bima sakti alterra

SOSIALISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

bima sakti alterra

Agenda

- Keamanan Infomasi
- Sistem Manajemen Keamanan Informasi
- Sekilas Standar ISO 27001:2013
- Penerapan SMKI
- Panduan Implementasi
- Diskusi

Apa yang dimaksud dengan INFORMASI?

Sesuatu (data) yang **memiliki nilai (bisnis dan operasional) bagi organisasi**.

Sesuatu (data) yang **kritikal bagi operasional organisasi**.

Information :
Database, storage media
Procedures, etc

Software:
Application software
System software

Contract documents
Asset list

Intangibles :
Goodwill, reputation
Confidence, image

Physical:
Computer, printers, fax
Phone, mobile phone

Informasi dimana – mana

- ***Informasi menjadi lebih penting bagi organisasi.***
- ***Berapa banyak informasi yang dimiliki?***

bima sakti alterra

Keamanan Informasi

Apa yang dimaksud dengan KEAMANAN INFORMASI?

Terlindunginya informasi dari akses yang tidak terotorisasi, kesalahan penggunaan, kebocoran, kerusakan, dan modifikasi, berdasarkan aspek kerahasiaan (*confidentiality*), keakuratan *(integrity)*, dan ketersediaan (*availability*).

Confidentiality

Suatu aspek yang menjamin kerahasian suatu data dan akses terhadap informasi tersebut sesuai dengan kewenangan yang diberikan.

Integrity

Suatu aspek yang menjamin bahwa data atau informasi tidak boleh berubah tanpa seizin pemilik data sehingga terjaga akurasi dan kelengkapannya.

Availability

Suatu aspek yang menjamin bahwa data atau informasi harus dapat tersedia setiap saat ketika dibutuhkan.

Mengapa diperlukan KEAMANAN INFORMASI?

Infomasi adalah aset, seperti aset bisnis penting lainnya, yang memiliki nilai bagi suatu organisasi sehingga pada akhirnya perlu untuk diamankan. (ISO 27002:2013).

Sasaran Pengamanan Informasi

- mengurangi **tingkat dampak** dari insiden keamanan informasi
- mengurangi **tingkat kemungkinan** dari terjadinya insiden keamanan informasi
- upaya **mencegah** terjadinya insiden keamanan informasi
- **melindungi** informasi dari dampak akibat terjadinya insiden
- upaya **deteksi dini** terjadinya insiden atau dampak dari insiden
- **respon yang tepat** terhadap kejadian insiden untuk meminimasi dampak terhadap bisnis
- **pemulihan** yang cepat ketika terjadi insiden

Manfaat Pengamanan Informasi Bagi Bisnis

- mempertahankan kepercayaan *stakeholder* dalam organisasi
- mempertahankan posisi bisnis
- memastikan keberlangsungan bisnis

Komponen Keamanan Informasi

Staff Organisasi

Personil yang menggunakan atau berinteraksi dengan informasi

Proses Bisnis

Merupakan alur kerja mengenai beberapa aktivitas yang mendukung tujuan bisnis

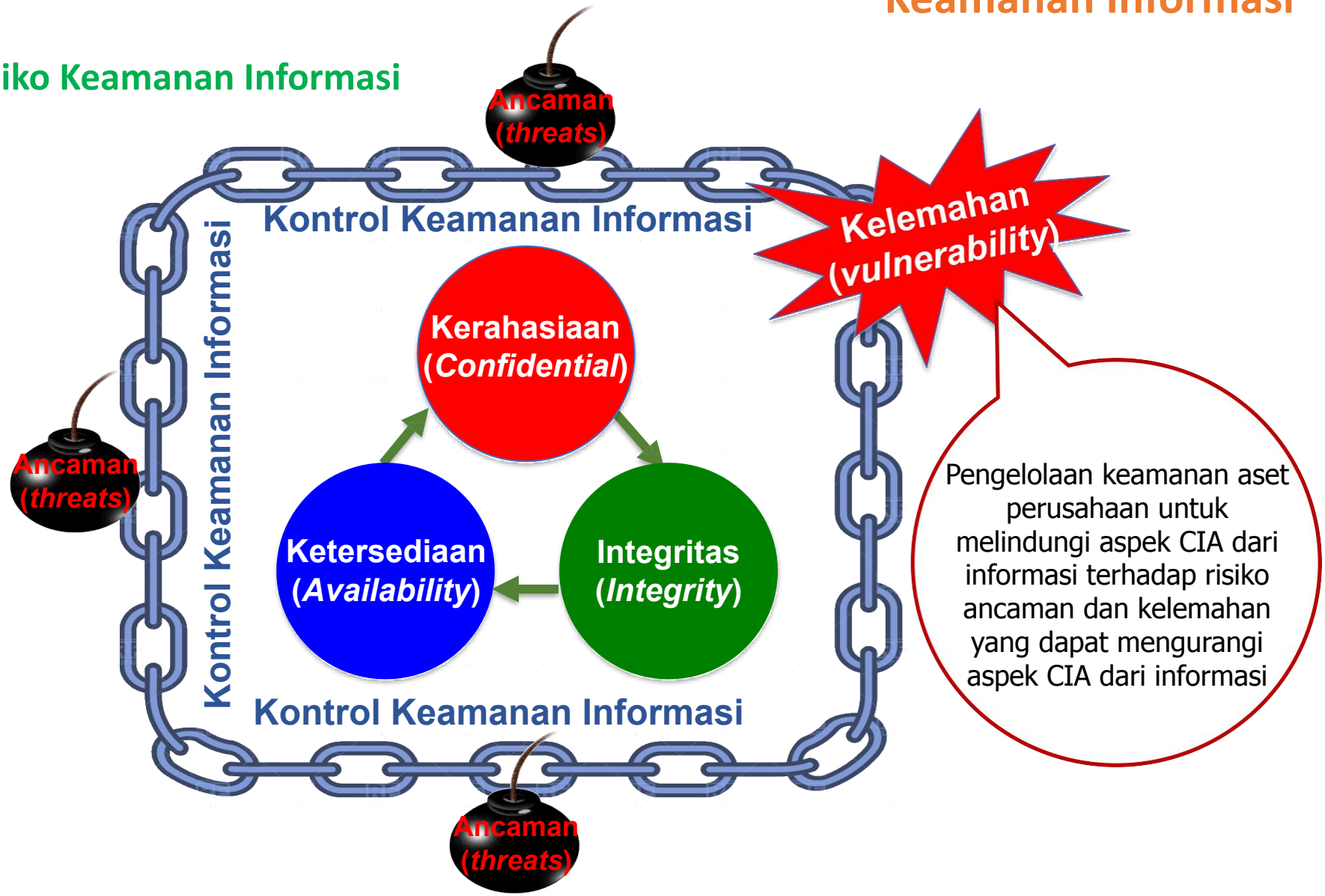
Teknologi Yang Digunakan

Apa yang digunakan untuk meningkatkan aktivitas proses

bima sakti alterra

Keamanan Informasi

Risiko Keamanan Informasi



Contoh Sumber Ancaman Keamanan Informasi

High User Knowledge of IT Systems

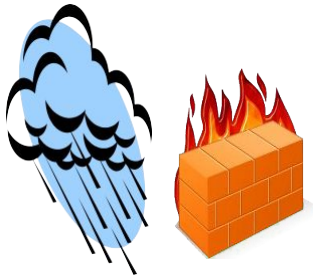
Theft, Sabotage, Misuse

Virus Attacks

Systems & Network Failure

Lack Of Documentation

Lapse in Physical Security



Natural Calamities & Fire

Kasus Keamanan Informasi

Virus Ransomware WannaCry Serang Perpustakaan Universitas Jember

Reporter: Tempo.co
Editor: MC Nieke Indrietta Baiduri

Selasa, 16 Mei 2017 08:38 WIB

KOMENTAR 0 0 0 0 3

Ilustrasi hacker. crashonline.gr

TEMPO.CO, Jember - Perpustakaan Universitas Jember, Jawa Timur, terserang virus ransomware WannaCry. Akibatnya, pelayanan perpustakaan dalam jaringan (daring) dan manual dihentikan sementara oleh pihak pengelola perpustakaan setempat.

Diserang Virus Ransomware, Komputer Rumah Sakit Dharmais Lumpuh

Reporter: Tempo.co
Editor: Suseno TNR

Senin, 15 Mei 2017 19:14 WIB

0 KOMENTAR 0 0 0 0 6

Ilustrasi virus ransomware

TEMPO.CO, Jakarta - Abdul Kadir, Direktur Utama Rumah Sakit Kanker Dharmais, mengatakan sekitar 600 unit komputer di rumah sakitnya tidak bisa digunakan setelah diserang virus Ransomware Wannacry pada Sabtu lalu. Saat ini sekitar 15 teknisi tengah bekerja keras untuk membersihkan virus. “Dua hari ini semua komputer diinstal ulang,” kata Abdul di kantornya, Senin, 15 Mei 2017.

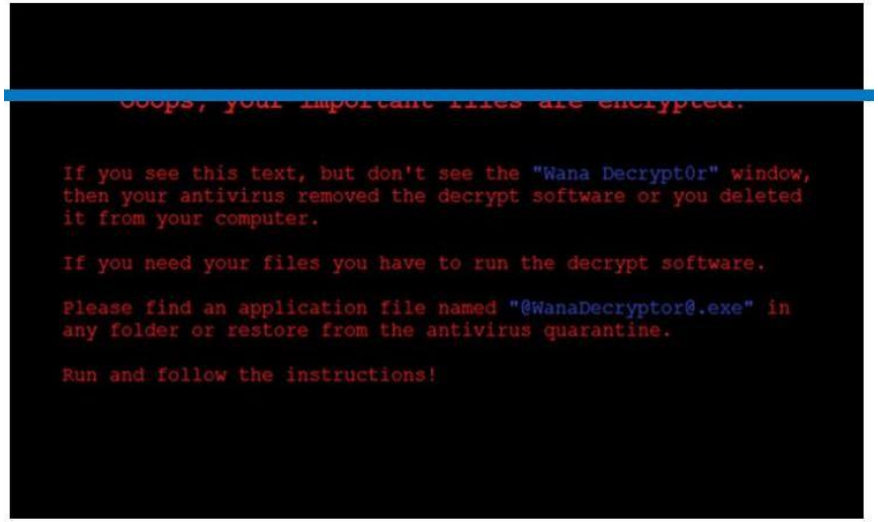
Kasus Keamanan Informasi

Home / Tekno / Internet

Kena Ransomware, Rumah Sakit Ini Terpaksa Bayar Tebusan Rp 226 Juta

YOGA HASTYADI WIDIARTANTO

Kompas.com - 14/05/2017, 11:18 WIB



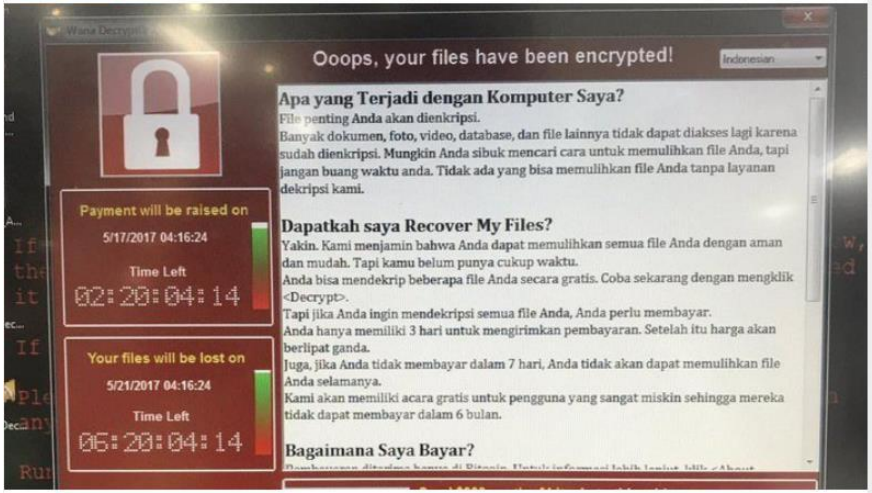
Tampilan wallpaper di komputer korban yang diganti oleh ransomware Wanna Decryptor. (Avast Software)

Minggu, 06 Mei 2018 12:40 WIB

Serangan WannaCry di Indonesia Terbesar Kedua di Dunia

Muhammad Alif Goenawan - detikInet

1 komentar



WannaCry di Indonesia. Foto: @ilhamnegara

bima sakti alterra

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen
(ISO 27000:2018 Klausul 4.2.5)
Kerangka kerja yang mencakup panduan, kebijakan, prosedur, proses, dan sumber daya terkait **untuk memastikan sebuah organisasi mencapai tujuannya**

Keamanan Informasi
(ISO 27000:2018 Klausul 4.2.3)
Kondisi dimana terjaganya aspek **kerahasiaan**, **integritas,** dan **ketersediaan** dari informasi

Implementasi mencakup:

- Persyaratan dan Kebijakan
- Perencanaan Implementasi
- Implementasi dan Operasi
- Pemantauan dan Peninjauan
- Peningkatan Berkesinambungan


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

bima sakti alterra

Sistem Manajemen Keamanan Informasi (SMKI)

Kunci Keberhasilan Penerapan SMKI

1. Implementasi SMKI harus didasari oleh target pencapaian sasaran yang diinginkan.
2. Implementasi SMKI harus memperoleh **dukungan aktif** dari manajemen senior / **manajemen puncak**.
3. Manajemen harus memandang SMKI sebagai langkah dan proses perubahan dengan **perbaikan yang berkesinambungan atas proses operasional**, tidak hanya sebagai proyek.
4. Implementasi SMKI **bukan hanya sekedar inisiatif TI**.
5. **Fokus pada konsistensi penerapan** untuk mencapai sasaran, bukan kepada sertifikat tercantum di dinding.

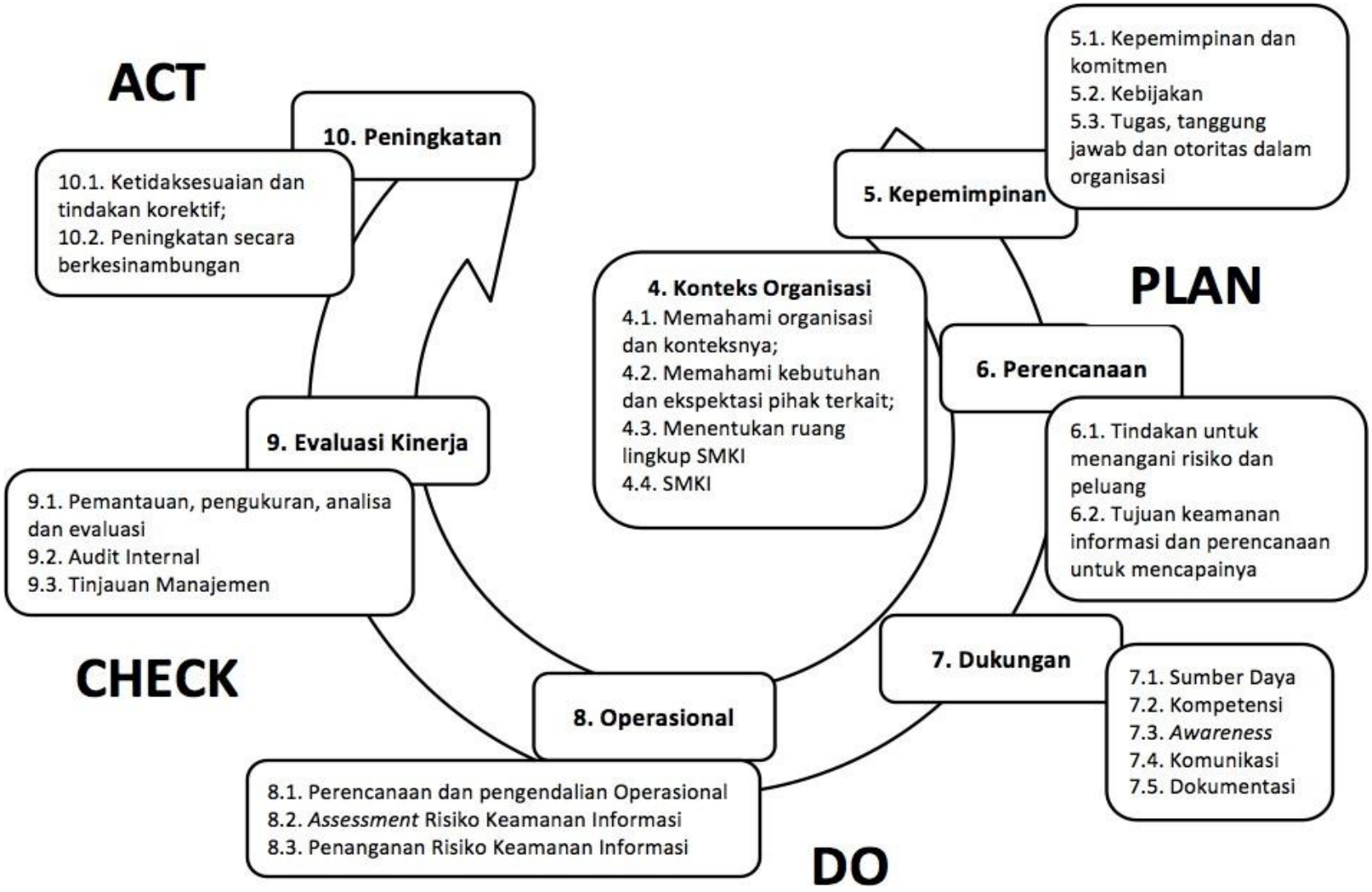
bima sakti alterra

Standar ISO 27001:2013

bima sakti alterra

Standar ISO 27001:2013

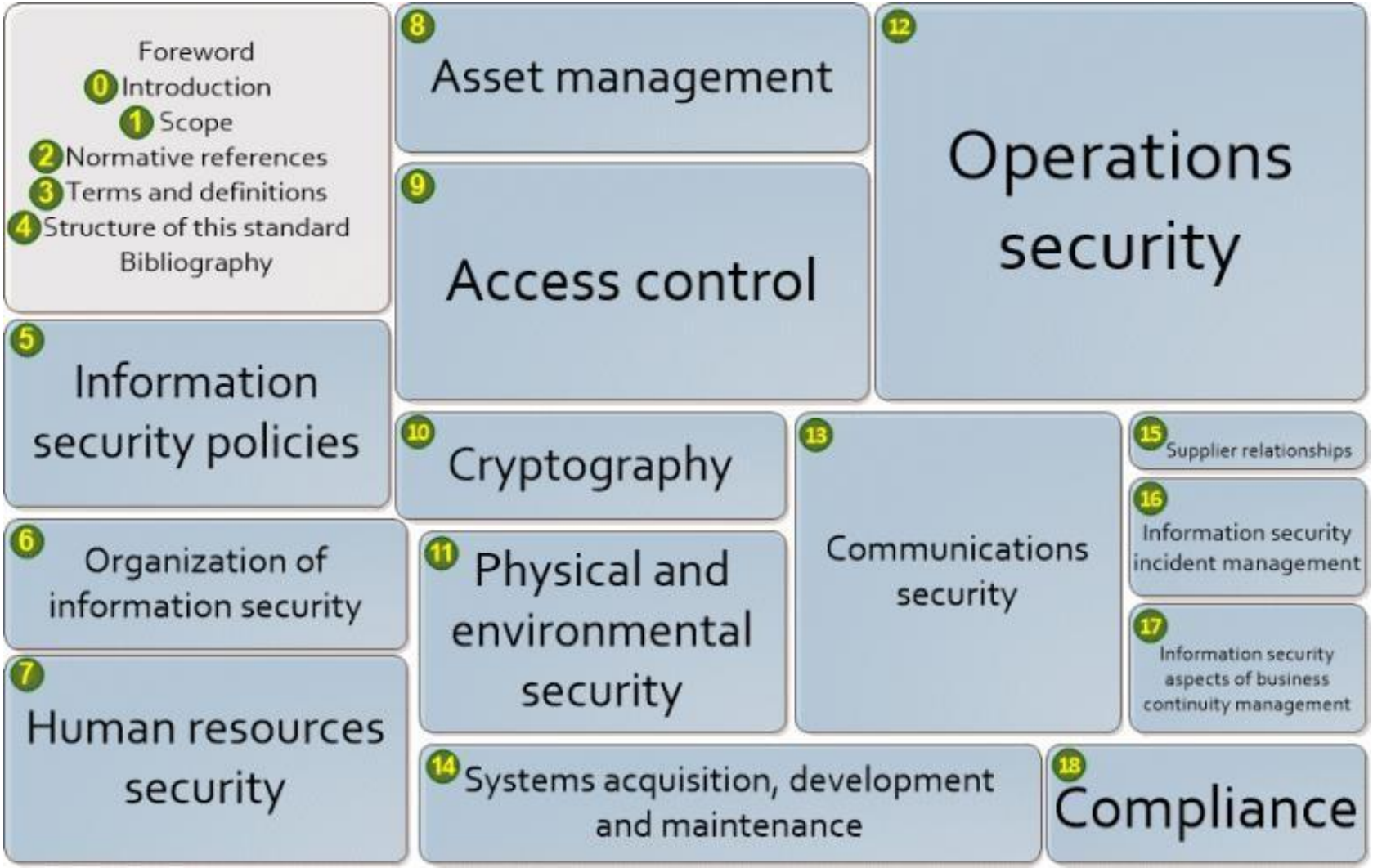
Klausul ISO 27001:2013



bima sakti alterra

Standar ISO 27001:2013

Annex A ISO 27001:2013



bima sakti alterra

Standar ISO 27001:2013

Domain Kontrol Annex A ISO 27001:2013 : 14 Domain | 114 Kontrol

Annex A	Prasyarat	Kontrol
A.5	Kebijakan Keamanan Informasi	2
A.6	Organisasi Keamanan Informasi	7
A.7	Keamanan Sumber Daya Manusia	6
A.8	Pengelolaan Aset	10
A.9	Pengelolaan Akses	14
A.10	Kriptografi	2
A.11	Keamanan Fisik dan Lingkungan	15
A.12	Keamanan Operasional	14
A.13	Keamanan Komunikasi	7
A.14	Akuisisi, Pengembangan, dan Pemeliharaan Sistem	13
A.15	Hubungan Dengan Pemasok	5
A.16	Pengelolaan Insiden Keamanan Informasi	7
A.17	Aspek Keamanan Informasi Dalam Keberlangsungan Bisnis	4
A.18	Kepatuhan	8

bima sakti alterra

Panduan Implementasi

PENGELOLAAN INFORMASI / DOKUMEN

Informasi harus diinventarisasi, diberi identifikasi & label sesuai ketentuan & klasifikasinya

Distribusi Informasi hanya kepada pihak yang terotorisasi

Simpan informasi kritikal ditempat yang aman

Pastikan informasi kritikal yang sudah tidak digunakan telah dimusnahkan

Tidak membuang informasi kritikal di tempat sampah tanpa dihancurkan dahulu

Tidak memberikan akses ke informasi kritikal kepada pihak yang tidak terotorisasi.

Tidak meninggalkan dokumen informasi rahasia/kritikal saat tidak digunakan atau sedang di cetak pada mesin

bima sakti alterra

Panduan Implementasi

PENGELOLAAN SDM

Pastikan seluruh pegawai & para pihak terkait telah diberikan *awareness* keamanan informasi

Pastikan kebijakan dan prosedur serta dokumen terkait SMKI telah disosialisasikan kepada seluruh pegawai

Setiap terdapat perubahan status kepegawaian, lakukan & dokumentasikan penyesuaian terhadap pencatatan aset dan hak akses

bima sakti alterra

Panduan Implementasi

PENGELOLAAN ASET

Tinjau Register Aset secara berkala, pastikan kesesuaian catatan dengan kondisi di lapangan

Pastikan & dokumentasikan proses pengembalian aset ketika terdapat perubahan / pemberhentian personil

Gunakan Flashdisk hanya untuk proses pemindahan informasi (*Copy-Cut-Paste*)

Tidak menggunakan *Flashdisk / Memory Card*
untuk menyimpan informasi dalam jangka panjang

bima sakti alterra

Panduan Implementasi

PENGELOLAAN AKSES

Pastikan setiap pemberian akses telah terotorisasi & didokumentasikan

Berikan akses sesuai dengan tugas & kewenangannya

Lakukan peninjauan (*review*) Hak Akses secara berkala & dokumentasikan

- **Gunakan *password* sesuai dengan standar yang berlaku : Minimal 8 Karakter kombinasi angka, huruf besar & kecil.**
- **Ubah *password* secara berkala utk sistem kritikal**

bima sakti alterra

Panduan Implementasi

PENGELOLAAN AKSES

Tidak menuliskan *password* dan menempelkannya di tempat yang dapat terlihat publik

Tidak memberitahukan *password* pada orang lain

Tidak menggunakan *password* yang mudah ditebak

Tidak mengaktifkan fitur "*Remember Password*" pada browser

Tidak mengirimkan informasi *password* secara langsung pada *body* email

bima sakti alterra

Panduan Implementasi

KEAMANAN FISIK & LINGKUNGAN

Selalu menggunakan ID Card/ Access Card miik sendiri

Tidak meminjamkan ID Card/ Access card kepada siapa pun

Jika terdapat orang yang tidak dikenal, tanyakan kepentingannya

Pastikan ruangan kerja terjaga atau terkunci
ketika anda akan meninggalkan area kerja

Pastikan tersedia perangkat yang memadai untuk perlindungan terhadap ancaman lingkungan(contoh: APAR untuk ruang kerja)

Aktifkan CCTV pada area kritikal, pastikan rekaman dapat diakses ketika dibutuhkan

bima sakti alterra

Panduan Implementasi

KEAMANAN FISIK & LINGKUNGAN

Lakukan pemeliharaan perangkat secara
berkala & dokumentasikan

Terapkan *Clear Desk* & *Clear Screen*

Selalu mengunci layar PC/Notebook dengan menekan Windows+L atau Log Off ketika akan meninggalkan meja kerja

Terapkan *Secure Disposal* terhadap media penyimpan informasi ketika akan dilakukan pemusnahan / penggunaan kembali perangkat

Tidak meninggalkan meninggalkan perangkat kerja tanpa perlindungan / penjagaan terutama di tempat umum

bima sakti alterra

Panduan Implementasi

KEAMANAN OPERASIONAL

Setiap perubahan harus terotorisasi & terdokumentasi

Lakukan pemantauan pemantauan, pelaporan, & proyeksi kapasitas secara berkala

Instal, *update*, aktifkan *auto-scan* & *full- scan* antivirus di PC/Notebook

Lakukan *scanning* dengan antivirus sebelum membuka file/dokumen

Lakukan *backup* terhadap informasi kritikal & data *backup* diuji secara periodik

bima sakti alterra

Panduan Implementasi

KEAMANAN OPERASIONAL

Instalasi *software* & perubahan konfigurasi keamanan hanya dapat dilakukan administrator

Instalasi *software* diluar Daftar Software Yang Diizinkan harus memperoleh otorisasi & didokumentasikan

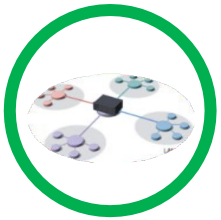
Lakukan *monitoring* & *review Log* secara berkala, pastikan *Log records* tersimpan & dapat diakses setiap dibutuhkan

Tidak melakukan instalasi *software* dari sumber yang tidak resmi / tidak dapat dipastikan keamanannya

bima sakti alterra

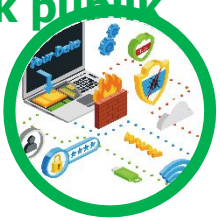
Panduan Implementasi

KEAMANAN JARINGAN & KOMUNIKASI



Lakukan pemisahan (segregasi) jaringan antara jaringan internal dan jaringan untuk publik

Instalasi / Aktifkan *Firewall*, lakukan pemantauan secara berkala & analisa jika terdapat ketidaksesuaian akses ke jaringan



Periksa kembali isi dan lampiran dari email yang akan dikirimkan

Pastikan alamat email yang dituju sudah benar

Berikan pengamanan (*password*) untuk pengiriman informasi kritikal

Kirimkan informasi *password* untuk *attachment*

bima sakti alterra

Panduan Implementasi

KEAMANAN JARINGAN & KOMUNIKASI

Pastikan website yang akan diakses tidak berbahaya dan bebas dari *spyware*

Tidak mengakses *website* yang tidak dikenal/tidak dapat dipercaya, atau mengakses URL yang diberikan dalam *website* tersebut

Hindari melakukan akses ke jaringan organisasi menggunakan fasilitas publik

Tidak membuka email yang terlihat mencurigakan, hapus email jika tidak yakin akan kebenarannya

Tidak menggunakan internet untuk keperluan pribadi dan mengunduh file diluar pekerjaan

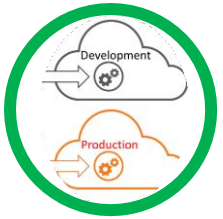
bima sakti alterra

Panduan Implementasi

PENGEMBANGAN & PEMELIHARAAN SISTEM

Pastikan spesifikasi & desain system / *software* telah mencakup persyaratan keamanan informasi

Lakukan pemisahan antara lingkungan pengembangan & pengujian dengan lingkungan produksi/operasional



Setiap perubahan pada proses pengembangan sistem harus terotorisasi & terdokumentasi

Lakukan & dokumentasikan UAT & *Security Testing*, pastikan seluruh persyaratan telah terpenuhi

Tidak melakukan proses perubahan / pengembangan langsung di lingkungan produksi / operasional

bima sakti alterra

Panduan Implementasi

PENGELOLAAN PEMASOK (*SUPPLIER*)

Pastikan seluruh pemasok (*supplier*) telah diberikan *awareness* keamanan informasi

Pastikan seluruh pemasok (*supplier*) telah menandatangani NDA

Lakukan & dokumentasikan *progress meeting* secara berkala dalam rangka proses *monitoring* kinerja pemasok

***Review* & pastikan kesesuaian hasil pekerjaan dari pemasok dengan perjanjian / spesifikasi yang telah ditetapkan**

bima sakti alterra

Panduan Implementasi

PENGELOLAAN INSIDEN

Laporkan & dokumentasikan setiap insiden / potensi insiden / ketidaksesuaian yang terjadi

Analisa akar penyebab & tentukan tindakan koreksi & korektif atas insiden yang terjadi

Dokumentasikan hasil analisa & tindak lanjut penanganan insiden

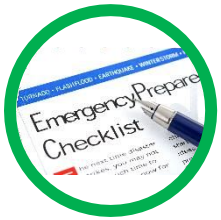
bima sakti alterra

Panduan Implementasi

PENGELOLAAN KEBERLANGSUNGAN BISNIS

Lakukan peninjauan berkala terhadap Perencanaan Keberlangsungan Bisnis (BCP), pastikan kesesuaian dengan kondisi / proses bisnis terkini

Lakukan pengujian keberlangsungan bisnis secara berkala & dokumentasikan



bima sakti alterra

Panduan Implementasi

KEPATUHAN

Gunakan *Software* berlisensi resmi/legal

Pelajari setiap ketentuan persyaratan yang terkait sebelum menggunakan informasi / dokumen / *software*

Pastikan setiap penggunaan informasi / dokumen / *software* telah sesuai dengan ketentuan persyaratan & hukum yang berlaku

bima sakti alterra

Pertanyaan & Diskusi