KOMDIGI
Kementerian Komunikasi dan Digital
Republik Indonesia

BADAN SIBER DAN SANDI NEGARA

GTA Government Transformation Academy

digitalent

MANAJEMEN RISIKO KEAMANAN SPBE

Pengenalan Manajemen Risiko Keamanan SPBE

Nama Pengajar

Jakarta, 22 Januari 2025

KOMDIGI
Kementerian Komunikasi dan Digital
Republik Indonesia

BADAN SIBER DAN SANDI NEGARA

GTA Government Transformation Academy

digitalent

Profil Pengajar

<Nama Pengajar>

Asal Instansi:

Pendidikan:

Pengalaman:

Dsb..

KOMDIGI
Kementerian Komunikasi dan Digital Republik Indonesia

BADAN SIBER DAN SANDI NEGARA

GTA Government Transformation Academy

digitalent

MATA PELATIHAN

1. Pengenalan Manajemen Risiko Keamanan SPBE (Hari Pertama);
2. Kebijakan Manajemen Risiko Keamanan SPBE (Hari Pertama);
3. Metodologi Identifikasi Risiko Keamanan SPBE;
4. Evaluasi Kerentanan dan Ancaman Keamanan SPBE;
5. Metodologi Evaluasi Risiko;
6. Pengelolaan Risiko melalu Kontrol Keamanan (Mitigasi Risiko Keamanan SPBE);
7. Pemantauan Mitigasi Risiko Keamanan SPBE;
8. Mitigasi Penanganan Risiko Keamanan SPBE.

DESKRIPSI SINGKAT

Setelah selesai pembelajaran peserta diharapkan mampu mengetahui Manajemen Risiko Keamanan SPBE yang terdiri dari Risk-Based Security, Prinsip Keamanan Informasi, Cluster Domain Keamanan, Prinsip Keamanan SPBE, Ilustrasi Risiko Keamanan SPBE, Prinsip Manajemen Risiko dalam Keamanan SPBE, Tahapan Manajemen Risiko Keamanan SPBE.

HASIL BELAJAR

Setelah selesai pembelajaran peserta diharapkan mampu mengetahui Manajemen Risiko Keamanan SPBE.

INDIKATOR HASIL BELAJAR

Peserta dapat :

1. Menjelaskan Risk-Based Security;
2. Menjelaskan Prinsip Keamanan Informasi;
3. Menjelaskan Cluster Domain Keamanan;
4. Menyebutkan Prinsip Keamanan SPBE;
5. Menyebutkan Ilustrasi Risiko Keamanan SPBE;
6. Menyebutkan Prinsip Manajemen Risiko dalam Keamanan SPBE;
7. Menyebutkan Tahapan Manajemen Risiko Keamanan SPBE.

KOMDIGI
Kementerian Komunikasi dan Digital
Republik Indonesia

BADAN SIBER DAN SANDI NEGARA

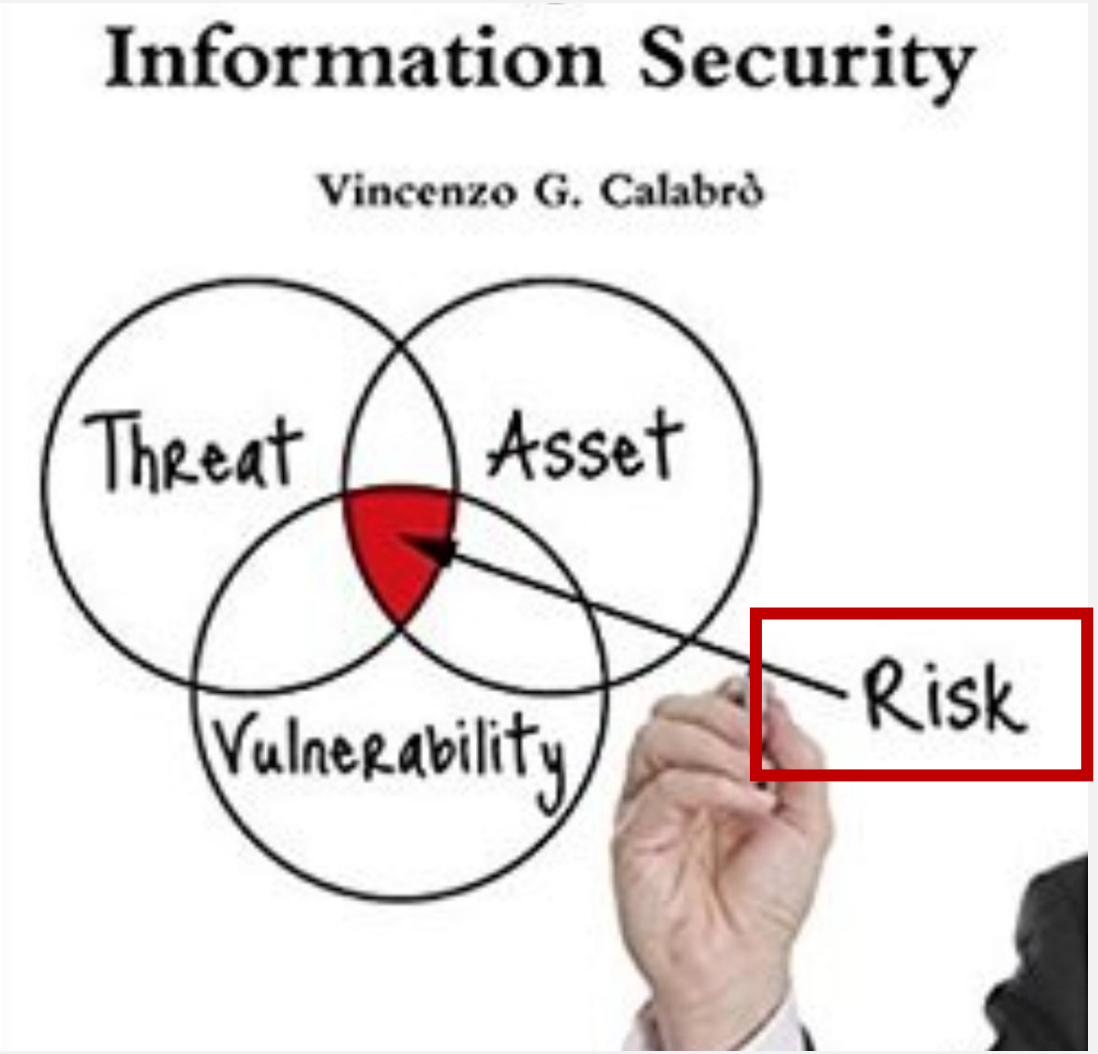
GTA Government Transformation Academy

digitalent

OUTLINE MATERI

1. Risk-Based Security;
2. Prinsip Keamanan Informasi;
3. Cluster Domain Keamanan;
4. Prinsip Keamanan SPBE;
5. Ilustrasi Risiko Keamanan SPBE;
6. Prinsip Manajemen Risiko dalam Keamanan SPBE;
7. Tahapan Manajemen Risiko Keamanan SPBE.

1. RISK-BASED SECURITY



Keamanan Informasi harus berdasarkan risiko

Keamanan informasi yang berdasarkan risiko (risk-based information security) adalah sebuah pendekatan untuk melindungi informasi dengan fokus pada aset informasi yang paling penting dan risiko yang paling signifikan. Pendekatan ini membantu organisasi untuk:

1. Mengoptimalkan sumber daya:

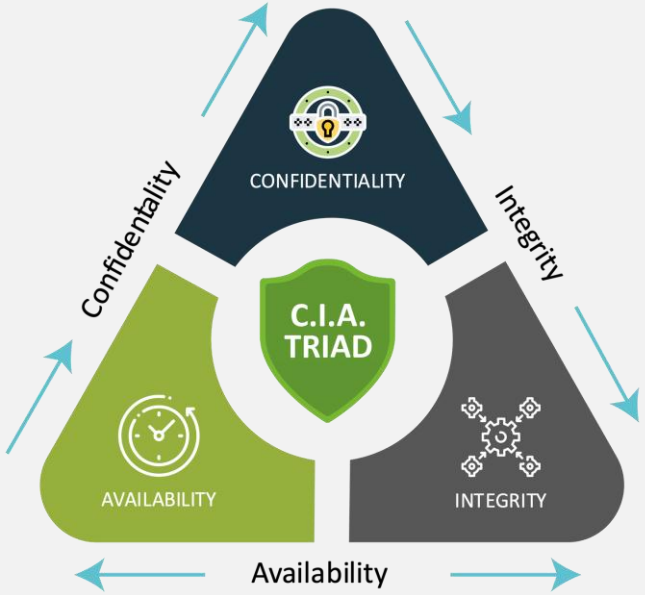
- Mengalokasikan sumber daya keamanan informasi ke area yang paling membutuhkannya.
- Menghindari pemborosan sumber daya untuk melindungi aset yang tidak terlalu penting.

2. Meningkatkan efektivitas:

- Memfokuskan upaya pada risiko yang paling besar kemungkinan terjadi dan berdampak paling besar.
- Meningkatkan peluang untuk mendeteksi dan mencegah pelanggaran keamanan.
- Meningkatkan potensi kepatuhan jika sudah diketahui akan menghadapi risiko yang akan berdampak bagi organisasi

RISK-BASE SECURITY

2. PRINSIP KEAMANAN INFORMASI



Confidentiality

- Protection of information that allows authorized users to access crucial data
- Any information that is sensitive and accessible to limited users

Integrity

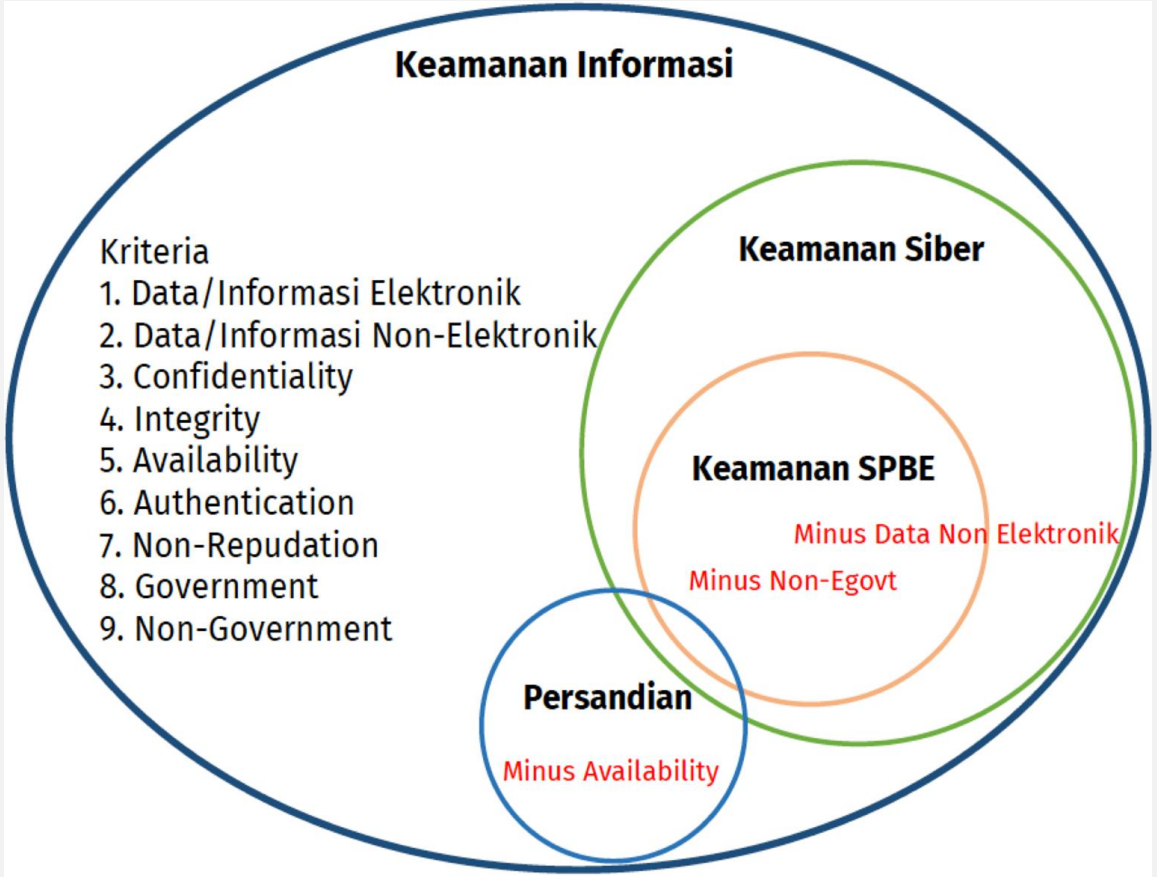
- To ensure the accuracy, consistency and completeness of the data
- Keeping the data from being modified or altered

Availability

- Data and resources are available to authorized users
- Attackers can execute the denial-of-service of attack if failed in the first two principles

modify from: websitesecuritystore.com

3. CLUSTER DOMAIN KEAMANAN



Gambar 1 Cluster Terminology

Tabel 1. Fokus Keamanan

Fokus/Prinsip Keamanan	Persandian	Keamanan Siber	Keamanan Informasi	Keamanan SPBE
Confidentiality	√	√	√	√
Integrity	√	√	√	√
Availability	-	√	√	√
Authentication	√	√	√	√
Non-Repudation	√	√	√	√

Tabel 2. Area Keamanan

Area	Persandian	Keamanan Siber	Keamanan Informasi	Keamanan SPBE
Data Elektronik	√	√	√	√
Data Non-Elektronik	√	-	√	-
Government	√	√	√	√
Non-eGovernment	√	√	√	-

KEAMANAN SPBE

Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE

[Pasal 1 angka 24, Perpres 95/2018]

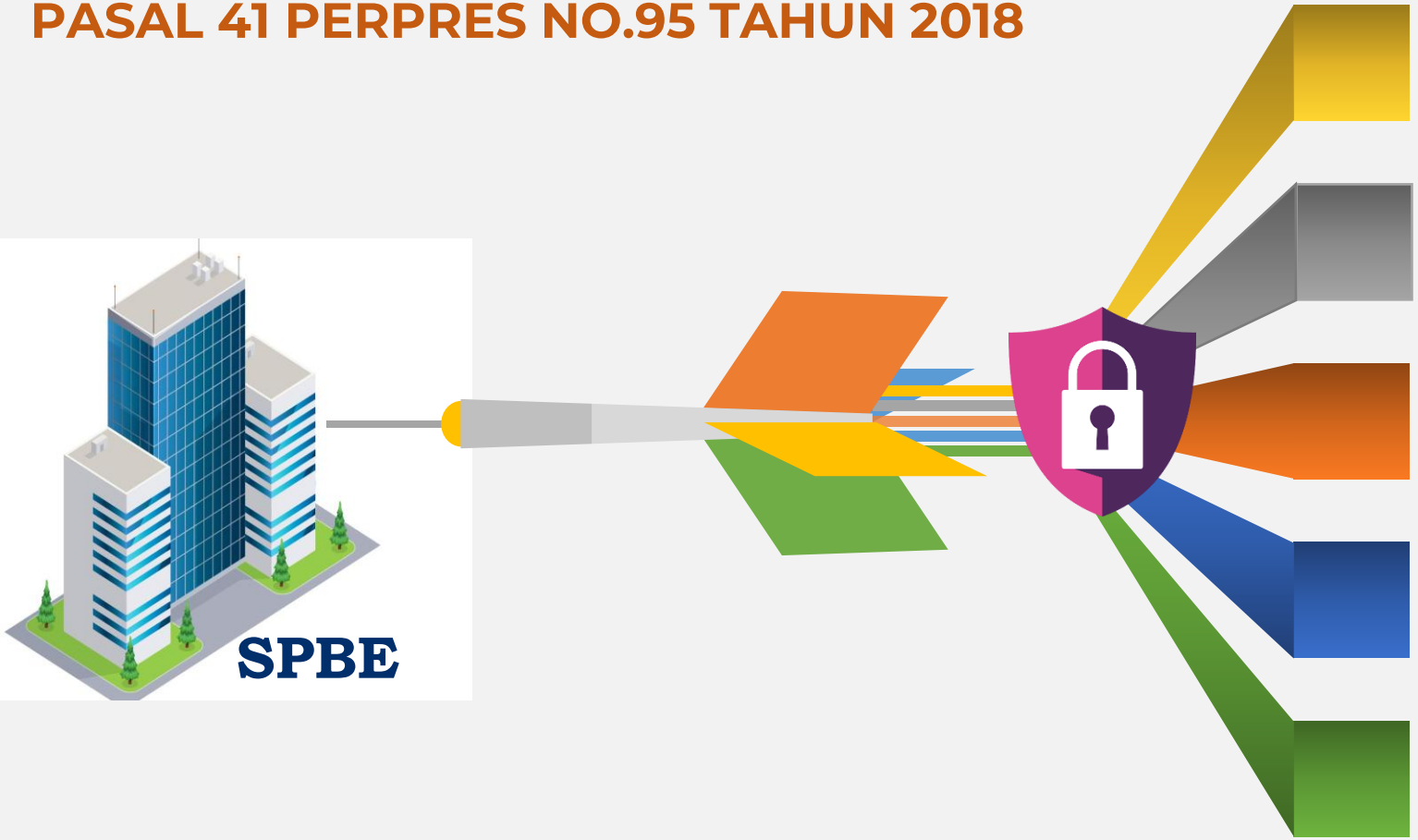
Keamanan sebagai salah satu prinsip SPBE

Merupakan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan *(nonrepudiation)* sumber daya yang mendukung SPBE.

[Pasal 2 ayat (8), Perpres 95/2018]

4. PRINSIP KEAMANAN SPBE

PASAL 41 PERPRES NO.95 TAHUN 2018



PENJAMINAN KERAHASIAAN

Penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan/enkripsi dan kriptografi.

KEUTUHAN

Pendeteksian modifikasi dan tanda tangan elektronik tersertifikasi.

KETERSEDIAAN

Penyediaan cadangan, perencanaan untuk menjamin data dan informasi dapat selalu diakses, dan pemulihan.

KEASLIAN

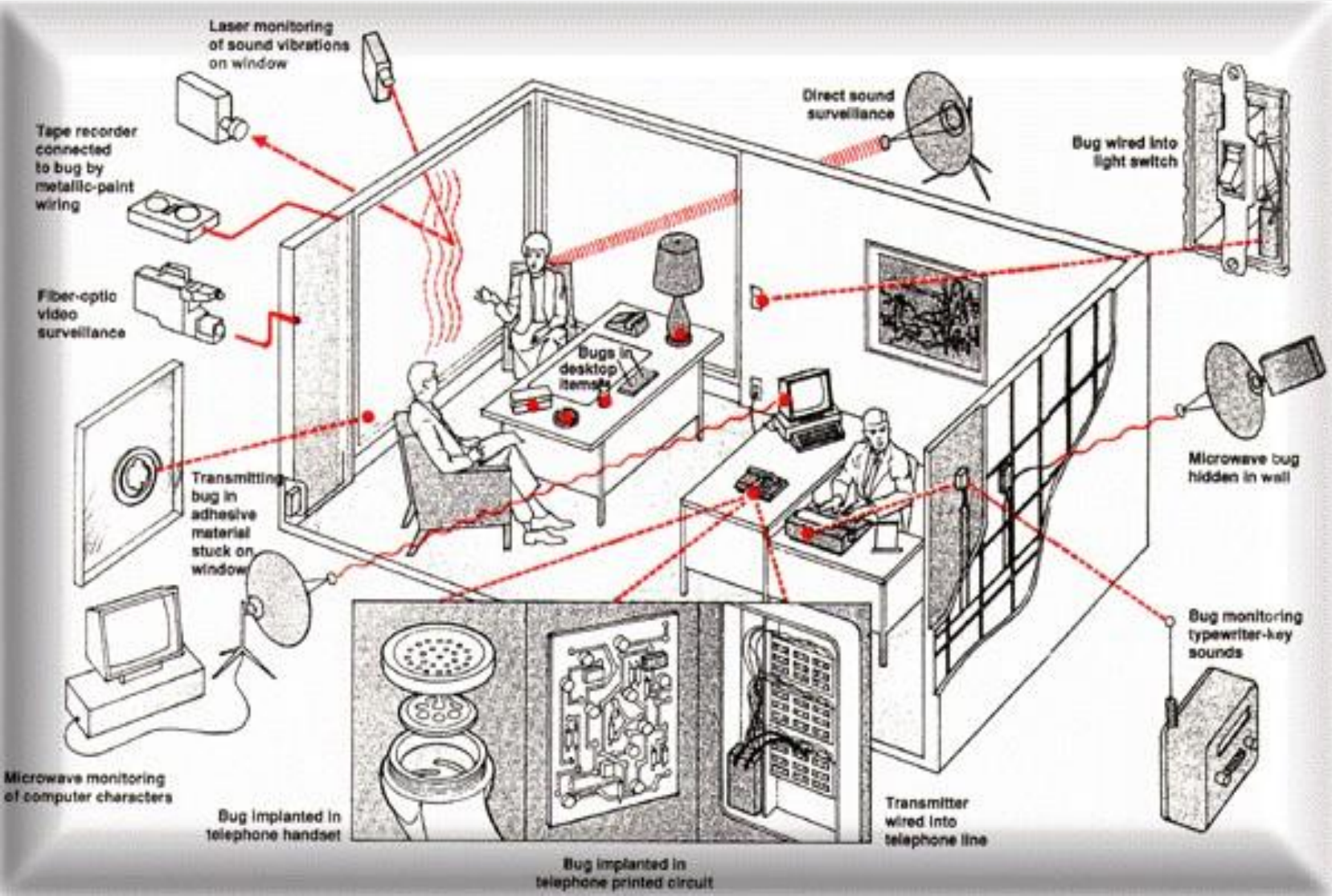
Penyediaan mekanisme verifikasi, validasi dan hush function.

KENIRSANGKALAN (NON-REPUDIATION)

Penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

5. Ilustrasi Risiko Keamanan SPBE

ILUSTRASI RISIKO ERA OLD VERSION



Berdasarkan ilustrasi risiko era old versioan tersebut, Domain keamanan apa yang harus diterapkan suatu Organisasi, apakah:

a. Keamanan Informasi;
b. Keamanan SPBE;
c. Persandian; dan/atau
d. Keamanan Siber.

ASET SPBE

SISTEM PENGHUBUNG LAYANAN

DATA DAN INFORMASI ELEKTRONIK

APLIKASI SPBE

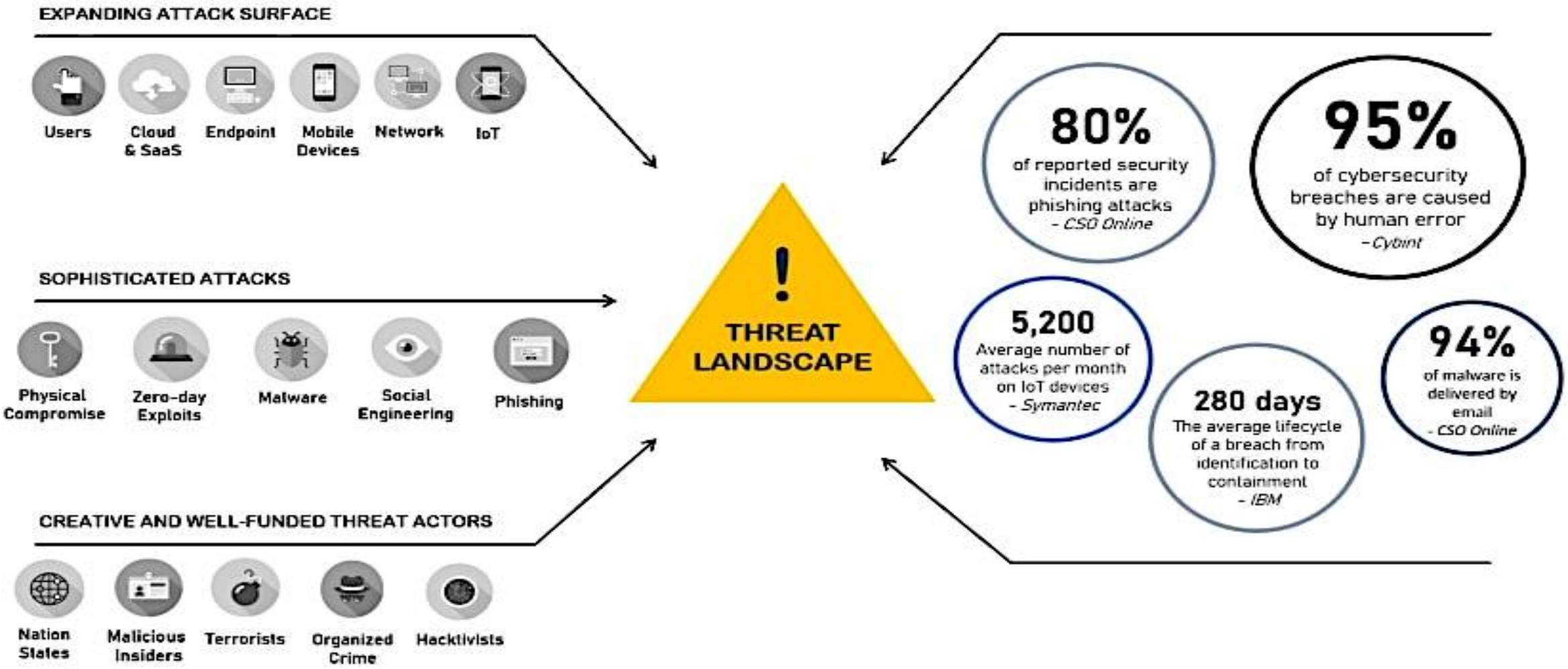
Web/Mobile

PUSAT DATA

JARINGAN INTRA

ANALOGI KONDISI SUBJEK DAN OBJEK | RISIKO KEAMANAN

RISIKO MAPPING KEAMANAN SPBE

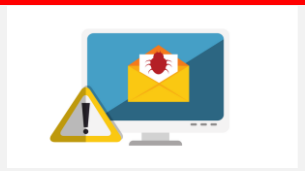


Adopt from : Businesstechweekly.com

ANCAMAN ERA SPBE / *E-GOVERNMENT*

ATTACK GOVERNMENT IT SYSTEM

TRUST & MANIPULATING PUBLIC OPINION

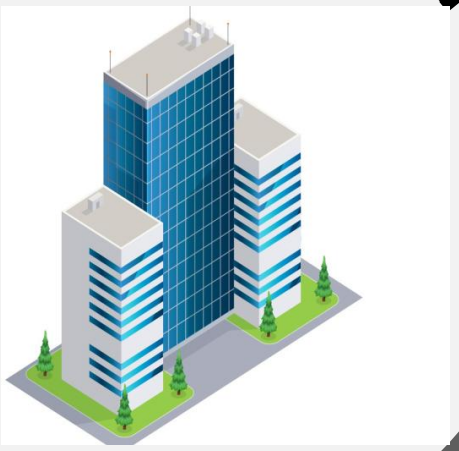


Malware & Ransomware

Denial of service

HOAX

Fake News



Phising Attack

Social Engineering

WEB DEFACEMENT

SQL Injection

SLOT GACOR

Contoh Serangan Defacement Judi Online pada Website Pemerintah dan Universitas

DKP PAPUA
https://dkp.papua.go.id › mposatu · Translate this page

MPO1221 💸 5 Daftar Bandar Situs Judi Online Terpercaya.

MPO1221 adalah salah satu situs slot gacor yang menggunakan server thailand dengan tingkat kemenangan member yang besar, dan memberikan RTP Slot setiap hari ...

JDIH KAB JENEPONTO
https://jdihn.jenepontokab.go.id › ... · Translate this page

paito papua

Kini situs PAITO **PAPUA** telah hadir permainan **slot gacor** maxwin tanpa daftar dan tanpa deposit, Cukup login disitus PAITO **PAPUA** dan langsung bisa bermain ...

mantra88
https://pafikotajayapura.org · Translate this page

MANTRA88: Situs Judi Slot Online Ga

... **GO**-PAY, DANA, LINK AJA & Bank Lokal Indonesia .. menjadi satu diantara game **slot gacor** ... **ID** saja. Apa

Pemerintah Kabupaten Sorong
https://sorongkab.go.id › Unduhan · Translate this page

PPID

... **Papua** Bar. 98415. **slot** demo · **slot gacor** · **slot** pulsa · sgp. +6285715100xxx. kominfokabsor@gmail.com. Tautan.

Inspektorat Provinsi Papua
https://inspektorat.papua.go.id › sej... · Translate this page

Sejarah - Inspektorat Provinsi Papua

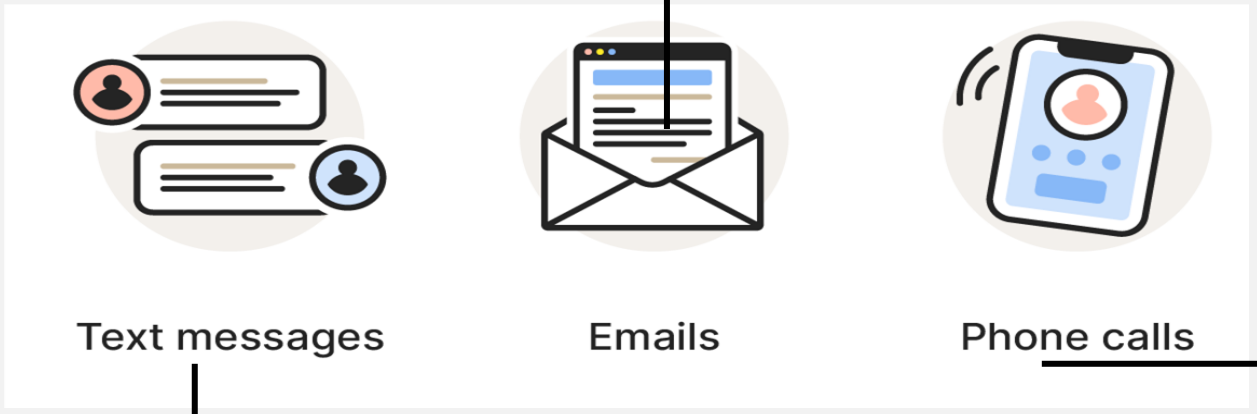
https://**slot-gacor**-mania.bookofraonlinespiele.org/ ... https://mbkm.fatek.untad.ac.id/**slot**-raffi-ahmad/ ... https://inspektorat.**papua.go.id**/wp-includes/certificates ...

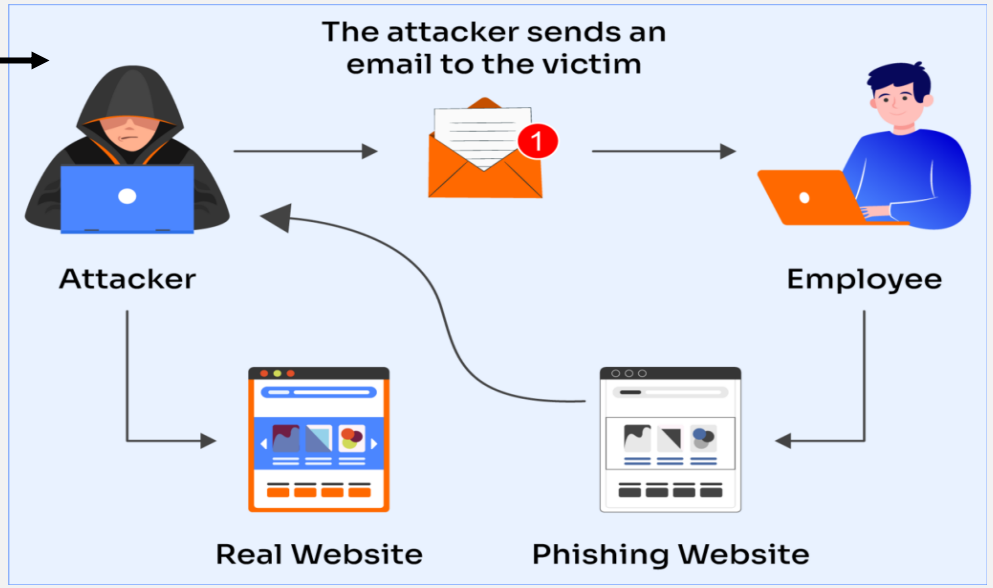
Universitas Papua (UNIPA)
https://s3il.pasca.unipa.ac.id · Translate this page

Program S3 Ilmu Lingkungan - Universitas Papua

https://**slot-gacor**-mania.bookofraonlinespiele.org/ · https://slotdana.bookofraonlinespiele.org/ · https://s2sipil.fatek.untad.**ac.id**/.tmb/**slot**-raffi-ahmad/ ...

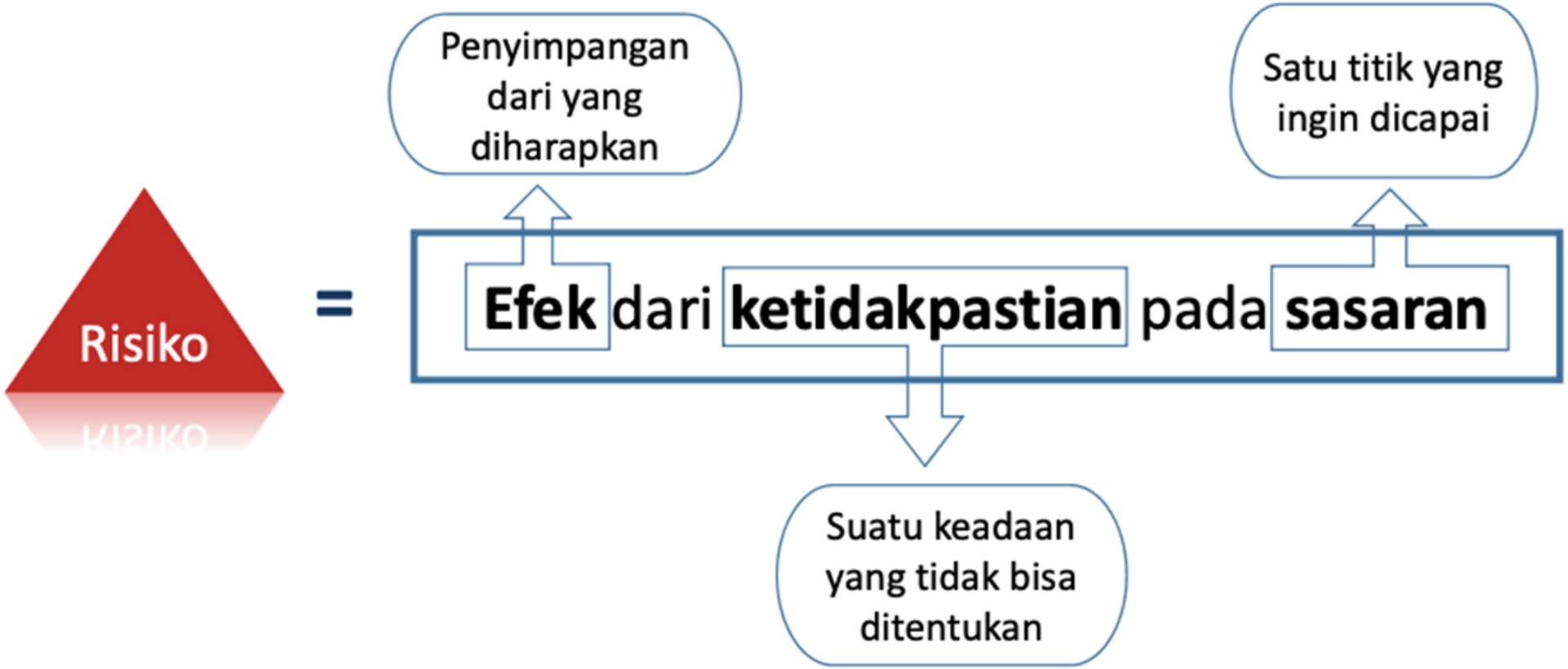
COMMON TYPE OF PHISHING ATTACK





6. Prinsip Manajemen Risiko dalam Keamanan SPBE

- Definisi Risiko



(*Effect of uncertainty on objectives* – ISO 31000)

PENGERTIAN MANAJEMEN RISIKO

Rangkaian kebijakan yang berisi kebijakan dan prosedur untuk meminimalisasi persitiwa yang merugikan organisasi.

Suatru proses terstruktur dalam mengidentifikasi, memetakan, mengukur, mengembangkan solusi penanganan risiko.

Pengelolaan fungsi mnanajemen dalam mengelola risiko. Di dalamnya termasuk aktivitas merencanakan, Menyusun dan mengorganisir kegiatan penanggulangan risiko

Sebuah proses mengawasi, mengelola dan mengambil keputusan gun amenghindari risiko kerugian pada sebuah organisasi.

MANAJEMEN RISIKO KEAMANAN SPBE

a. **Manajemen Risiko SPBE** adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE (Permenpan No. 5 Tahun 2020).

b. **Keamanan SPBE** adalah pengendalian keamanan yang terpadu dalam SPBE (Pasal 1/Perban No.4 Tahun 2021).

c. **Keamanan SPBE mencakup** penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE (Pasal 40/Perpres No.95 Tahun 2018).

d. **Manajemen risiko keamanan SPBE** adalah proses sistematis yang dilakukan untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko keamanan informasi dalam implementasi SPBE.

PRINSIP RISIKO

THE RISK CAN'T BE ZERO, BUT IT CAN BE REDUCED

Ruang lingkup keamanan informasi atau keamanan SPBE mengacu pada kenyataan bahwa risiko tidak dapat sepenuhnya dihilangkan, tetapi dapat diminimalisir hingga tingkat yang dapat diterima melalui langkah-langkah dan kontrol keamanan (mitigasi risiko) yang efektif.

Prinsip Manajemen Risiko dalam Keamanan SPBE

A. Risiko Tidak Dapat Di Nol-kan:

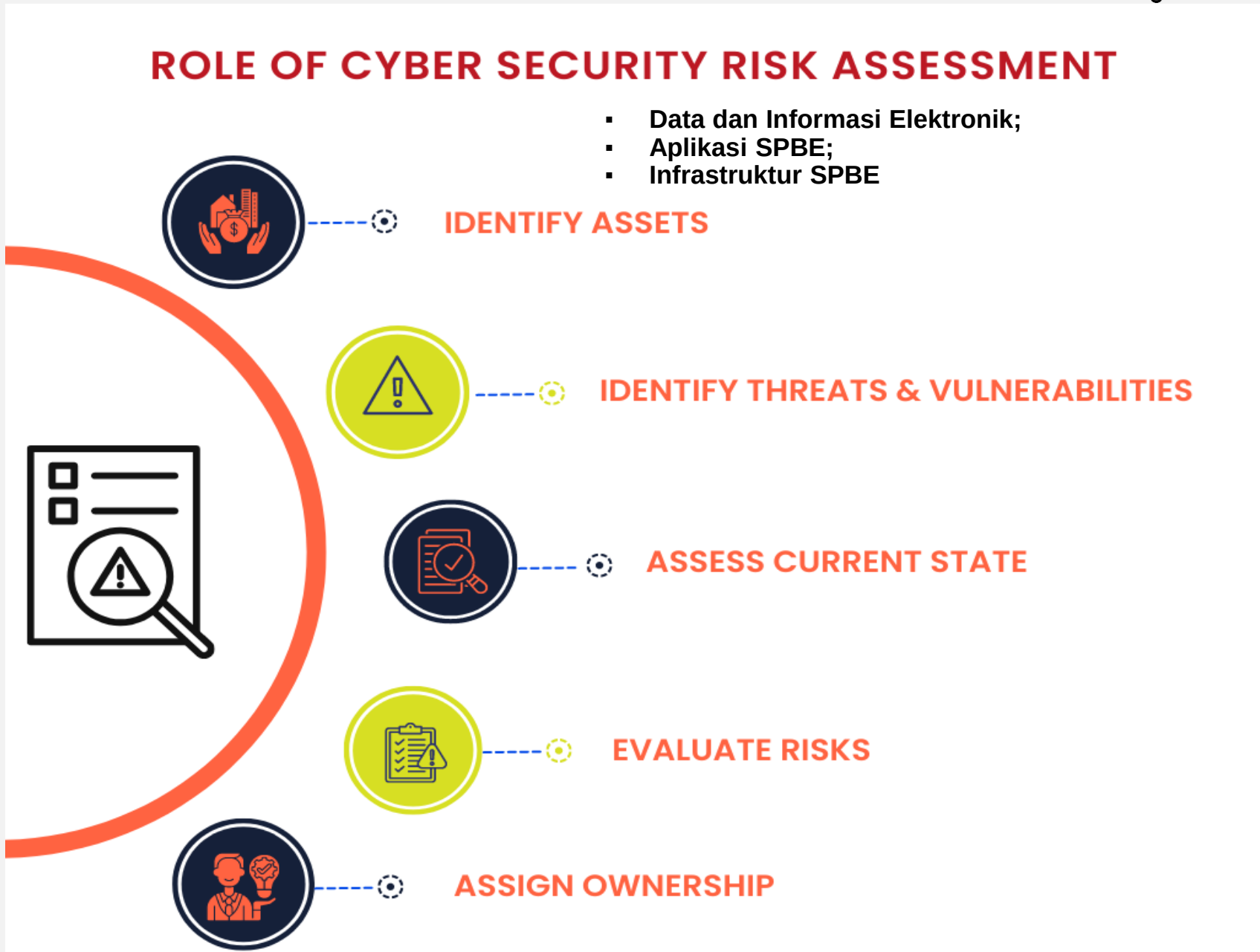
- **Kehadiran Ancaman**: Selalu ada ancaman potensial terhadap SPBE, seperti serangan siber, kesalahan manusia, kegagalan sistem, bencana alam, dll
- **Kerentanan Sistem**: Sistem Pemerintahan Berbasis Elektronik sebagaimana sistem eletronik selalu memiliki kerentanan yang bisa dieksploitasi oleh ancaman.
- **Evolusi Ancaman**: Ancaman keamanan terus berkembang dan berubah seiring waktu, menciptakan risiko baru bahkan setelah langkah-langkah keamanan diterapkan.

B. Pengurangan Risiko:

- **Implementasi Kontrol Keamanan:** Menggunakan langkah-langkah teknis, fisik, dan administratif untuk mengurangi kemungkinan dan dampak risiko. Contohnya termasuk penggunaan firewall, enkripsi data, kontrol akses, dan kebijakan keamanan.
- **Pemantauan dan Tinjauan Berkala:** Melakukan pemantauan dan peninjauan secara rutin untuk mendeteksi dan menanggapi ancaman baru serta memastikan kontrol keamanan yang ada tetap efektif.
- **Pelatihan dan Kesadaran :** Meningkatkan kesadaran pegawai terhadap praktik keamanan SPBE dan memberikan pelatihan yang diperlukan untuk mengurangi risiko yang berasal dari kesalahan manusia.

7. TAHAPAN MANAJEMEN RISIKO KEAMANAN SPBE

MANAJEMEN RISIKO KEAMANAN SPBE



TUGAS 1

Tugas Individu:

1. Identifikasi/Iventarisasi Aset SPBE yang ada dalam Organisasi Anda (Min 2 Aset);
2. Tentukan Kerentanan, Ancaman dan Potensi Risiko yang paling tinggi terjadi (Lakukan pada masing-masing Aset yang sudah diinventarisasi).

Tugas dikumpulkan dalam LMS dengan ketentuan :

1. Format tugas dalam bentuk file .pdf
2. Penamaan file : **T1_<NamaPeserta>.pdf**
3. Waktu Pengumpulan : Hari Ke-1, paling lambat pukul 22.00 WIB

Terima Kasih

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten
Harmonis Loyal Adaptif Kolaboratif

#JadiJagoanDigital Puspa Komdigi puspakomdigi