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

**MATA KULIAH :**



Disusun Oleh:

Anugrah Ageng Prasetyo 221011401510

Muhammad Ihsan 221011401786

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

Daftar isi

[BAB I PENDAHULUAN 4](#_Toc212558354)

[1.1 Latar Belakang 4](#_Toc212558355)

[1.2 Tujuan 5](#_Toc212558356)

[1.3 Ruang Lingkup 5](#_Toc212558357)

[BAB II PROFIL ORGANISASI ( Tahap 1) 7](#_Toc212558358)

[2.1 Gambaran Umum 7](#_Toc212558359)

[2.2 Visi dan Misi 7](#_Toc212558360)

[2.3 Struktur Organisasi Divisi Teknologi Informasi (Divisi IT) 8](#_Toc212558361)

[2.4 Fungsi dan Tanggung Jawab Divisi IT 9](#_Toc212558362)

[2.5 Layanan Utama Divisi IT 9](#_Toc212558363)

[2.6 Aset Informasi Penting 10](#_Toc212558364)

[2.7 Budaya dan Nilai Organisasi 11](#_Toc212558365)

[BAB III 12](#_Toc212558366)

[ANALISIS KONTEKS ORGANISASI ( Tahap 2 ) 12](#_Toc212558367)

[3.1 Pendahuluan 12](#_Toc212558368)

[3.2 Konteks Internal Organisasi 12](#_Toc212558369)

[3.3 Konteks Eksternal Organisasi 14](#_Toc212558370)

[3.4 Pihak Berkepentingan (Stakeholder) dan Kebutuhan Keamanan Informasi 16](#_Toc212558371)

[3.5 Analisis Hasil Konteks Organisasi 17](#_Toc212558372)

[BAB IV 19](#_Toc212558373)

[PENILAIAN RISIKO KEAMANAN INFORMASI 19](#_Toc212558374)

[4.1 Identifikasi Aset Informasi, Ancaman, dan Kerentanan 19](#_Toc212558375)

[4.1.1 Aset Informasi Utama 19](#_Toc212558376)

[4.1.2 Identifikasi Ancaman 20](#_Toc212558377)

[4.1.3 Identifikasi Kerentanan 20](#_Toc212558378)

[4.1.4 Tabel Identifikasi Aset, Ancaman, dan Kerentanan 21](#_Toc212558379)

[4.2 Analisis Risiko Keamanan Informasi 21](#_Toc212558380)

[4.2.1 Kriteria Penilaian Risiko 21](#_Toc212558381)

[4.2.2 Matriks Penentuan Level Risiko 22](#_Toc212558382)

[4.2.3 Hasil Analisis Risiko 22](#_Toc212558383)

[4.2.4 Analisis Hasil dan Interpretasi 23](#_Toc212558384)

[4.3 Evaluasi dan Prioritas Risiko 24](#_Toc212558385)

[4.3.1 Tujuan Evaluasi Risiko 24](#_Toc212558386)

[4.3.2 Hasil Evaluasi Risiko 24](#_Toc212558387)

[4.3.3 Analisis Prioritas dan Pengambilan Keputusan 25](#_Toc212558388)

[4.4 Rencana Tindakan Mitigasi Risiko 26](#_Toc212558389)

[4.4.1 Tujuan Mitigasi Risiko 26](#_Toc212558390)

[4.4.2 Strategi Pengendalian Risiko 26](#_Toc212558391)

[4.4.3 Rencana Mitigasi Risiko PT. ITI 27](#_Toc212558392)

[4.4.4 Monitoring dan Tinjauan Berkala 28](#_Toc212558393)

# PENDAHULUAN

## 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.

## 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.

## 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.

# PROFIL ORGANISASI ( Tahap 1)

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.

## **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.

## **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.

## **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.

## **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.

## **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*).

## **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).

## **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.

# 

# ANALISIS KONTEKS ORGANISASI ( Tahap 2 )

## Pendahuluan

Analisis konteks organisasi merupakan tahap penting dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001:2022. Tahapan ini bertujuan untuk memahami berbagai faktor internal dan eksternal yang dapat memengaruhi kemampuan organisasi dalam menetapkan, menerapkan, memelihara, serta meningkatkan efektivitas SMKI. Melalui analisis konteks, organisasi dapat mengidentifikasi kondisi lingkungan operasionalnya, tantangan keamanan yang dihadapi, serta ekspektasi pihak-pihak berkepentingan terhadap keamanan informasi.

Bagi PT. Inovasi Teknologi Indonesia (PT. ITI), analisis konteks organisasi menjadi langkah awal dalam memastikan bahwa setiap kebijakan dan kontrol keamanan informasi yang diterapkan benar-benar relevan dengan kebutuhan bisnis dan risiko yang dihadapi. PT. ITI sebagai perusahaan yang bergerak di bidang pengembangan perangkat lunak dan layanan konsultasi teknologi informasi memiliki ketergantungan tinggi terhadap sistem informasi, data klien, serta infrastruktur TI yang kompleks. Oleh karena itu, pemahaman menyeluruh terhadap konteks organisasi sangat penting untuk menentukan ruang lingkup SMKI dan prioritas pengamanan yang tepat.

Dalam bab ini, akan diuraikan hasil identifikasi faktor internal dan eksternal yang berpengaruh terhadap keamanan informasi di PT. ITI, serta pihak-pihak berkepentingan (stakeholder) yang memiliki kepentingan terhadap perlindungan aset informasi perusahaan. Analisis ini akan menjadi dasar dalam penentuan strategi implementasi dan penilaian risiko keamanan informasi yang akan dibahas pada bab selanjutnya.

## Konteks Internal Organisasi

Konteks internal organisasi mencakup seluruh faktor di dalam perusahaan yang dapat memengaruhi penerapan dan efektivitas Sistem Manajemen Keamanan Informasi (SMKI). Faktor-faktor ini meliputi struktur organisasi, budaya kerja, sumber daya manusia, proses bisnis, serta kebijakan dan infrastruktur teknologi yang dimiliki. Pemahaman terhadap konteks internal membantu organisasi dalam menilai kesiapan serta menentukan kontrol keamanan yang sesuai dengan kondisi aktual.

**PT. Inovasi Teknologi Indonesia (PT. ITI)** memiliki struktur organisasi yang cukup terpusat pada **Divisi Teknologi Informasi (Divisi IT)**, yang terdiri dari beberapa tim utama seperti Infrastruktur dan Jaringan, Pengembangan Aplikasi, Keamanan Siber & Kepatuhan, serta Helpdesk. Divisi ini memegang peran vital dalam pengelolaan seluruh aset informasi, baik yang digunakan secara internal maupun untuk layanan kepada klien. Struktur organisasi ini menunjukkan bahwa pengelolaan keamanan informasi sebagian besar bergantung pada kebijakan dan praktik yang dijalankan di dalam divisi tersebut.

Dari sisi **budaya organisasi**, PT. ITI menjunjung nilai inovasi, kolaborasi, dan keterbukaan dalam bekerja. Nilai-nilai ini mendukung produktivitas dan kreativitas, namun juga dapat menimbulkan potensi risiko apabila tidak diimbangi dengan kesadaran terhadap keamanan informasi. Misalnya, kecenderungan karyawan untuk mencoba teknologi baru tanpa prosedur penilaian keamanan dapat membuka peluang terhadap kerentanan sistem.

Dalam hal **sumber daya manusia**, sebagian besar karyawan Divisi IT memiliki kompetensi teknis yang baik, namun belum seluruhnya memiliki pemahaman mendalam mengenai kebijakan dan prosedur keamanan informasi. Kondisi ini menunjukkan perlunya peningkatan **awareness** dan **pelatihan keamanan** secara berkala agar seluruh personel memahami tanggung jawabnya dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi.

Sementara dari aspek **teknologi dan infrastruktur**, PT. ITI telah menggunakan berbagai sistem pendukung seperti server internal, layanan cloud, sistem manajemen proyek (Jira, Confluence), serta repositori kode (Git). Namun, masih terdapat beberapa kelemahan seperti dokumentasi keamanan yang belum lengkap, backup data yang belum sepenuhnya terotomatisasi, dan kontrol akses yang belum terstandarisasi di seluruh proyek. Hal ini menunjukkan bahwa implementasi SMKI perlu diarahkan pada penguatan pengelolaan aset dan pengendalian akses terhadap data penting.

Untuk menggambarkan kondisi tersebut secara ringkas, berikut tabel analisis konteks internal PT. ITI:

|  |  |  |
| --- | --- | --- |
| **Faktor Internal** | **Deskripsi** | **Dampak terhadap Keamanan Informasi** |
| Struktur Organisasi | Divisi IT terdiri dari tim pengembang, infrastruktur, keamanan, dan helpdesk | Menunjang fokus keamanan, tetapi koordinasi antar tim perlu diperkuat |
| Budaya Kerja | Inovatif, kolaboratif, dan terbuka | Mendorong produktivitas, namun berpotensi membuka risiko kebocoran informasi |
| Sumber Daya Manusia | SDM kompeten secara teknis, kesadaran keamanan masih bervariasi | Perlu peningkatan pelatihan dan sosialisasi SMKI |
| Infrastruktur TI | Server internal, repositori kode, sistem cloud | Membutuhkan kebijakan akses, enkripsi, dan backup teratur |
| Kebijakan dan Prosedur | Belum ada dokumen formal terkait SMKI | Menyulitkan konsistensi penerapan kontrol keamanan |
| Aset Informasi | Source code, data klien, dan dokumentasi proyek | Membutuhkan prioritas perlindungan dan manajemen akses ketat |

## Konteks Eksternal Organisasi

Konteks eksternal organisasi mencakup faktor-faktor di luar perusahaan yang dapat memengaruhi penerapan dan efektivitas **Sistem Manajemen Keamanan Informasi (SMKI)**. Faktor-faktor ini berasal dari lingkungan industri, regulasi, teknologi, hingga kondisi sosial dan ekonomi yang memengaruhi cara organisasi dalam melindungi aset informasinya. Dengan memahami konteks eksternal, PT. Inovasi Teknologi Indonesia (PT. ITI) dapat menyesuaikan kebijakan dan kontrol keamanan informasinya agar tetap relevan dan adaptif terhadap perubahan lingkungan.

Sebagai perusahaan yang bergerak di bidang **pengembangan perangkat lunak dan konsultasi teknologi informasi**, PT. ITI beroperasi di industri dengan tingkat persaingan dan risiko siber yang tinggi. Ancaman seperti **serangan ransomware**, **phishing**, dan **kebocoran data** klien menjadi tantangan nyata yang dihadapi oleh banyak perusahaan TI, termasuk PT. ITI. Selain itu, tuntutan dari klien untuk menjaga **kerahasiaan kode sumber (source code)** dan data proyek semakin meningkat seiring dengan kesadaran publik terhadap keamanan data.

Dari sisi **regulasi**, PT. ITI juga harus memperhatikan **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)** yang mewajibkan organisasi untuk mengelola data pribadi dengan prinsip keamanan, transparansi, dan akuntabilitas. Selain itu, penerapan standar internasional seperti **ISO/IEC 27001:2022** juga menjadi bentuk kepatuhan terhadap praktik terbaik (best practice) dalam tata kelola keamanan informasi yang diakui secara global. Regulasi ini menuntut organisasi untuk memiliki sistem keamanan informasi yang terdokumentasi dan dapat diaudit.

Faktor eksternal lainnya berasal dari **perkembangan teknologi informasi** yang sangat cepat. Adopsi teknologi cloud computing, remote working, serta penggunaan aplikasi pihak ketiga meningkatkan efisiensi kerja, tetapi juga menambah potensi risiko kebocoran atau kehilangan data jika tidak dikelola dengan baik. Oleh karena itu, PT. ITI perlu menerapkan pendekatan keamanan berbasis risiko agar tetap sejalan dengan perubahan teknologi dan pola kerja modern.

Selain itu, **harapan pelanggan (customer trust)** menjadi faktor penting dalam konteks eksternal. Klien dari sektor perbankan, ritel, maupun manufaktur yang bekerja sama dengan PT. ITI umumnya menuntut jaminan keamanan terhadap data proyek mereka. Reputasi perusahaan dalam menjaga keamanan informasi dapat menjadi nilai tambah yang signifikan dalam menjaga loyalitas klien dan menarik kerja sama baru.

Untuk merangkum faktor-faktor eksternal tersebut, berikut tabel analisis konteks eksternal PT. ITI:

|  |  |  |
| --- | --- | --- |
| **Faktor Eksternal** | **Deskripsi** | **Dampak terhadap Keamanan Informasi** |
| Lingkungan Industri | Sektor teknologi dengan tingkat ancaman siber tinggi | Menuntut penerapan kontrol keamanan proaktif |
| Regulasi dan Kepatuhan | UU PDP 2022 dan standar ISO/IEC 27001:2022 | Mewajibkan tata kelola keamanan data yang terstruktur |
| Harapan Klien | Klien menuntut jaminan keamanan data proyek | Meningkatkan kebutuhan sertifikasi dan audit keamanan |
| Perkembangan Teknologi | Penggunaan cloud, remote access, dan integrasi sistem | Memerlukan kontrol akses dan monitoring yang ketat |
| Persaingan Pasar | Banyak perusahaan TI berlomba menunjukkan kepatuhan keamanan | SMKI menjadi faktor keunggulan kompetitif |
| Ancaman Siber Global | Ransomware, phishing, social engineering | Memerlukan sistem deteksi dini dan mitigasi risiko |

## Pihak Berkepentingan (Stakeholder) dan Kebutuhan Keamanan Informasi

Dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI), penting bagi organisasi untuk mengidentifikasi pihak-pihak yang memiliki kepentingan terhadap sistem tersebut, baik secara langsung maupun tidak langsung. Pihak-pihak ini disebut stakeholder, yaitu individu, kelompok, atau entitas yang memiliki pengaruh, kepentingan, atau ekspektasi terhadap kinerja keamanan informasi organisasi.

Analisis stakeholder membantu PT. Inovasi Teknologi Indonesia (PT. ITI) dalam memahami kebutuhan dan harapan mereka, sehingga kebijakan serta kontrol keamanan yang diterapkan dapat disesuaikan dengan tujuan bisnis dan kepatuhan terhadap standar yang berlaku.

Sebagai perusahaan pengembang perangkat lunak dan penyedia layanan konsultasi TI, PT. ITI memiliki berbagai pihak berkepentingan yang terlibat dalam proses bisnisnya, mulai dari manajemen, karyawan, klien, hingga regulator dan penyedia layanan eksternal. Setiap stakeholder memiliki peran dan tanggung jawab yang berbeda dalam menjaga keamanan informasi perusahaan.

Berikut ini adalah identifikasi pihak-pihak berkepentingan utama di PT. ITI beserta kebutuhan mereka terhadap keamanan informasi:

|  |  |  |
| --- | --- | --- |
| **Stakeholder** | **Peran dalam Organisasi** | **Kebutuhan terhadap Keamanan Informasi** |
| **Manajemen Puncak** | Pengambil keputusan strategis dan penanggung jawab utama SMKI | Memastikan efektivitas sistem keamanan, kepatuhan terhadap regulasi, dan perlindungan reputasi perusahaan |
| **Divisi Teknologi Informasi (IT)** | Mengelola infrastruktur TI, pengembangan aplikasi, serta pengamanan sistem | Memerlukan kebijakan dan kontrol teknis yang jelas untuk melindungi data dan aset digital |
| **Tim Keamanan Siber & Kepatuhan (InfoSec)** | Menangani insiden keamanan, audit, dan pemantauan risiko | Memerlukan dukungan manajemen dan sumber daya untuk implementasi serta monitoring kontrol keamanan |
| **Karyawan** | Pengguna sistem informasi dalam kegiatan operasional sehari-hari | Membutuhkan panduan, pelatihan, dan kesadaran keamanan untuk mencegah human error |
| **Klien / Pelanggan** | Pengguna layanan dan pemilik data proyek yang dikelola PT. ITI | Menuntut jaminan kerahasiaan, integritas, dan ketersediaan data proyek mereka |
| **Regulator / Pemerintah** | Mengatur dan mengawasi kepatuhan terhadap UU Perlindungan Data Pribadi | Menuntut perusahaan untuk mematuhi regulasi keamanan data dan pelaporan insiden |
| **Penyedia Layanan Eksternal (Vendor / Cloud Provider)** | Mendukung operasional TI seperti hosting, penyimpanan data, dan backup | Diharuskan mematuhi standar keamanan dan perjanjian kerahasiaan (NDA) |
| **Masyarakat / Publik** | Pihak yang menilai reputasi perusahaan dari sisi keamanan dan kepercayaan | Mengharapkan transparansi dan tanggung jawab perusahaan dalam menjaga data pribadi |

## Analisis Hasil Konteks Organisasi

Berdasarkan hasil identifikasi terhadap faktor **internal**, **eksternal**, serta **pihak berkepentingan (stakeholder)**, dapat disimpulkan bahwa PT. Inovasi Teknologi Indonesia (PT. ITI) memiliki kondisi organisasi yang cukup matang secara teknis namun masih membutuhkan penguatan pada aspek kebijakan, kesadaran, dan tata kelola keamanan informasi. Analisis konteks ini memberikan gambaran menyeluruh mengenai posisi perusahaan dalam kaitannya dengan penerapan **Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001:2022.**

Dari sisi konteks internal, kekuatan utama PT. ITI terletak pada struktur organisasi Divisi Teknologi Informasi yang sudah jelas, didukung oleh sumber daya manusia dengan kemampuan teknis tinggi. Namun, masih ditemukan beberapa kelemahan, seperti belum adanya kebijakan keamanan formal, kurangnya dokumentasi prosedur pengamanan, serta belum meratanya kesadaran keamanan informasi di antara seluruh karyawan. Aspek budaya organisasi yang menekankan inovasi dan keterbukaan juga perlu diarahkan agar tetap sejalan dengan prinsip keamanan informasi tanpa menghambat kreativitas.

Sementara itu, dari sisi konteks eksternal, PT. ITI beroperasi di industri yang sangat dinamis dan kompetitif, dengan risiko serangan siber yang terus berkembang. Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) menuntut perusahaan untuk memperkuat mekanisme pengamanan data dan memastikan kepatuhan terhadap prinsip transparansi serta akuntabilitas. Selain itu, meningkatnya kesadaran pelanggan terhadap keamanan data menjadi tekanan tambahan bagi PT. ITI untuk menunjukkan komitmen dan bukti nyata penerapan standar keamanan internasional.

Hasil analisis stakeholder menunjukkan bahwa seluruh pihak yang terlibat memiliki peran penting dalam keberhasilan implementasi SMKI. Manajemen puncak memegang tanggung jawab strategis untuk memastikan ketersediaan sumber daya dan arah kebijakan, sementara Divisi IT dan Tim Keamanan Siber menjadi pelaksana teknis yang memastikan seluruh kontrol berjalan efektif. Dukungan dari karyawan, vendor, dan klien juga berpengaruh besar terhadap keberlanjutan sistem keamanan informasi.

Dengan mempertimbangkan seluruh faktor tersebut, dapat disimpulkan bahwa penerapan SMKI di PT. ITI perlu difokuskan pada beberapa aspek prioritas berikut:

1. **Pembentukan dan dokumentasi kebijakan keamanan informasi** yang sesuai dengan konteks organisasi.
2. **Peningkatan kesadaran dan pelatihan keamanan informasi** bagi seluruh karyawan.
3. **Penerapan kontrol teknis dan prosedural** untuk mengurangi risiko kebocoran data dan serangan siber.
4. **Pemenuhan kepatuhan terhadap regulasi keamanan data**, khususnya UU PDP.
5. **Peningkatan kolaborasi antar tim dan stakeholder** dalam pelaksanaan serta evaluasi SMKI.

# 

# PENILAIAN RISIKO KEAMANAN INFORMASI

## Identifikasi Aset Informasi, Ancaman, dan Kerentanan

Penilaian risiko keamanan informasi merupakan tahapan penting dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001:2022. Tujuannya adalah untuk mengidentifikasi aset informasi yang kritis, menilai potensi ancaman serta kerentanan yang dapat memengaruhi aset tersebut, dan memberikan dasar bagi proses analisis serta mitigasi risiko di tahap selanjutnya.

Pada PT. Inovasi Teknologi Indonesia (PT. ITI), aset informasi memiliki peran strategis karena menjadi tulang punggung bagi seluruh proses bisnis, terutama dalam pengembangan perangkat lunak, penyimpanan data klien, serta manajemen infrastruktur TI. Oleh karena itu, identifikasi aset informasi dilakukan secara sistematis untuk memastikan seluruh aset yang bernilai tinggi dapat dilindungi secara optimal.

### Aset Informasi Utama

Berdasarkan hasil analisis pada tahap sebelumnya, aset informasi utama yang menjadi fokus penilaian risiko di PT. ITI meliputi:

1. **Kode Sumber (Source Code)** – Produk utama dan kekayaan intelektual perusahaan yang berisi logika bisnis, algoritma, dan konfigurasi sistem.
2. **Data Klien dan Data Karyawan** – Informasi sensitif yang mencakup data pribadi, finansial, dan operasional.
3. **Dokumentasi Proyek dan Desain Teknis** – Berisi detail spesifikasi sistem, arsitektur perangkat lunak, serta rencana proyek.
4. **Infrastruktur TI (Server, Jaringan, dan Penyimpanan Data)** – Mendukung operasional dan hosting aplikasi internal maupun klien.
5. **Akun dan Kredensial Sistem (User Access)** – Termasuk hak akses ke repositori kode, sistem cloud, dan database.
6. **Hak Kekayaan Intelektual (HKI) dan Strategi Bisnis Internal** – Informasi strategis yang mendukung daya saing perusahaan.

### Identifikasi Ancaman

Ancaman merupakan setiap potensi kejadian yang dapat menyebabkan kerusakan, kehilangan, atau penyalahgunaan terhadap aset informasi. Ancaman yang teridentifikasi pada PT. ITI antara lain:

* **Serangan Siber** seperti *phishing*, *ransomware*, *brute force*, dan *SQL injection* terhadap server aplikasi.
* **Kebocoran Data (Data Leakage)** akibat kesalahan konfigurasi, *insider threat*, atau akses tidak sah.
* **Kegagalan Sistem atau Hardware Failure** yang dapat mengganggu ketersediaan layanan.
* **Kesalahan Manusia (Human Error)** seperti salah menghapus file penting, kesalahan konfigurasi sistem, atau membocorkan data tanpa sengaja.
* **Kehilangan atau Kerusakan Data** akibat backup yang tidak rutin atau serangan malware.
* **Bencana Fisik** seperti kebakaran, banjir, atau pemadaman listrik yang dapat mengakibatkan kerusakan infrastruktur.

### Identifikasi Kerentanan

Kerentanan (vulnerability) adalah kelemahan yang dapat dimanfaatkan oleh ancaman untuk menimbulkan kerusakan terhadap aset informasi. Beberapa kerentanan yang teridentifikasi di PT. ITI adalah sebagai berikut:

* Tidak adanya kebijakan keamanan formal dan kontrol akses yang terstandarisasi.
* Backup data tidak dilakukan secara otomatis dan terjadwal.
* Kurangnya pelatihan kesadaran keamanan (security awareness training) bagi karyawan.
* Sistem keamanan jaringan belum memiliki sistem deteksi dini (IDS/IPS) yang aktif.
* Penggunaan perangkat lunak pihak ketiga tanpa uji keamanan.
* Dokumentasi keamanan belum lengkap dan belum tersosialisasi ke seluruh tim.

### Tabel Identifikasi Aset, Ancaman, dan Kerentanan

|  |  |  |  |
| --- | --- | --- | --- |
| **Aset Informasi** | **Ancaman** | **Kerentanan** | **Dampak Potensial** |
| Kode Sumber (Source Code) | Pencurian data, akses tidak sah, serangan malware | Akses repositori tidak dibatasi dengan baik, tidak ada enkripsi | Kehilangan kekayaan intelektual, kerugian finansial |
| Data Klien dan Karyawan | Kebocoran data pribadi, *phishing*, *data breach* | Tidak adanya enkripsi data pribadi, autentikasi lemah | Pelanggaran hukum (UU PDP), kehilangan kepercayaan klien |
| Dokumentasi Proyek | Hilang, dicuri, atau dibagikan tanpa izin | Tidak adanya pengendalian hak akses | Gangguan proyek, kebocoran strategi bisnis |
| Server dan Jaringan | Serangan *ransomware* atau *DoS attack* | Firewall tidak diperbarui, tidak ada IDS | Gangguan layanan, downtime sistem |
| Akun & Kredensial Sistem | Penyalahgunaan akun, pencurian identitas | Password lemah, tidak ada *multi-factor authentication* | Akses tidak sah, manipulasi data |
| Infrastruktur Penyimpanan Data (NAS/Cloud) | Kerusakan fisik, kegagalan sistem | Tidak ada backup otomatis | Kehilangan data penting dan waktu pemulihan lama |

## Analisis Risiko Keamanan Informasi

Setelah dilakukan identifikasi terhadap aset informasi, ancaman, dan kerentanan pada tahap sebelumnya, langkah selanjutnya adalah melakukan analisis risiko. Analisis ini bertujuan untuk menentukan tingkat risiko (risk level) berdasarkan kombinasi antara dampak (impact) dan kemungkinan terjadinya (likelihood) suatu ancaman terhadap aset informasi.

Analisis risiko ini dilakukan menggunakan pendekatan kualitatif, di mana setiap ancaman dinilai berdasarkan tingkat dampak dan kemungkinan dengan skala rendah (Low), sedang (Medium), dan tinggi (High). Hasil dari penilaian ini kemudian digunakan untuk menentukan tingkat risiko keseluruhan, yang menjadi dasar dalam proses evaluasi dan prioritas mitigasi risiko pada tahap berikutnya.

### Kriteria Penilaian Risiko

Untuk menilai tingkat risiko, PT. ITI menggunakan dua parameter utama yaitu dampak (impact) dan kemungkinan (likelihood) yang masing-masing diklasifikasikan dalam tiga tingkat penilaian berikut:

|  |  |  |
| --- | --- | --- |
| **Tingkat** | **Dampak (Impact)** | **Kemungkinan (Likelihood)** |
| **Tinggi (3)** | Mengakibatkan kerugian besar seperti kehilangan data penting, gangguan layanan kritis, atau pelanggaran hukum. | Ancaman sangat mungkin terjadi karena sering muncul dalam lingkungan kerja atau sistem yang digunakan. |
| **Sedang (2)** | Menyebabkan gangguan sebagian pada layanan atau kebocoran data terbatas yang masih dapat dikendalikan. | Ancaman dapat terjadi sesekali akibat kelemahan sistem atau kesalahan manusia. |
| **Rendah (1)** | Menyebabkan dampak kecil yang tidak berpengaruh signifikan terhadap operasional perusahaan. | Ancaman jarang terjadi atau memerlukan kondisi khusus untuk muncul. |

### Matriks Penentuan Level Risiko

Untuk menentukan tingkat risiko keseluruhan, digunakan matriks kombinasi antara nilai dampak dan kemungkinan seperti berikut:

|  |  |  |  |
| --- | --- | --- | --- |
| **Dampak / Kemungkinan** | **Rendah (1)** | **Sedang (2)** | **Tinggi (3)** |
| **Rendah (1)** | Rendah | Rendah | Sedang |
| **Sedang (2)** | Rendah | Sedang | Tinggi |
| **Tinggi (3)** | Sedang | Tinggi | Tinggi |

Hasil kombinasi tersebut menghasilkan tiga kategori utama risiko:

* **Risiko Tinggi** → memerlukan tindakan mitigasi segera.
* **Risiko Sedang** → perlu pengendalian dan pemantauan rutin.
* **Risiko Rendah** → dapat diterima, tetapi tetap diawasi.

### Hasil Analisis Risiko

Berdasarkan hasil identifikasi aset informasi dan potensi ancaman pada sub-bab 4.1, diperoleh hasil analisis risiko sebagai berikut:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Aset Informasi** | **Ancaman Utama** | **Dampak (1–3)** | **Kemungkinan (1–3)** | **Level Risiko** | **Keterangan** |
| 1 | Kode Sumber (Source Code) | Pencurian data, modifikasi tidak sah | 3 | 3 | **Tinggi** | Aset utama perusahaan, sangat sensitif dan bernilai tinggi |
| 2 | Data Klien & Karyawan | Kebocoran data pribadi, *phishing* | 3 | 2 | **Tinggi** | Risiko hukum (UU PDP) dan reputasi tinggi |
| 3 | Dokumentasi Proyek | Hilang/disebar tanpa izin | 2 | 2 | **Sedang** | Dapat mengganggu jadwal proyek dan kepercayaan klien |
| 4 | Server & Jaringan | Serangan *ransomware*, *DoS* | 3 | 3 | **Tinggi** | Menyebabkan downtime layanan dan kerugian besar |
| 5 | Akun & Kredensial Sistem | Penyalahgunaan akun, *brute force attack* | 2 | 3 | **Tinggi** | Dapat membuka akses ilegal ke sistem internal |
| 6 | Infrastruktur Penyimpanan (NAS/Cloud) | Kegagalan sistem, kerusakan fisik | 2 | 2 | **Sedang** | Kehilangan data jika backup tidak otomatis |
| 7 | Strategi Bisnis & HKI | Akses tidak sah, kebocoran dokumen internal | 3 | 1 | **Sedang** | Dapat merusak posisi kompetitif perusahaan |
| 8 | SDM (Karyawan IT) | Human error, kurangnya pelatihan keamanan | 2 | 3 | **Tinggi** | Risiko tidak langsung yang berdampak sistemik |

### Analisis Hasil dan Interpretasi

Berdasarkan tabel di atas, dapat disimpulkan bahwa sebagian besar aset informasi PT. ITI memiliki tingkat risiko tinggi, terutama pada aset yang bersifat digital dan terhubung langsung dengan sistem inti perusahaan seperti kode sumber, data klien, dan server jaringan.

Faktor utama penyebab tingginya risiko antara lain:

* Akses repositori dan data sensitif yang belum sepenuhnya dilindungi dengan kontrol berlapis.
* Kurangnya otomatisasi dalam backup dan enkripsi data.
* Rendahnya kesadaran keamanan di tingkat karyawan.

Oleh karena itu, hasil analisis risiko ini akan digunakan sebagai dasar untuk:

1. Menentukan prioritas mitigasi (dibahas pada sub-bab 4.3).
2. Menyusun rencana tindakan pengendalian risiko (dibahas pada sub-bab 4.4).
3. Menetapkan rencana peningkatan berkelanjutan SMKI pada tahap implementasi selanjutnya.

## Evaluasi dan Prioritas Risiko

Tahapan evaluasi risiko bertujuan untuk menilai hasil analisis risiko yang telah dilakukan sebelumnya dan menentukan tingkat prioritas dalam penanganannya. Melalui proses ini, PT. Inovasi Teknologi Indonesia (PT. ITI) dapat mengarahkan sumber daya keamanan informasi secara efektif terhadap area yang memiliki dampak terbesar terhadap operasional dan reputasi perusahaan.

### Tujuan Evaluasi Risiko

Evaluasi risiko dilakukan untuk:

* Menentukan risiko mana yang dapat diterima (acceptable risk) dan mana yang memerlukan tindakan pengendalian segera.
* Menetapkan prioritas mitigasi berdasarkan tingkat keparahan (severity) dan kemungkinan terjadinya ancaman.
* Menjadi dasar dalam penyusunan rencana tindakan pengendalian risiko pada tahap selanjutnya.

Dengan adanya evaluasi ini, organisasi dapat memastikan bahwa keputusan pengendalian risiko selaras dengan konteks bisnis, kebutuhan keamanan, dan kebijakan perusahaan.

### Hasil Evaluasi Risiko

Berdasarkan hasil analisis risiko pada sub-bab 4.2, diperoleh gambaran umum bahwa sebagian besar aset informasi PT. ITI memiliki tingkat risiko tinggi. Risiko-risiko ini umumnya berkaitan dengan aset yang bernilai tinggi, berdampak langsung terhadap bisnis, atau melibatkan data pribadi yang diatur oleh regulasi.

Tabel berikut menggambarkan hasil evaluasi dan klasifikasi risiko berdasarkan tingkat prioritasnya:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Aset Informasi** | **Risiko Utama** | **Level Risiko** | **Kategori Prioritas** |
| 1 | Kode Sumber (Source Code) | Pencurian, modifikasi tidak sah | Tinggi | Sangat Prioritas |
| 2 | Data Klien & Karyawan | Kebocoran data pribadi | Tinggi | Sangat Prioritas |
| 3 | Server & Jaringan | Serangan *ransomware* atau *DoS attack* | Tinggi | Tinggi |
| 4 | Akun & Kredensial Sistem | Penyalahgunaan akses | Tinggi | Tinggi |
| 5 | Dokumentasi Proyek | Hilang/disebar tanpa izin | Sedang | Sedang |
| 6 | Infrastruktur Penyimpanan Data | Kegagalan sistem, kehilangan data | Sedang | Sedang |
| 7 | Strategi Bisnis & HKI | Akses tidak sah | Sedang | Menengah |
| 8 | SDM (Karyawan IT) | Human error, kurang kesadaran keamanan | Tinggi | Tinggi |

### Analisis Prioritas dan Pengambilan Keputusan

Hasil evaluasi di atas menunjukkan bahwa risiko dengan kategori sangat prioritas dan tinggi perlu segera mendapatkan perhatian dalam bentuk tindakan mitigasi konkret, baik melalui penerapan kontrol teknis maupun kebijakan organisasi. Beberapa langkah strategis yang perlu diprioritaskan antara lain:

1. **Pengamanan Kode Sumber dan Data Klien**

* Mengimplementasikan kontrol akses berbasis peran (role-based access control).
* Menerapkan enkripsi pada repositori dan data sensitif.
* Melakukan audit keamanan secara rutin.

1. **Perlindungan Server dan Infrastruktur Jaringan**

* Penerapan firewall dan sistem deteksi serangan (IDS/IPS).
* Melakukan pembaruan sistem (patching) secara berkala.
* Menyiapkan sistem disaster recovery dan backup otomatis.

1. **Manajemen Kredensial dan Kesadaran Karyawan**

* Penerapan autentikasi ganda (multi-factor authentication).
* Pelatihan keamanan informasi bagi seluruh karyawan.
* Pembentukan budaya keamanan (security culture) di lingkungan kerja.

Risiko dengan kategori sedang seperti kehilangan dokumentasi proyek atau gangguan penyimpanan data dapat ditangani melalui peningkatan prosedur internal dan pengawasan rutin.

Sementara risiko rendah masih perlu dipantau secara berkala sebagai bagian dari mekanisme continuous improvement dalam sistem manajemen keamanan informasi.

## Rencana Tindakan Mitigasi Risiko

Setelah dilakukan evaluasi terhadap hasil penilaian risiko, langkah berikutnya adalah menyusun rencana tindakan mitigasi risiko. Tahapan ini bertujuan untuk menentukan langkah-langkah pengendalian (controls) yang tepat dalam mengurangi tingkat risiko hingga berada pada level yang dapat diterima oleh organisasi.

Rencana mitigasi risiko harus mempertimbangkan efektivitas, kelayakan, serta kesesuaian dengan kebijakan keamanan informasi yang diterapkan. Pendekatan mitigasi di PT. ITI mengacu pada prinsip “defense in depth”, yaitu penerapan pengendalian berlapis untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad).

### Tujuan Mitigasi Risiko

Tujuan utama dari tindakan mitigasi adalah:

1. Mengurangi kemungkinan terjadinya ancaman terhadap aset informasi.
2. Meminimalkan dampak apabila ancaman terjadi.
3. Menjamin kelangsungan operasional dan reputasi organisasi.
4. Memastikan kepatuhan terhadap regulasi seperti UU Perlindungan Data Pribadi (UU PDP) dan standar ISO/IEC 27001:2022.

### Strategi Pengendalian Risiko

Dalam proses mitigasi, PT. ITI menerapkan empat strategi utama pengendalian risiko:

* **Risk Avoidance** → menghindari kegiatan yang berisiko tinggi (contoh: menonaktifkan layanan yang tidak aman).
* **Risk Reduction** → menerapkan kontrol untuk mengurangi kemungkinan atau dampak risiko (contoh: enkripsi data, firewall).
* **Risk Transfer** → memindahkan sebagian risiko kepada pihak ketiga (contoh: asuransi, kontrak layanan cloud).
* **Risk Acceptance** → menerima risiko yang tidak signifikan dan dipantau secara berkala.

### Rencana Mitigasi Risiko PT. ITI

Tabel berikut merangkum rencana tindakan mitigasi untuk setiap aset informasi berdasarkan hasil evaluasi sebelumnya:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Aset Informasi** | **Risiko Utama** | **Tindakan Mitigasi** | **Jenis Kontrol** | **Penanggung Jawab** |
| 1 | Kode Sumber (Source Code) | Pencurian atau modifikasi tidak sah | - Implementasi kontrol akses berbasis peran (RBAC) - Enkripsi repositori Git - Audit log aktivitas developer | Teknis & Prosedural | Tim Keamanan Siber & Pengembangan |
| 2 | Data Klien & Karyawan | Kebocoran data pribadi | - Enkripsi data pribadi dan komunikasi - Pembatasan akses berdasarkan kebutuhan - Penerapan kebijakan privasi dan NDA | Teknis & Organisasi | Divisi IT & HR |
| 3 | Server & Jaringan | Serangan *ransomware*, *DoS attack* | - Penerapan firewall dan IDS/IPS - Patch dan update sistem berkala - Backup harian otomatis | Teknis | Tim Infrastruktur & Keamanan |
| 4 | Akun & Kredensial Sistem | Penyalahgunaan akses | - Multi-Factor Authentication (MFA) - Kebijakan rotasi password - Pembatasan hak admin | Teknis | Tim Keamanan & Admin Sistem |
| 5 | Dokumentasi Proyek | Hilang atau dibocorkan tanpa izin | - Penyimpanan di server internal dengan kontrol akses - Penggunaan watermark pada dokumen sensitif | Prosedural | Project Manager & IT Support |
| 6 | Infrastruktur Penyimpanan Data | Kegagalan sistem atau kehilangan data | - Implementasi *disaster recovery plan* (DRP) - Backup otomatis dan pengujian restore - Monitoring kapasitas penyimpanan | Teknis & Prosedural | Tim Infrastruktur |
| 7 | Strategi Bisnis & HKI | Akses tidak sah atau kebocoran dokumen | - Pembatasan akses kepada level manajerial - Penggunaan enkripsi file - Audit akses berkala | Organisasi | Manajemen & Tim Legal |
| 8 | SDM (Karyawan IT) | Human error, kurang kesadaran keamanan | - Pelatihan keamanan berkala - Sosialisasi kebijakan SMKI - Simulasi penanganan insiden | Non-Teknis | HR & Tim Keamanan |

### Monitoring dan Tinjauan Berkala

Untuk memastikan efektivitas mitigasi risiko, PT. ITI perlu melakukan pemantauan dan tinjauan berkala terhadap seluruh kontrol yang diterapkan. Kegiatan ini meliputi:

* Audit internal keamanan informasi minimal dua kali setahun.
* Review terhadap efektivitas kontrol teknis (enkripsi, firewall, backup).
* Evaluasi ulang risiko jika terdapat perubahan sistem, proyek, atau kebijakan.

Hasil pemantauan akan menjadi dasar dalam proses perbaikan berkelanjutan **(Continual Improvement)** sesuai dengan siklus PDCA (Plan-Do-Check-Act) dalam standar **ISO/IEC 27001:2022**.

Dengan adanya rencana mitigasi ini, PT. Inovasi Teknologi Indonesia memiliki pedoman yang jelas dalam mengendalikan risiko keamanan informasi serta memastikan penerapan SMKI berjalan secara konsisten dan berkelanjutan.