LAPORAN
ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001 POINT 1 - 3

Dosen Pengampu: Bpk. Agung Perdananto, S.Kom, M.Kom

Disusun Oleh:

Nama	: Muhammad Fauzan Syahdan
NIM	: 221011402326
Kelas	: 07TPLM008
Mata Kuliah	: Keamanan Komputer

YAYASAN SASMITA JAYA
UNIVERSITAS PAMULANG
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA S-1

Jl. Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan Ujian Tengah Semester (UTS) dengan judul **"Analisis dan Implementasi Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO/IEC 27001 pada PT Volans Indonesia"** dengan baik dan tepat waktu.

Laporan ini disusun sebagai salah satu bentuk pemenuhan tugas mata kuliah yang membahas tentang **Standar Internasional Sistem Manajemen Keamanan Informasi (ISO/IEC 27001)**. Tujuan utama dari penyusunan laporan ini adalah untuk memberikan pemahaman yang lebih mendalam mengenai penerapan prinsip-prinsip manajemen keamanan informasi dalam suatu organisasi, baik nyata maupun fiktif. Selain itu, laporan ini juga diharapkan dapat menjadi referensi awal dalam membangun kesadaran pentingnya pengelolaan keamanan informasi secara sistematis dan berkelanjutan.

Dalam penyusunan laporan ini, penulis menggunakan pendekatan berbasis simulasi dengan memilih **PT Volans Indonesia**, sebuah perusahaan fiktif di bidang teknologi informasi, sebagai objek analisis. Melalui pendekatan ini, penulis berupaya menggambarkan bagaimana standar ISO/IEC 27001 dapat diimplementasikan dalam lingkungan organisasi yang bergerak di sektor IT, dengan mempertimbangkan aspek kontekstual, risiko keamanan informasi, serta kebutuhan para pemangku kepentingan.

Penulis menyadari bahwa dalam penyusunan laporan ini masih terdapat berbagai kekurangan, baik dari segi analisis maupun penyajian data, mengingat keterbatasan waktu dan sumber referensi. Namun, besar harapan penulis agar laporan ini tetap dapat memberikan manfaat bagi pembaca, khususnya bagi mahasiswa, praktisi keamanan informasi, serta pihak-pihak yang ingin memahami lebih jauh tentang penerapan **Sistem Manajemen Keamanan Informasi (SMKI)** berbasis ISO/IEC 27001.

Tangerang, 29 Oktober 2025

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar belakang

Keamanan informasi merupakan salah satu aspek krusial dalam menjaga keberlangsungan operasional organisasi di era digital. Ancaman terhadap kerahasiaan, integritas, dan ketersediaan data menimbulkan dampak signifikan, baik dari sisi finansial maupun reputasi. Oleh karena itu, penerapan **Sistem Manajemen Keamanan Informasi (SMKI)** berdasarkan standar **ISO/IEC 27001** menjadi langkah strategis bagi organisasi dalam membangun tata kelola keamanan informasi yang terukur dan berkelanjutan.

Laporan ini bertujuan untuk menganalisis dan merancang kerangka awal SMKI pada **PT Volans Indonesia,** yang berfokus pada tiga tahap utama, yaitu: pemilihan organisasi, analisis konteks organisasi, dan penilaian risiko keamanan informasi. Ketiga tahap ini menjadi dasar dalam perancangan sistem keamanan informasi yang efektif dan sesuai dengan prinsip ISO/IEC 27001.

Ruang lingkup analisis dalam laporan ini terbatas pada Divisi Teknologi Informasi (IT) PT Volans Indonesia, yang mengelola infrastruktur digital utama organisasi, termasuk server, sistem jaringan, dan basis data pelanggan. Divisi ini memiliki peran penting dalam memastikan bahwa seluruh sistem dan data yang digunakan oleh organisasi dapat berjalan secara aman, efisien, serta sesuai dengan kebijakan keamanan yang berlaku.

Di tengah meningkatnya ketergantungan organisasi terhadap teknologi digital, muncul pula beragam ancaman baru seperti serangan siber, kebocoran data, dan penyalahgunaan akses oleh pihak yang tidak berwenang. Ancaman-ancaman tersebut menuntut organisasi untuk memiliki sistem manajemen keamanan informasi yang tidak hanya reaktif, tetapi juga proaktif dalam mengidentifikasi dan mengendalikan risiko. ISO/IEC 27001 hadir sebagai standar internasional yang memberikan panduan sistematis dalam mengelola keamanan informasi melalui pendekatan berbasis risiko dan perbaikan berkelanjutan (*continual improvement*).

Selain itu, penerapan ISO/IEC 27001 juga dapat membantu organisasi dalam meningkatkan kepercayaan pelanggan dan mitra bisnis. Dengan adanya sistem yang terstandarisasi, organisasi dapat menunjukkan komitmen nyata terhadap perlindungan data dan pemenuhan regulasi, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Bagi PT Volans Indonesia, hal ini menjadi nilai tambah yang signifikan dalam memperkuat reputasi perusahaan di industri teknologi informasi yang sangat kompetitif.

Melalui laporan ini, diharapkan pembaca dapat memahami pentingnya penerapan standar keamanan informasi ISO/IEC 27001 serta proses analisis awal yang diperlukan dalam merancang sebuah Sistem Manajemen Keamanan Informasi (SMKI). Tahap-tahap yang dibahas dalam laporan ini akan menjadi dasar bagi pengembangan kontrol keamanan dan kebijakan informasi yang lebih komprehensif pada tahap berikutnya.

1.2 Maksud dan Tujuan

1. Menganalisis konteks organisasi PT Volans Indonesia, baik dari faktor internal maupun eksternal yang dapat memengaruhi keamanan informasi.
2. Mengindentifikasi aset informasi penting, ancaman, dan kerentanan yang ada dalam lingkungan organisasi.
3. Melakukan penilaian risiko keamanan informasi berdasarkan pendekatan kualitatif, untuk menentukan prioritas mitigasi terhadap risiko yang paling kritis.
4. Menyediakan dasar bagi perancangan SMKI pada tahap berikutnya, yaitu pemilihan kontrol keamanan dan penyusunan dokumen kebijakan sesuai standar ISO/IEC 27001.
5. Mendukung proses pembelajaran akademik, khususnya dalam memahami penerapan standar internasional di bidang manajemen keamanan informasi.

BAB II

PEMILIHAN ORGANISASI

2.1 Profil dan Alasan Pemilihan Organisasi

Organisasi yang menjadi objek analisis dalam laporan ini adalah **PT Volans Indonesia**, sebuah perusahaan fiktif yang bergerak di bidang teknologi informasi dan solusi digital. Perusahaan ini didirikan pada tahun 2018 dan berpusat di **Tangerang**, dengan visi menjadi penyedia layanan teknologi inovatif dan terpercaya di tingkat nasional. PT Volans Indonesia berkomitmen untuk memberikan solusi teknologi yang tidak hanya efisien dan modern, tetapi juga aman serta sesuai dengan standar industri yang berlaku.

Pemilihan PT Volans Indonesia sebagai objek simulasi didasarkan pada pertimbangan bahwa sektor teknologi informasi merupakan salah satu bidang yang paling rentan terhadap ancaman keamanan data. Perusahaan IT mengelola berbagai jenis aset informasi sensitif, mulai dari data pelanggan hingga sistem infrastruktur digital yang menjadi tulang punggung layanan bisnis. Oleh karena itu, penerapan **Sistem Manajemen Keamanan Informasi (SMKI)** berbasis **ISO/IEC 27001** sangat relevan untuk dianalisis sebagai langkah strategis dalam menjaga keberlangsungan operasional dan kepercayaan pelanggan.

Selain itu, perusahaan ini dipilih karena memiliki karakteristik yang menggambarkan realitas industri digital di Indonesia, di mana masih banyak organisasi yang mulai beralih ke sistem berbasis cloud dan layanan daring namun belum sepenuhnya menerapkan tata kelola keamanan informasi secara terstandarisasi. Dengan menjadikan PT Volans Indonesia sebagai studi kasus fiktif, penulis dapat melakukan simulasi penerapan prinsip-prinsip ISO/IEC 27001 secara lebih kontekstual, terukur, dan realistis.

2.2 Struktur Organisasi Singkat

Struktur organisasi merupakan elemen penting dalam menentukan tata kelola dan pembagian tanggung jawab di dalam perusahaan. Struktur yang baik akan mendukung efektivitas penerapan Sistem Manajemen Keamanan Informasi (SMKI)

karena setiap individu dan divisi memiliki peran yang jelas dalam menjaga keamanan data serta memastikan kelancaran operasional teknologi informasi.

Pada PT Volans Indonesia, struktur organisasi disusun secara fungsional, di mana pembagian tugas dilakukan berdasarkan bidang keahlian dan tanggung jawab masing-masing divisi. Model struktur ini dipilih agar koordinasi antarbagian dapat berjalan lebih efektif, serta memudahkan penerapan kebijakan keamanan informasi yang bersifat lintas-divisi.

Secara garis besar, struktur organisasi PT Volans Indonesia terdiri dari beberapa tingkatan dan unit kerja sebagai berikut:

1. **Direktur Utama**
   Bertanggung jawab penuh terhadap arah strategis dan pengambilan keputusan penting perusahaan. Direktur Utama juga berperan dalam mengesahkan kebijakan dan prosedur yang berkaitan dengan keamanan informasi.

2. **Divisi Teknologi Informasi (IT)**
   Divisi ini merupakan pusat operasional teknologi perusahaan. Tugas utamanya meliputi pengelolaan infrastruktur jaringan, pengembangan sistem aplikasi, pemeliharaan server, serta pengawasan terhadap keamanan data dan sistem. Divisi IT juga menjadi **ruang lingkup utama penerapan SMKI** berdasarkan ISO/IEC 27001.

3. **Divisi Keuangan**
   Bertanggung jawab atas pengelolaan keuangan, termasuk perencanaan anggaran, pelaporan keuangan, audit internal, serta pengawasan pengeluaran yang berkaitan dengan investasi perangkat dan sistem keamanan informasi.

4. **Divisi Sumber Daya Manusia (SDM)**
   Mengelola seluruh aspek terkait karyawan, mulai dari rekrutmen, pelatihan, hingga evaluasi kinerja. Dalam konteks keamanan informasi, divisi ini juga berperan penting dalam membangun **kesadaran keamanan (security awareness)** di kalangan karyawan.

5. **Divisi Pemasaran dan Layanan Pelanggan**
   Bertugas dalam promosi layanan, hubungan dengan pelanggan, dan penanganan keluhan. Divisi ini juga bertanggung jawab menjaga keamanan informasi pelanggan serta memastikan komunikasi data berjalan melalui saluran yang aman dan terenkripsi.

Struktur organisasi ini memungkinkan PT Volans Indonesia untuk menerapkan pengendalian keamanan informasi secara **terintegrasi** antara aspek teknis, administratif, dan sumber daya manusia. Dengan adanya pembagian peran yang jelas, setiap divisi dapat berkontribusi dalam mendukung kebijakan keamanan informasi yang sejalan dengan prinsip **Confidentiality (kerahasiaan)**, **Integrity (integritas)**, dan **Availability (ketersediaan)** sebagaimana diatur dalam standar **ISO/IEC 27001**.

2.3 Layanan Utama Perusahaan

Sebagai perusahaan yang bergerak di bidang teknologi informasi dan solusi digital, PT Volans Indonesia menawarkan berbagai layanan yang berfokus pada pengembangan sistem berbasis teknologi, manajemen infrastruktur IT, serta keamanan data digital. Layanan-layanan ini dikembangkan untuk menjawab kebutuhan pasar terhadap solusi teknologi yang efisien, adaptif, dan aman di tengah pesatnya transformasi digital.

PT Volans Indonesia berkomitmen untuk menjadi mitra strategis bagi klien dari berbagai sektor, seperti pemerintahan, pendidikan, perbankan, dan bisnis komersial. Setiap layanan yang diberikan tidak hanya berorientasi pada hasil teknologi yang inovatif, tetapi juga mengutamakan keamanan informasi, keandalan sistem, serta kepatuhan terhadap standar internasional, termasuk ISO/IEC 27001.

Adapun layanan utama yang disediakan oleh PT Volans Indonesia meliputi:

1. Pengembangan Aplikasi Berbasis Web dan Mobile
   PT Volans Indonesia menyediakan jasa pengembangan perangkat lunak (*software development*) untuk kebutuhan bisnis dan institusi. Layanan ini mencakup perancangan sistem, pengkodean, pengujian, dan pemeliharaan aplikasi berbasis web maupun mobile. Setiap proyek pengembangan dilakukan

dengan memperhatikan prinsip keamanan aplikasi, seperti penggunaan enkripsi data, kontrol akses, dan pengujian kerentanan sistem (*vulnerability testing*).

2. Layanan Cloud Hosting dan Manajemen Server

   Sebagai penyedia layanan cloud, PT Volans Indonesia menawarkan solusi penyimpanan dan pengelolaan data secara daring dengan tingkat keamanan tinggi. Infrastruktur cloud yang dimiliki perusahaan memungkinkan klien untuk mengakses data mereka kapan pun dan di mana pun dengan jaminan ketersediaan (*availability*) dan keandalan sistem (*reliability*). Pengamanan dilakukan dengan menerapkan sistem cadangan data (*backup system*), firewall berlapis, serta monitoring server secara real-time.

3. Konsultasi Keamanan Siber dan Infrastruktur IT

   PT Volans Indonesia juga memberikan layanan konsultasi bagi organisasi yang ingin memperkuat sistem keamanan informasinya. Layanan ini meliputi analisis risiko keamanan siber, audit sistem, serta penyusunan rekomendasi pengendalian keamanan yang sesuai dengan standar ISO/IEC 27001. Melalui layanan ini, perusahaan membantu klien untuk mencapai kepatuhan terhadap peraturan keamanan data serta meningkatkan kesiapan menghadapi ancaman digital.

4. Integrasi Sistem dan Dukungan Teknis (IT Support)

   Layanan ini berfokus pada integrasi berbagai sistem dan aplikasi agar dapat berfungsi secara terpadu di lingkungan organisasi klien. Selain itu, PT Volans Indonesia juga menyediakan layanan dukungan teknis dan pemeliharaan jaringan, yang bertujuan untuk memastikan sistem informasi selalu berjalan optimal dan terlindungi dari gangguan operasional maupun serangan eksternal.

5. Pelatihan dan Edukasi Keamanan Informasi

   Sebagai bentuk tanggung jawab profesional, PT Volans Indonesia juga menyelenggarakan pelatihan terkait kesadaran keamanan informasi (*security awareness training*) bagi karyawan dan klien. Program ini bertujuan untuk meningkatkan pemahaman mengenai pentingnya menjaga kerahasiaan data,

mengenali potensi ancaman siber, dan menerapkan praktik keamanan dasar dalam kegiatan operasional sehari-hari.

Dengan berbagai layanan tersebut, PT Volans Indonesia tidak hanya berperan sebagai penyedia solusi teknologi, tetapi juga sebagai mitra strategis dalam transformasi digital yang aman dan berkelanjutan. Setiap layanan dirancang untuk mengintegrasikan nilai inovasi dengan keamanan, sehingga dapat memberikan manfaat maksimal bagi pelanggan sekaligus menjaga reputasi perusahaan sebagai penyedia layanan IT yang profesional dan terpercaya.

2.4 Aset Informasi Penting

Dalam konteks penerapan Sistem Manajemen Keamanan Informasi (SMKI), aset informasi merupakan komponen utama yang harus diidentifikasi dan dilindungi. Aset informasi mencakup segala bentuk data, perangkat, dan sumber daya yang memiliki nilai bagi organisasi dan berkontribusi terhadap pencapaian tujuan bisnis. Pengelolaan aset informasi yang baik akan mempermudah proses identifikasi risiko serta penerapan kontrol keamanan yang sesuai dengan standar ISO/IEC 27001.

Bagi PT Volans Indonesia, sebagai perusahaan yang bergerak di bidang teknologi informasi, aset informasi tidak hanya berupa data digital, tetapi juga meliputi perangkat keras, perangkat lunak, infrastruktur jaringan, dan sumber daya manusia yang mengelola sistem tersebut. Aset-aset ini berperan penting dalam mendukung kegiatan operasional perusahaan, mulai dari pengembangan aplikasi, penyimpanan data pelanggan, hingga komunikasi internal antar pegawai.

Adapun aset informasi utama yang dimiliki PT Volans Indonesia dapat dikelompokkan sebagai berikut:

1. Aset Data dan Informasi Digital
    - Database Pelanggan: berisi informasi pribadi, data proyek, kontrak kerja, dan rekam jejak komunikasi dengan klien.

- Data Keuangan: mencakup laporan keuangan, penggajian, dan data transaksi bisnis yang bersifat rahasia.

- Dokumen Internal: meliputi kebijakan perusahaan, dokumen proyek, serta arsip administratif dan legalitas.

- Email Korporat: digunakan sebagai sarana komunikasi resmi antarpegawai dan dengan pihak eksternal.

2. Aset Teknologi dan Infrastruktur

    - Server Cloud Internal dan Eksternal: menyimpan data proyek serta mendukung layanan cloud hosting perusahaan.

    - Perangkat Jaringan (Router, Firewall, dan Switch): mengatur lalu lintas data dan menjadi lapisan utama dalam pertahanan keamanan jaringan.

    - Sistem Aplikasi dan Repositori Kode Sumber: mencakup perangkat lunak yang dikembangkan secara internal maupun untuk klien, termasuk *source code*, modul, dan dokumentasi teknis.

3. Aset Fisik dan Fasilitas Pendukung

    - Perangkat Komputer dan Laptop Karyawan: digunakan dalam aktivitas operasional dan pengembangan sistem.

    - Ruang Server (Data Center): lokasi penyimpanan utama perangkat server yang dilengkapi dengan sistem keamanan fisik seperti pengawasan CCTV dan kontrol akses.

    - Perangkat Penyimpanan Eksternal (Hard Drive dan Backup Storage): digunakan untuk pencadangan data penting dan pemulihan bencana (*disaster recovery*).

4. Aset Manusia (Human Assets)

    - Administrator Sistem dan Jaringan: bertanggung jawab terhadap pengelolaan keamanan sistem dan pemeliharaan infrastruktur IT.

    - Tim Developer: mengembangkan dan memelihara aplikasi perusahaan dengan memperhatikan standar keamanan kode.

    - Staf Keuangan dan HR: mengelola data sensitif terkait karyawan dan transaksi perusahaan.

    - Manajemen dan Pengambil Keputusan: menentukan arah kebijakan keamanan informasi dan pengendalian risiko organisasi.

Setiap aset tersebut memiliki tingkat kepentingan dan kerentanan yang berbeda. Oleh karena itu, dalam penerapan SMKI, PT Volans Indonesia perlu melakukan klasifikasi aset berdasarkan nilai dan tingkat sensitivitasnya terhadap bisnis. Klasifikasi ini akan mempermudah proses penilaian risiko (risk assessment) pada tahap selanjutnya, serta menjadi dasar dalam menentukan kontrol keamanan (security controls) yang sesuai dengan prinsip *confidentiality*, *integrity*, dan *availability*.

Dengan pengelolaan aset informasi yang sistematis, PT Volans Indonesia dapat memastikan bahwa setiap aset yang dimiliki tidak hanya mendukung kegiatan operasional perusahaan, tetapi juga terlindungi dari ancaman internal maupun eksternal yang dapat mengganggu stabilitas bisnis dan reputasi organisasi.

BAB III

ANALISIS KONTEKS ORGANISASI

3.1 Gambaran Umum Konteks Organisasi

Dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001, pemahaman terhadap konteks organisasi merupakan langkah awal yang penting. Analisis konteks membantu organisasi untuk mengidentifikasi berbagai faktor internal dan eksternal yang dapat memengaruhi kemampuan perusahaan dalam mencapai tujuan keamanan informasinya. Dengan memahami konteks ini, organisasi dapat menentukan ruang lingkup, kebijakan, dan strategi pengamanan yang paling relevan dan efektif.

Bagi PT Volans Indonesia, sebagai perusahaan yang beroperasi di bidang teknologi informasi, konteks organisasi memiliki pengaruh besar terhadap keberhasilan penerapan SMKI. Aktivitas bisnis yang melibatkan data pelanggan, layanan cloud, serta pengembangan aplikasi menuntut adanya tata kelola keamanan yang kuat dan konsisten. Oleh karena itu, pemetaan faktor internal, eksternal, serta kebutuhan para pemangku kepentingan menjadi dasar bagi penyusunan kebijakan keamanan informasi perusahaan.

3.2 Isu Internal dan Eksternal

Analisis terhadap isu internal dan eksternal bertujuan untuk mengidentifikasi berbagai kondisi yang dapat mendukung maupun menghambat penerapan keamanan informasi di PT Volans Indonesia.

Faktor-faktor ini meliputi kondisi organisasi, sumber daya, teknologi yang digunakan, hingga perubahan lingkungan eksternal seperti regulasi dan ancaman siber.

a. Isu Internal

No	Isu Internal	Deskripsi	Dampak terhadap Keamanan Informasi
1	Keterbatasan anggaran keamanan IT	Anggaran keamanan masih tergabung dalam anggaran operasional umum sehingga pembaruan perangkat keamanan tidak optimal	Meningkatkan risiko serangan terhadap infrastruktur jaringan
2	Kurangnya ketersadaran keamanan karyawan	Sebagian karyawan belum memahami pentingnya perlindungan data dan penggunaan password yang aman	Berpotensi terjadinya kebocoran data akibat human error
3	Ketergantungan tinggi terhadap sistem cloud	Sebagian besar layanan dan data pelanggan tersimpan di server cloud eksternal	Risiko gangguan kebocoran data apabila penyedia layanan cloud mengalami serangan
4	Prosedur keamanan belum terdokumentasi secara formal	Kebijakan keamanan masih bersifat informasi dan belum dilakukan	Menghambat penerapan kontrol keamanan yang konsisten
5	Kurangnya audit keamanan berkala	Evaluasi keamanan sistem belum dilakukan secara rutin	Menyulitkan deteksi dini terhadap kerentanan sistem

b. Isu Eksternal

No	Isu Eksternal	Deskripsi	Dampak Terhadap Kemanan Informasi
1	Meningkatnya ancaman siber global	Serangan seperti pishing, ramsomware, dan DDoS semakin sering terjadi pada perusahaan IT	Potensi kerugian besar dan gangguan layanan
2	Perubahan regulasi perlindungan data (UU PDP)	Adanya kewajiban kepatuhan terhadap peraturan baru tentang data pribadi	Diperlukan penyesuaian kebijakan dan prosedur internal

3	Persaingan industri IT yang ketat	Tekanan untuk berinovasi cepat dapat menyebabkan penurunan kontrol keamanan	Risiko pengabaian standar keamanan dalam pengembangan sistem
4	Ketergantungan terhadap pihak ketiga	Beberapa layanan masih bergantung pada vendor eksternal	Risiko kebocoran data jika mitra tidak memiliki sistem keamanan yang memadai
5	Perubahan teknologi yang cepat	Evolusi teknologi dapat menyebabkan sistem lama menjadi rentan	Diperlukan pembaruan berkelanjutan terhadap sistem keamanan

Analisis faktor-faktor di atas menunjukkan bahwa PT Volans Indonesia menghadapi tantangan baik dari sisi internal maupun eksternal. Oleh karena itu, diperlukan kebijakan dan strategi yang adaptif untuk menjaga keamanan informasi sekaligus mempertahankan keunggulan kompetitif perusahaan di sektor teknologi.

3.3 Pihak Berkepentingan (Stakeholder) dan Kebutuhan Kemanan Informasi

Identifikasi pihak berkepentingan (stakeholder) dilakukan untuk memahami siapa saja yang memiliki pengaruh atau kepentingan terhadap pengelolaan keamanan informasi di PT Volans Indonesia. Setiap stakeholder memiliki kebutuhan dan harapan yang berbeda, sehingga organisasi perlu memastikan bahwa sistem manajemen keamanan informasi dapat memenuhi seluruh kepentingan tersebut.

No	Stakeholder	Kebutuhan Keamanan Informasi	Dampak terhadap SMKI
1	Pelanggan	Perlindungan terhadap data pribadi, transaksi, dan proyek rahasia	Meningkatkan kepercayaan dan loyalitas pelanggan
2	Manajemen puncak (Direktur Utama)	Laporan keamanan yang akurat untuk pengambilan keputasan strategis	Menjadi dasar kebijakan dan invenstasi keamanan
3	Karyawan	Sistem kerja yang aman, stabil, dan	Menjamin

		mudah diakses	kenyamanan kerja dan produktivitas
4	Regulator dan pemerintah	Kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) dan regulasi TI	Menghindari sanksi hukum dan menjaga reputasi organisasi
5	Mitra Bisnis dan Vendor	Mekanisme komunikasi dan pertukaran data yang aman	Memastikan keberlanjutan kerja sama dan kepercayaan antarorganisasi
6	Tim Keamanan IT	Akses terhadap alat, kebijakan, dan dukungan manajemen untuk pengelolaan keamanan	Memastikan efektivitas pengawasan dan tanggapan terhadap insiden

Pemahaman terhadap kebutuhan para pemangku kepentingan ini sangat penting agar implementasi SMKI di PT Volans Indonesia tidak hanya memenuhi persyaratan teknis, tetapi juga selaras dengan harapan pihak internal dan eksternal. Dengan demikian, penerapan standar ISO/IEC 27001 dapat memberikan manfaat nyata dalam meningkatkan kepercayaan, efisiensi, serta kesiapan organisasi menghadapi ancaman keamanan informasi yang kompleks.

BAB IV

PENILAIAN RISIKO KEAMANAN INFORMASI

4.1 Gambaran Umum Penilaian Risiko

Penilaian risiko keamanan informasi merupakan salah satu tahap paling krusial dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001. Tujuan utama dari proses ini adalah untuk mengidentifikasi, menilai, dan memprioritaskan risiko yang dapat mempengaruhi kerahasiaan (*confidentiality*), integritas (*integrity*), serta ketersediaan (*availability*) informasi di lingkungan organisasi.

Bagi PT Volans Indonesia, kegiatan penilaian risiko dilakukan untuk memahami sejauh mana ancaman dan kerentanan yang mungkin timbul terhadap aset-aset informasi penting yang telah diidentifikasi sebelumnya. Proses ini juga berfungsi sebagai dasar dalam menentukan strategi mitigasi dan pengendalian keamanan (controls) yang akan digunakan pada tahap implementasi SMKI berikutnya.

Dalam laporan ini, metode penilaian risiko dilakukan secara kualitatif, yaitu dengan menilai tingkat dampak dan kemungkinan dari setiap ancaman berdasarkan skala rendah, sedang, dan tinggi. Hasil kombinasi kedua parameter tersebut menghasilkan tingkat risiko (risk level) yang menjadi prioritas penanganan.

4.2 Metodologi Penilaian Risiko

Penilaian risiko di PT Volans Indonesia dilakukan melalui beberapa tahapan berikut:

1. Identifikasi Aset Informasi
   Mengidentifikasi seluruh aset informasi penting yang mendukung proses bisnis perusahaan, termasuk data, perangkat keras, perangkat lunak, serta sumber daya manusia yang terlibat.

2. Identifikasi Ancaman dan Kerentanan

   Menentukan potensi ancaman (*threats*) yang dapat memengaruhi aset, serta kerentanan (*vulnerabilities*) yang dapat dimanfaatkan oleh ancaman tersebut.

3. Penilaian Dampak dan Kemungkinan

   Menilai seberapa besar dampak jika suatu ancaman terjadi, serta seberapa mungkin ancaman tersebut terealisasi.

4. Penentuan Level Risiko

   Menggabungkan hasil analisis dampak dan kemungkinan untuk menentukan tingkat risiko (tinggi, sedang, rendah).

5. Perumusan Tindakan Mitigasi

   Menyusun rekomendasi tindakan untuk mengurangi, mentransfer, atau menerima risiko sesuai tingkat prioritas.

4.3 Hasil Penilaian Risiko

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
1	Database Pelanggan	Serangan SQL Injection atau peretasan basis data	Sistem keamanan aplikasi belum diperbarui secara rutin	Tinggi	Sedang	Tinggi	Sistem keamanan aplikasi belum diperbarui secara rutin
2	Server Cloud Internal dan Eksternal	Serangan DDoS dan gangguan layanan	Kapasitas bandwidth dan proteksi masih terbatas	Tinggi	Rendah	Sedang	Menggunakan layanan *anti-DDoS*, load balancing, dan sistem pemantauan (*monitoring*) real-time
3	Email Korporat	Serangan phishing dan	Kurangnya kesadaran keamanan	Sedang	Tinggi	Tinggi	Menyelenggarakan pelatihan kesadaran

		malware	pada pengguna				keamanan (*security awareness training*) dan menerapkan *email filter system*
4	Repositori Kode Sumber (Source Code Repository)	Akses tidak sah oleh pihak internal atau eksternal	Pengelolaan hak akses belum optimal	Tinggi	Sedang	Tinggi	Menerapkan autentikasi multi-faktor (*multi-factor authentication*) dan kontrol akses berbasis peran (*role-based access control*)
5	Data Keuangan dan Laporan Audit	Pencurian atau kebocoran data akibat malware	Perangkat keamanan endpoint belum diperbarui	Tinggi	Sedang	Tinggi	Penerapan *endpoint protection*, enkripsi file, dan audit akses berkala
6	Perangkat Komputer dan Laptop Karyawan	Kehikangan atau pencurian perangkat	Tidak semua perangkat memiliki enkripsi disk	Sedang	Sedang	Sedang	Mengaktifkan enkripsi perangkat (*disk encryption*) dan kebijakan penggunaan perangkat pribadi (*BYOD policy*)
7	Jaringan Internal Perusahaan	Akses tidak sah melalui jaringan Wi-Fi	Password jaringan tidak diganti secara berkala	Sedang	Sedang	Sedang	Menggunakan autentikasi WPA3 dan penggantian sandi jaringan secara rutin
8	Backup Data Eksternal	Kerusakan atau kehilangan media penyimpanan	Tidak adanya lokasi penyimpanan cadangan terpisah	Tinggi	Rendah	Sedang	Menyediakan lokasi penyimpanan backup off-site dan melakukan uji pemulihan data secara berkala

4.4 Analisis dan Interpretasi Risiko

Hasil penilaian menunjukkan bahwa sebagian besar risiko pada PT Volans Indonesia berada pada kategori **sedang hingga tinggi**, terutama yang berkaitan dengan **data pelanggan**, **repositori kode sumber**, dan **email korporat**. Risiko-risiko tersebut memiliki potensi dampak besar terhadap reputasi dan keberlangsungan layanan perusahaan apabila tidak ditangani secara tepat.

Faktor dominan penyebab tingginya risiko antara lain adalah kurangnya kesadaran keamanan informasi di kalangan karyawan, keterbatasan dalam pembaruan sistem keamanan, serta belum adanya kebijakan formal yang mengatur tata kelola keamanan informasi.

Oleh karena itu, PT Volans Indonesia perlu melakukan langkah-langkah strategis, antara lain:

- Membentuk **tim keamanan informasi (Information Security Team)** yang bertugas melakukan monitoring dan audit berkala.

- Menetapkan **kebijakan keamanan informasi (Information Security Policy)** secara resmi dan terintegrasi antar-divisi.

- Menyelenggarakan **pelatihan keamanan siber** secara periodik bagi seluruh karyawan.

- Mengimplementasikan **kontrol teknis** sesuai rekomendasi *Annex A ISO/IEC 27001:2022* pada tahap implementasi selanjutnya.

4.5 Kesimpulan Sementara Tahap Penilaian Risiko

Dari hasil analisis risiko yang dilakukan, dapat disimpulkan bahwa PT Volans Indonesia memiliki tingkat risiko yang cukup tinggi terhadap ancaman keamanan informasi, terutama pada aset digital utama yang berhubungan langsung dengan

layanan kepada pelanggan. Penerapan pengendalian yang tepat sangat dibutuhkan agar organisasi dapat menurunkan tingkat risiko ke level yang dapat diterima.

Penilaian risiko ini juga menjadi dasar bagi perancangan **kebijakan dan kontrol keamanan informasi** yang akan dibahas pada tahap selanjutnya (Tahap 4), yaitu pemilihan dan penerapan kontrol keamanan dari *Annex A ISO/IEC 27001:2022*.

Dengan pemahaman yang jelas mengenai risiko yang dihadapi, PT Volans Indonesia dapat menyusun strategi perlindungan data yang komprehensif, efisien, dan berkelanjutan guna menjaga kepercayaan pelanggan serta meningkatkan kesiapan organisasi dalam menghadapi tantangan keamanan informasi di masa mendatang.

BAB V

PENUTUP

Berdasarkan hasil analisis yang telah dilakukan terhadap penerapan awal Sistem Manajemen Keamanan Informasi (SMKI) di PT Volans Indonesia, dapat disimpulkan bahwa organisasi ini memiliki kesadaran yang cukup baik terhadap pentingnya keamanan informasi, namun masih terdapat sejumlah aspek yang perlu diperkuat agar sejalan dengan standar ISO/IEC 27001:2022.

Tahapan pertama hingga ketiga yang telah dibahas menunjukkan bahwa PT Volans Indonesia memiliki infrastruktur dan aset informasi yang kompleks, mencakup database pelanggan, server cloud, repositori kode sumber, serta sistem komunikasi internal. Aset-aset tersebut memiliki nilai strategis yang tinggi bagi keberlangsungan bisnis perusahaan.

Melalui analisis konteks organisasi (Tahap 2), ditemukan bahwa faktor internal seperti keterbatasan anggaran, kurangnya kesadaran keamanan karyawan, serta belum adanya dokumentasi kebijakan formal menjadi tantangan utama bagi perusahaan. Di sisi lain, faktor eksternal seperti peningkatan serangan siber global dan perubahan regulasi perlindungan data juga memberikan tekanan tambahan yang harus diantisipasi.

Sementara itu, hasil penilaian risiko (Tahap 3) menunjukkan bahwa beberapa aset memiliki tingkat risiko tinggi, terutama yang terkait dengan data pelanggan, email korporat, dan repositori kode sumber. Ancaman seperti serangan siber, kebocoran data, dan akses tidak sah menjadi risiko dominan yang perlu ditangani melalui kontrol keamanan yang terukur dan berkelanjutan.

Secara keseluruhan, analisis ini memberikan gambaran bahwa penerapan SMKI di PT Volans Indonesia masih berada pada tahap awal, namun memiliki potensi besar untuk dikembangkan menjadi sistem keamanan informasi yang matang dan sesuai standar internasional. Langkah-langkah awal yang dilakukan dalam laporan ini akan menjadi fondasi penting bagi penyusunan kebijakan, tujuan, dan kontrol keamanan pada tahap implementasi berikutnya.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2023). *Panduan Implementasi ISO/IEC 27001 di Lingkungan Pemerintahan dan Industri*. Jakarta: Direktorat Keamanan Siber dan Sandi Pemerintahan.

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

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2020). *Information Security Management Systems: Understanding ISO 27001 and ISO 27002*. Boca Raton: CRC Press.

Tanuwijaya, H. (2021). *Manajemen Keamanan Informasi: Penerapan ISO/IEC 27001 di Dunia Industri*. Yogyakarta: Deepublish.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Boston: Cengage Learning.

Wicaksono, A. (2022). *Keamanan Siber dan Perlindungan Data Pribadi di Era Digital*. Jakarta: Mitra Wacana Media.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang *Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 200.