan informasi.

Penerapan ISO/IEC 27001 juga memperkuat tata kelola organisasi. Dengan memiliki kebijakan keamanan yang terstruktur dan terdokumentasi, perusahaan dapat menunjukkan komitmen dalam menjaga keamanan data serta meningkatkan kepercayaan dari pelanggan, mitra bisnis, dan regulator.

2.2 Tujuan dan Manfaat ISO/IEC 27001

Tujuan penerapan ISO/IEC 27001 bukan hanya untuk mencegah ancaman keamanan siber, tetapi juga untuk menciptakan budaya keamanan informasi di dalam organisasi. Berikut beberapa tujuan dan manfaat penerapannya:

1. **Perlindungan Aset Informasi:** Menjamin bahwa semua aset digital seperti data pelanggan, sistem logistik, dan dokumen bisnis dilindungi dari kehilangan dan penyalahgunaan.
2. **Manajemen Risiko:** Membantu organisasi mengidentifikasi, menganalisis, dan mengendalikan risiko keamanan informasi secara sistematis.

3. Kepatuhan Regulasi: Memastikan perusahaan patuh terhadap undang-undang seperti UU Perlindungan Data Pribadi (UU PDP).
4. Peningkatan Kepercayaan Pelanggan: Pelanggan cenderung lebih percaya pada perusahaan yang memiliki sertifikasi ISO 27001 karena dianggap lebih profesional dan aman.
5. Efisiensi Operasional: Proses keamanan yang standar membantu mengurangi duplikasi pekerjaan dan meningkatkan efisiensi internal.
6. Keunggulan Kompetitif: Di dunia bisnis logistik, perusahaan dengan keamanan data yang kuat memiliki nilai tambah dibanding kompetitor.

2.3 Prinsip Dasar Keamanan Informasi (CIA Triad)

Kerangka ISO 27001 dibangun berdasarkan tiga prinsip utama keamanan informasi yang dikenal sebagai CIA Triad:

1. Confidentiality (Kerahasiaan)

Prinsip ini memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki izin atau otorisasi. Dalam konteks PT Shopee Express, data pelanggan seperti nama, alamat, dan nomor telepon harus terlindungi dari akses tidak sah. Mekanisme seperti Multi-Factor Authentication (MFA) dan enkripsi digunakan untuk menjamin kerahasiaan.

2. Integrity (Integritas)

Integritas informasi memastikan bahwa data yang tersimpan atau dikirim tidak diubah tanpa izin. Misalnya, data pelacakan pengiriman tidak boleh dimodifikasi oleh pihak eksternal yang ingin mengubah status pengiriman barang. Shopee Express menjaga integritas data melalui sistem logging, checksum, dan kontrol versi data.

3. Availability (Ketersediaan)

Prinsip ini menjamin bahwa sistem informasi selalu dapat diakses oleh pengguna yang berhak kapan pun dibutuhkan. Untuk Shopee Express, hal ini berarti aplikasi pelacakan dan server pengiriman harus beroperasi 24 jam. Penerapan redundant server, load balancing, dan disaster recovery plan menjadi langkah penting untuk menjaga ketersediaan sistem.

Ketiga prinsip ini saling berkaitan dan menjadi dasar seluruh kebijakan keamanan yang diterapkan dalam organisasi.

2.4 Siklus PDCA (Plan–Do–Check–Act) dalam ISO/IEC 27001

ISO 27001 menggunakan pendekatan Plan–Do–Check–Act (PDCA) sebagai kerangka kerja manajemen berkelanjutan. Siklus PDCA memastikan bahwa setiap proses keamanan informasi tidak hanya diterapkan tetapi juga terus dievaluasi dan diperbaiki.

Tahap	Deskripsi	Implementasi di PT Shopee Express
Plan (Perencanaan)	Menetapkan kebijakan keamanan, sasaran, proses, dan prosedur yang sesuai dengan tujuan organisasi	Membentuk tim keamanan informasi, menentukan ruang lingkup SMKI, dan mengidentifikasi aset serta risiko
Do (Pelaksanaan)	Menerapkan dan mengoperasikan kebijakan serta kontrol keamanan informasi.	Penerapan sistem autentikasi, enkripsi data, backup rutin, dan firewall jaringan.
Check(Pemeriksaan)	Memantau dan mengevaluasi efektivitas kontrol keamanan terhadap kebijakan yang ditetapkan.	Audit internal, peninjauan insiden, dan pemantauan log sistem.
Act (Tindakan)	Melakukan tindakan korektif dan perbaikan berkelanjutan untuk meningkatkan sistem keamanan.	Mengupdate kebijakan keamanan, memperbarui perangkat lunak, dan melatih karyawan.

Pendekatan PDCA membantu perusahaan menjaga siklus keamanan tetap hidup dan adaptif terhadap perubahan teknologi dan ancaman baru.

2.5 Komponen Utama Sistem Manajemen Keamanan Informasi (SMKI)

Penerapan ISO 27001 melibatkan beberapa komponen penting yang saling berhubungan. Berikut adalah komponen utama dalam implementasi SMKI:

1. Kebijakan Keamanan Informasi (Information Security Policy):

Merupakan dokumen utama yang menjelaskan komitmen manajemen terhadap keamanan informasi. Di Shopee Express, kebijakan ini disusun untuk mengatur seluruh kegiatan pengolahan data pelanggan dan operasional logistik digital.

2. Manajemen Risiko (Risk Management):

Proses identifikasi, penilaian, dan pengendalian risiko terhadap aset informasi. Hasil dari manajemen risiko menjadi dasar dalam penentuan kontrol keamanan yang diterapkan.

3. Kontrol Keamanan (Security Controls):

Langkah-langkah teknis dan administratif yang diambil untuk mengurangi risiko. Contohnya, penggunaan firewall, antivirus, sistem deteksi intrusi, dan pelatihan kesadaran keamanan bagi karyawan.

4. Audit Internal (Internal Audit):

Audit dilakukan secara berkala untuk memastikan bahwa sistem keamanan informasi berjalan sesuai kebijakan. Audit juga membantu menemukan celah keamanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab.

5. Tinjauan Manajemen (Management Review):

Evaluasi menyeluruh yang dilakukan oleh manajemen puncak untuk menilai kinerja SMKI dan menentukan langkah-langkah perbaikan.

6. Peningkatan Berkelanjutan (Continuous Improvement):

Proses berkelanjutan untuk memastikan SMKI tetap relevan dan efektif menghadapi ancaman baru yang terus berkembang.

2.6 Annex A ISO/IEC 27001:2022

Lampiran Annex A dalam ISO/IEC 27001:2022 berisi 93 kontrol keamanan informasi yang dikelompokkan dalam empat kategori besar:

Kategori	Jumlah Kontrol	Contoh Implementasi di Shopee Express
----------	----------------	---------------------------------------

A.5 – Organizational Controls	37 kontrol	Penetapan kebijakan keamanan, pengelolaan aset, tanggung jawab keamanan di tiap departemen.
A.6 – People Controls	8 kontrol	Pelatihan kesadaran keamanan, pemeriksaan latar belakang karyawan, pengendalian akses.
A.7 – Physical Controls	14 kontrol	Pengamanan ruang server, kamera pengawas (CCTV), sistem kartu akses.
A.8 – Technological Controls	34 kontrol	Enkripsi data, firewall, monitoring jaringan, sistem backup otomatis.

Shopee Express menggunakan kontrol dari keempat kategori ini untuk melindungi seluruh aspek operasionalnya, mulai dari sumber daya manusia hingga infrastruktur teknologi.

2.7 Hubungan ISO/IEC 27001 dengan Standar Lain

ISO/IEC 27001 memiliki keterkaitan erat dengan standar manajemen lainnya:

- ISO 9001 (Manajemen Mutu): Menjamin kualitas proses layanan.
- ISO 22301 (Manajemen Keberlanjutan Bisnis): Menjamin layanan tetap berjalan saat terjadi gangguan.
- ISO 20000 (Manajemen Layanan TI): Fokus pada tata kelola layanan teknologi informasi.

Integrasi antara ISO 27001 dan standar-standar tersebut menciptakan sistem manajemen yang holistik, efisien, dan terukur di Shopee Express.

BAB III

ANALISIS DAN IMPLEMENTASI SMKI PADA PT SHOPEE EXPRESS

3.1 Profil Perusahaan

PT Shopee Express merupakan anak perusahaan dari Shopee Indonesia yang bergerak di bidang logistik dan pengiriman barang. Didirikan pada tahun 2019, perusahaan ini berfokus pada layanan pengiriman cepat (express delivery) untuk mendukung ekosistem e-commerce Shopee. Dengan slogan “Cepat, Aman, dan Terpercaya”, Shopee Express memiliki jaringan distribusi yang tersebar di seluruh Indonesia.

Struktur organisasi PT Shopee Express terdiri dari beberapa divisi utama:

1. Divisi Operasional, bertanggung jawab terhadap proses pengiriman barang, gudang, dan armada transportasi.
2. Divisi Teknologi Informasi, mengelola sistem pelacakan (tracking system), aplikasi kurir, dan keamanan data pelanggan.
3. Divisi Keuangan dan Administrasi, menangani transaksi, laporan pengiriman, dan pembayaran.
4. Divisi Sumber Daya Manusia (SDM), mengelola pelatihan, rekrutmen, dan kebijakan internal.
5. Divisi Keamanan Informasi, bertugas memastikan perlindungan data pelanggan dan sistem TI.

Shopee Express memanfaatkan teknologi seperti cloud computing, big data analytics, dan Internet of Things (IoT) untuk memantau pengiriman barang secara real-time. Oleh karena itu, keberhasilan operasional sangat bergantung pada keamanan informasi dan keandalan sistem digital.

Tabel 3.1 Profil Perusahaan

Aspek	Keterangan
Nama Perusahaan	PT Shopee Express
Tahun Berdiri	2019
Kantor Pusat	Jakart Selatan, Indonesia
Sistem Utama	Aplikasi pelacakan (Shopee Express Tracking),

	system manajemen armada
Visi	Menjadi penyedia layanan logistic digital terdepan di Asia Tenggara

3.2 Analisis Konteks Organisasi

Analisis konteks organisasi bertujuan untuk memahami faktor internal dan eksternal yang mempengaruhi sistem manajemen keamanan informasi di Shopee Express.

Faktor Internal:

1. Infrastruktur TI yang kompleks dan terhubung ke platform Shopee.
2. Jumlah data pelanggan yang sangat besar dan terus bertambah.
3. Karyawan dengan tingkat kesadaran keamanan informasi yang bervariasi.
4. Ketergantungan tinggi terhadap sistem jaringan dan internet.

Faktor Eksternal:

1. Regulasi pemerintah mengenai keamanan data pribadi (UU PDP 2022).
2. Ancaman siber global seperti ransomware, phishing, dan DDoS attack.
3. Persaingan ketat dengan perusahaan logistik lain (J&T, Ninja Xpress, SiCepat).
4. Ekspektasi pelanggan terhadap kecepatan dan keamanan layanan.

Tabel 3.2 Analisis Konteks Organisasi

Aspek	Internal	Eksternal
Kekutan	Infrastruktur TI kuat, dukungan Shopee Group	Kepercayaan pelanggan tinggi
Kelemahan	Kesadaran keamanan karyawan rendah Regulasi	Peningkatan permintaan layanan e-commerce

	data pribadi semakin ketat Peluang Ekspansi jaringan dan teknologi baru	
Ancaman	Serangan siber dan kebocoran data	Kompetitor logistik dengan sistem AI dan cloud

3.3 Identifikasi Aset Informasi

Shopee Express memiliki berbagai aset informasi yang harus dilindungi agar operasional berjalan lancar. Aset ini dibagi menjadi tiga kategori: data digital, infrastruktur teknologi, dan sumber daya manusia.

Tabel 3.3 Aset informasi PT Shopee Express

No	Kategori	Jenis Aset	Kepemilikan	Nilai Kritis
1	Data	Data Pelanggan	Divisi IT	Tinggi
2	Data	Data transaksi	Divisi Operasional	Tinggi
3	Insfrastruktur	Server pusat dan backup	Divisi IT	Tinggi
4	Insfratruktur	Sistem jaringan Kantor cabang	Divisi IT	Sedang
5	SDM	Akses pengguna internal	Divisi SDM	Sedang
6	Aplikasi	Sistem pelacakan berbasis web dan mobile	Divisi TI	Tinggi
7	Perangkat	Laptop dan perangkat kurir	Divisi Operasional	Rendah

3.4 Analisis Risiko Keamanan Informasi

Setelah aset diidentifikasi, langkah berikutnya adalah menilai risiko yang mungkin terjadi. Risiko diukur berdasarkan kemungkinan (likelihood) dan dampak (impact) untuk menentukan tingkat prioritas mitigasi.

Tabel 3.4 Penilaian Risiko Keamanan Informasi

No	Aset	Ancaman	Dampak	Kemungkinan	Tingkat Risiko	Mitigasi
1	Data pelanggan	Pencurian data oleh pihak eksternal	Tinggi	Tinggi	Tinggi	Enkripsi dan firewall
2	Server pusat	Serangan DDoS dan gangguan - sistem	Tinggi	Sedang	Tinggi	IDS/IPS dan load-balancing
3	Data transaksi	Kesalahan input dan korupsi data	Sedang	Sedang	Sedang	Backup otomatis
4	Akses pengguna	Penyalahgunaan hak akses	Tinggi	Rendah	Tinggi	Sedang Multi-factor authentication
5	Jaringan kantor	Gangguan koneksi internet	Sedang	Tinggi	Tinggi	Redundansi jaringan dan VPN
6	Aplikasi tracking	Bug dan celah keamanan	Tinggi	Sedang	Tinggi	Pengujian patch dan patch rutin
7	Laptop kurir	Kehilangan perangkat	Rendah	Tinggi	Sedang	Enkripsi disk dan kunci otomatis

3.5 Penerapan Kontrol Keamanan Berdasarkan ISO/IEC 27001

Shopee Express menerapkan kontrol keamanan sesuai Annex A ISO/IEC 27001:2022 yang terdiri dari 93 kontrol dalam empat kategori utama. Beberapa kontrol utama yang diterapkan antara lain:

1. Kebijakan Keamanan Informasi: Dokumen resmi berisi aturan penggunaan data dan perangkat TI.
2. Manajemen Akses: Sistem autentikasi ganda (two-factor authentication) dan pengaturan hak akses berdasarkan peran (role-based access control).
3. Keamanan Fisik: Pengamanan ruang server dengan CCTV dan sistem kartu akses.

4. Manajemen Aset: Setiap perangkat dan sistem terdaftar dalam inventaris digital.
5. Pelatihan Keamanan: Program pelatihan keamanan untuk semua karyawan baru.
6. Keamanan Jaringan: Penggunaan firewall, IDS/IPS, dan enkripsi komunikasi data.
7. Backup dan Pemulihan: Sistem auto backup harian dan disaster recovery site.
8. Audit Internal: Evaluasi rutin untuk memastikan efektivitas kontrol.

Tabel 3.5 Daftar Kontrol Keamanan ISO/IEC 27001 di Shopee Express

No	Kategori	Contoh Kontrol	Status s
1	Organizational	Kebijakan keamanan & tata kelola risiko	Diterapkan
2	People	Pelatihan kesadaran keamanan	Berjalan
3	Physical	Pengamanan ruang server dan gudang	Diterapkan
4	Technological	Firewall, IDS/IPS, dan enkripsi data	Diterapkan
5	Compliance	Audit internal dan penilaian risiko tahunan	Terjadwal

3.6 Rencana Implementasi SMKI di PT Shopee Express

Shopee Express merencanakan implementasi ISO/IEC 27001 secara bertahap selama satu tahun penuh. Tahapan ini mencakup pembentukan tim, pelatihan, penilaian risiko, penerapan kontrol, hingga sertifikasi resmi.

Tabel 3.6 Rencana Implementasi SMKI

No	Aktivitas	Penanggung jawab	Waktu
1	Pembentukan Tim Keamanan Informasi	Manajer TI	Jan 2025
2	Identifikasi Aset dan Penilaian Risiko	Tim SMKI	Feb–Mar 2025
3	Penerapan Kontrol Keamanan	Divisi IT & Operasional	Apr–Jul 2025
4	Audit Internal dan Evaluasi	Auditor Internal	Ags 2025
5	Persiapan Sertifikasi ISO 27001	Manajemen Puncak	Sep 2025

3.7 Tantangan dan Solusi Implementasi

Dalam penerapan ISO 27001, Shopee Express menghadapi beberapa tantangan utama:

1. Kesadaran Karyawan: Tidak semua karyawan memahami pentingnya keamanan informasi.

Solusi: Pelatihan keamanan wajib dilakukan setiap 6 bulan sekali.

2. Skala Infrastruktur: Jaringan dan server yang luas mempersulit pengawasan.

Solusi: Menggunakan sistem monitoring terpusat berbasis cloud.

3. Biaya Implementasi: Sertifikasi dan perangkat keamanan memerlukan investasi besar.

Solusi: Penerapan bertahap berdasarkan prioritas risiko tertinggi.

4. Integrasi Sistem Lama: Beberapa sistem lama tidak kompatibel dengan kontrol baru.

Solusi: Migrasi bertahap ke infrastruktur modern dengan sandboxing.