SILABUS TRAINING

"AWARENESS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) BERBASIS STANDAR INTERNASIONAL ISO 27001"

Hari/Tanggal : Senin-Selasa, 9-10 Maret 2026

Durasi & Waktu : 2 Hari, 08.30-16.00 WIB

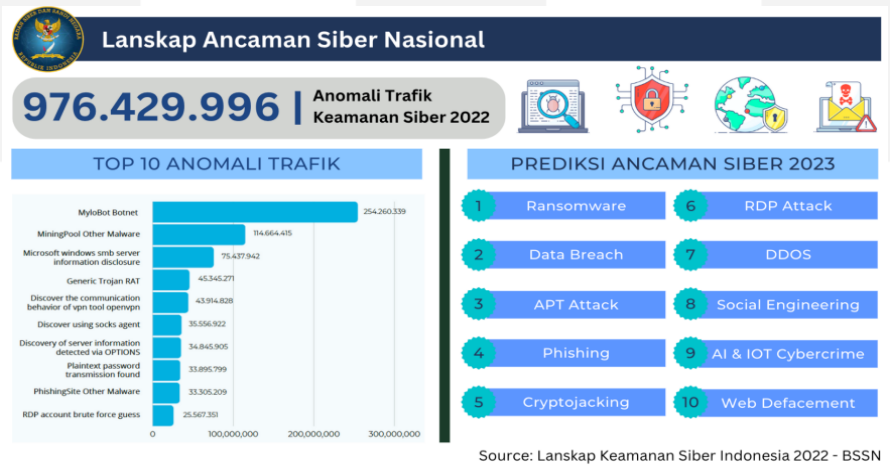
Lokasi : Jakarta, Hotel Bintang 4 (Hotel Ambhara / Hotel Cosmo Amaroosa, Tentative)

LATAR BELAKANG

Informasi merupakan aset yang sangat penting bagi setiap organisasi. Dalam persaingan bisnis, dapat dikatakan bahwa penguasaan informasi merupakan salah satu senjata utamanya.

Di lingkungan bisnis yang sangat kompetitif sekarang ini, informasi tersebut secara terus menerus mendapatkan ancaman dari banyak sumber seperti dari internal atau eksternal, yang disebabkan karena ketidaksengajaan atau memang suatu ancaman yang disengaja.

Penggunaan teknologi yang memberikan kemampuan organisasi untuk tumbuh dan mempertahankan pertumbuhannya, ternyata juga memperkenalkan risiko baru yaitu risiko keamanan informasi.



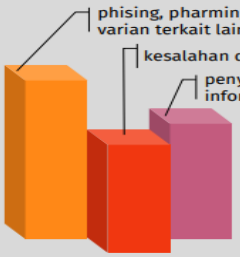
Source: Lanskap Keamanan Siber Indonesia 2022 - BSSN

PT. Infinity Berkah Indonesia | The Infinity Academy
Jl. Bango, Selosin Resident 2 Blok D No.2 Gunung Sindur, Bogor
Telp/HP : 0811-9878-785
Website: www.infinityacademyindonesia.com - www.infinityacademy.co.id

PROFIL RISIKO KEAMANAN SIBER SEKTOR INDUSTRI TAHUN 2022

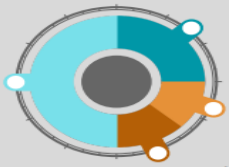
Direktorat KSSI melakukan manajemen risiko sektor industri dengan tujuan memberikan rekomendasi keamanan siber berdasarkan hasil penilaian risiko keamanan siber khususnya sektor industri.

Analisis risiko dilakukan terhadap beberapa stakeholder untuk memetakan beberapa hal diantaranya **lanskap ancaman, kerentanan serta profil risiko keamanan siber sektor industri.**



TOP #3 Ancaman Siber Sektor Industri 2022

TOP #3 Kerentanan Keamanan Siber Sektor Industri 2022



1. penggunaan hak akses yang tidak tepat (misalnya sharing password)
2. kurangnya kesadaran keamanan informasi dari personil yang terlibat.
3. kerentanan yang memungkinkan akses jaringan.

ANALISIS RISIKO KEAMANAN SIBER SEKTOR INDUSTRI

Risiko Tinggi :
- pencurian hak atas kekayaan intelektual perusahaan

Risiko Sedang :
- serangan DDOS yang menganggu produksi
- serangan malware, ransomware, zero days.

Risiko Sedang :
- hilangnya keandalan dan integritas produk,
- kerentanan akses jaringan,
- modifikasi/pencurian data customer, penyalahgunaan akses internet.

Pada tahun 2022, beberapa perusahaan sektor industri menjadi target serangan siber **Ransomware**. Serangan ini dilakukan dengan mengunci data yang dimiliki perusahaan dan meminta sejumlah tebusan agar pemilik data dapat mengakses kembali data yang dimiliki.
Hal ini menunjukkan bahwa keamanan siber harus menjadi kesadaran bersama semua pihak.

ISO/IEC 27001:2013 adalah Standar Sistem Manajemen Pengamanan Informasi yang membangun kesadaran terhadap pengelolaan keamanan Sistem Informasi organisasi secara menyeluruh dan meningkatkannya secara berkesinambungan.

Gambaran umum ISO/IEC 27001:2013

Ringkasan terkait ISO/IEC 27001:2013; mengapa organisasi memerlukan sertifikasi dan gambaran umum cara mendapatkan sertifikasi.

Apa?

ISO/IEC 27001 adalah **standar paling terkenal** yang menyediakan persyaratan untuk Sistem Manajemen Keamanan Informasi (SMKI). SMKI adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Ini termasuk **orang, proses dan sistem TI** dengan menerapkan proses manajemen risiko. Ini dapat membantu bisnis kecil, menengah dan besar di sektor apapun menjaga aset informasi tetap aman.

Mengapa?

ISO/IEC 27001 memberikan manfaat dari praktik keamanan informasi terkemuka. Organisasi mungkin memerlukan sertifikasi **untuk meyakinkan pelanggan, klien, *vendor, supplier,* dan/atau manajemen internal bahwa risiko keamanan informasi diidentifikasi dan dikurangi**. Sertifikasi menunjukkan bahwa organisasi bertanggung jawab untuk menangani dan **mengelola risiko terkait informasi sensitif dan aset**.

Bagaimana?

Organisasi akan membutuhkan **pihak ketiga yang independen** untuk melakukan audit sertifikasi. Hal ini dapat dicapai melalui **wawancara** dengan manajemen organisasi dan **melakukan pengujian kendali** untuk menentukan bagaimana SMKI ditangani. Hasil tes akan menentukan apakah pendekatan organisasi telah memenuhi kebutuhan SMKI secara efektif.

SNI ISO/IEC 27001:ISMS OVERVIEW

Why should the company implement SNI ISO 27001 ISMS?

Informasi adalah aset perusahaan, seperti aset bisnis penting lainnya, memiliki nilai bagi organisasi dan oleh karena itu perlu dilindungi

Information Security?

- Keamanan informasi adalah proses yang membuat informasi berharga 'bebas dari bahaya' (terlindungi, aman dari bahaya)
- *It is not something you* ***buy****, it is something you* ***do***
  - *It's a process not a product*
- Keamanan Informasi dapat dicapai dengan menggunakan kombinasi strategi dan pendekatan yang sesuai:
  - Implementasi dan integrasi Manajemen Risiko
  - Melindungi **CIA** (**C**onfidentiality, **I**ntegrity and **A**vailability)
  - Menghindari, mencegah, mendeteksi dan memulihkan dari insiden
  - Pengamanan people, processes *and* technology ... tidak hanya IT!

ISO 27001

ISO 27001 – INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah.

Perlindungan informasi atau pencegahan penyalahgunaan informasi

- Menjaga bisnis dan proses TI
- Membangun ketahanan sistem informasi
- Pemenuhan Persyaratan Regulas

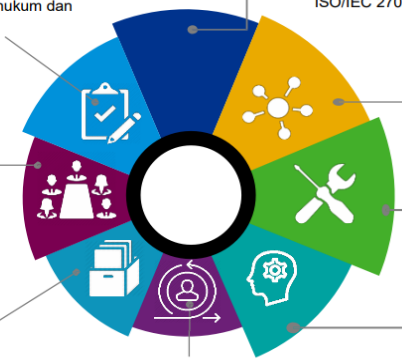
Manfaat utama implementasi standar keamanan

Pemantauan Ketaatan
Identifikasi dan pengelolaan berbagai persyaratan hukum dan peraturan dari beberapa fungsi.

Pengaturan Strategi
Penyelarasan yang lebih baik dengan standar ISO/IEC 27001:2013 dan praktik kerja industri lainnya.

Standardisasi Proses
Berfokus pada Penyesuaian diikuti oleh berbagai proses departemen.

Manajemen Risiko yang Efektif
Berfokus pada penerapan berbagai kendali untuk manajemen risiko yang efektif di seluruh organisasi.



Komitmen Manajemen
Arahan dan dukungan dari manajemen dalam meningkatkan Sistem Informasi Organisasi.

Kepuasan Pelanggan Lebih Tinggi
Meningkatkan layanan manajemen dan juga meningkatkan manajemen masalah dan insiden.

Berfokus pada Organisasi
Berfokus pada penerapan Keamanan Informasi di setiap departemen.

Mekanisme Tata Kelola yang jelas
Mengidentifikasi peran dan tanggung jawab pemangku jabatan yang mendorong kerangka kerja Keamanan Informasi.

TUJUAN

Setelah mengikuti training ini peserta dapat :

1. Mengetahui pentingnya melakukan pengamanan informasi.
2. Memahami berbagai standar best practice information security.
3. Memahami Sistem Manajemen Keamanan Informasi.
4. Memahani cara mengelola risiko kemanan informasi.
5. Memahami berbagai control atau pengendalian keamanan informasi.

MATERI

1. Trend dan status terkini cybercrime/cyber incident dan cybersecurity
   Mengetahui dan waspada terhadap berbagai tren insiden keamanan informasi sehingga peserta training mengerti betapa berharganya keamanan informasi
2. Best Practice standar internasional Information security dan Cybersecurity
   Mengetahui berbagai best practice standar internasional information security. Salah satunya Information Security Management System (ISMS) ISO 27001
3. Information Security Management System (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI)
   Mengetahui dan memahami konsep framework Keamanan Informasi sesuai standar internasional ISO 27001 (SMKI)

PESERTA

1. Pimpinan, manajer dan staf yang bertanggung jawab dan berperan dalam penyelenggaraan pengamanan informasi.
2. Pemimpin, manajer dan staf unit kerja pada bagian-bagian yang akan menjadi ruang lingkup pengamanan informasi.
3. Audit internal

INVESTASI

Investasi Normal	: Rp. 5.000.000,- Per Peserta
Investasi Grup	: Diskon 10% dari Investasi Normal Per Peserta untuk pendaftaran minimal 5 peserta
Fasilitas yang di dapat	: Sertifikat Cetak, Modul (hardcopy/cetak dan softcopy via email), Training KIT, Souvenir (T-shirt/Jaket/Tumbler - menyesuaikan stok), Meeting Room dan Fasilitasnya, Konsumsi selama training (coffee break dan makan siang, namun khusus untuk muslim yang berpuasa, makan siang diganti dengan buka puasa, di hotel atau *takeaway*), PPh
Non Fasilitas	: Transportasi dan Akomodasi Peserta, PPN

Catatan Pendaftaran Grup:

Untuk pendaftaran grup (minimal 5 peserta), peserta bisa *request* jadwal atau *request private class*

PT. Infinity Berkah Indonesia | The Infinity Academy
Jl. Bango, Selosin Resident 2 Blok D No.2 Gunung Sindur, Bogor
Telp/HP : 0811-9878-785
Website: www.infinityacademyindonesia.com - www.infinityacademy.co.id

INFORMASI LEBIH LANJUT, PENDAFTARAN & INHOUSE TRAINING

The Infinity Academy | PT Infinity Berkah Indonesia

Email: marketing@infinityacademy.co.id

Website : www.infinityacademy.co.id;

Sosial Media: (Instagram) theinfinity.academy; (Tiktok) theinfinity.acad

Marketing:

Ratna Samiah (Public dan Inhouse Training)

No Hp: 0811-9878785

Email: ratna.infinityacademy@gmail.com

Vina Firmalia (Inhouse Training)

No Hp: 0812-1849 9009

Email: vinafirmalia.infinityacademy@gmail.com