



IT SECURITY AWARENESS

Sebagai ASN /Organisasi dan Pribadi

Apakah layanan
/ Aplikasi SPBE
Anda, telah
lolos uji
keamanan ?





Permohonan Perekaman KTP Elektronik

Untuk sementara tidak dapat dilakukan, dikarenakan
alasan:

Dalam perbaikan sistem

 Pendaftaran

Terhenti Sementara, Layanan Antrian Online Dukcapil Aktif Kembali

BY **IRNI** ON 26 JUNI 2020 1260 DIBACA BERITA

G +1

Tweet

Like

WhatsApp



Jaringan Sistem OSS Down, Pelayanan DPMPTSP Kabupaten Bekasi Terganggu

1 min read

1 year ago admin

Hari ini (8/7/2019) DPMPTSP Kabupaten Bekasi menyampaikan pengumuman bahwa BKPM saat sedang melakukan pemeliharaan atau maintenance upgrade sistem OSS versi 1.0 ke versi 1.1. Akibatnya jaringan sistem OSS jadi tidak stabil atau down system. Kondisi ini menyebabkan loket pelayanan DPMPTSP untuk sementara dihentikan hingga sistem OSS kembali stabil. Atas gangguan layanan ini pihak DPMPTSP Kabupaten Bekasi menyampaikan permohonan maaf.



Banyak Temuan Pemesanan Data Kependudukan Palsu Jelang Pilkada, Polda Lampung Selidiki



Sabtu, 22 Februari 2020 270 Views Bandar Lampung

Data Pasien Positif Corona di Sulteng Bocor di Media Sosial, Pemda Pertanyakan



PALU POSO
Konten Redaksi Palu Poso



Risiko Ketika Data Pribadi Dicuri

CNN Indonesia | Kamis, 27/12/2018 07:25 WIB

Bagikan :  



Hati-hati 3 Situs Pemerintah Jepang Dipalsukan Untuk Mencuri Data

Kamis, 14 Mei 2020 17:48 WIB



TRUST



PALSU





4. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.

(1) Layanan SPBE terdiri atas:

- a. layanan administrasi pemerintahan berbasis elektronik; dan
- b. layanan publik|berbasis elektronik.

(1) Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 42 ayat (2) meliputi layanan yang mendukung kegiatan di bidang perencanaan, penganggaran, keuangan, pengadaan barang dan jasa, kepegawaian, kearsipan, pengelolaan barang milik negara, pengawasan, akuntabilitas kinerja, dan layanan lain sesuai dengan kebutuhan internal birokrasi pemerintahan.

APLIKASI UMUM

(1) Layanan publik berbasis elektronik sebagaimana dimaksud dalam Pasal 42 ayat (3) meliputi layanan yang mendukung kegiatan di sektor pendidikan, pengajaran, pekerjaan dan usaha, tempat tinggal, komunikasi dan informasi, lingkungan hidup, kesehatan, jaminan sosial, energi, perbankan, perhubungan, sumber daya alam, pariwisata, dan sektor strategis lainnya.

APLIKASI KHUSUS

	Integrasi Data dan Pengelolaan Portal Data Nasional	2019 - 2025
Pembangunan Sistem Keamanan Informasi Nasional	Manajemen Keamanan Informasi	2018 - 2020
	Teknologi Keamanan Informasi	2018 - 2025
	Budaya Keamanan Informasi	2018 - 2025
Pengembangan Teknologi Kecerdasan Buatan Untuk Pengambilan Keputusan yang Cepat dan Akurat	Kajian Teknologi Kecerdasan Buatan	2019 - 2025
	Penerapan Big Data Pemerintah	2019 - 2025
	Penerapan Kecerdasan Buatan	2019 - 2025

Prinsip

C.onfidentiality

I.ntegrity

A.vailability



Confidentiality (Kerahasiaan)



“ Informasi hanya bisa diakses oleh pihak yang berwenang ”

Integrity (Keutuhan)



“ Informasi hanya dapat **dirubah** oleh pihak yang berwenang ”

Availability (Ketersediaan)



“ Informasi **tersedia** saat dibutuhkan oleh pihak yang berwenang ”

Keaslian



“ Pihak yang terlibat dengan pertukaran informasi dapat **diidentifikasi** dengan benar dan adanya **jaminan** untuk keaslian identitas tersebut ”

Non Repudiation



“ Penerima informasi mampu **membuktikan** bahwa pengirim informasi benar-benar mengirimkan informasi tersebut ”

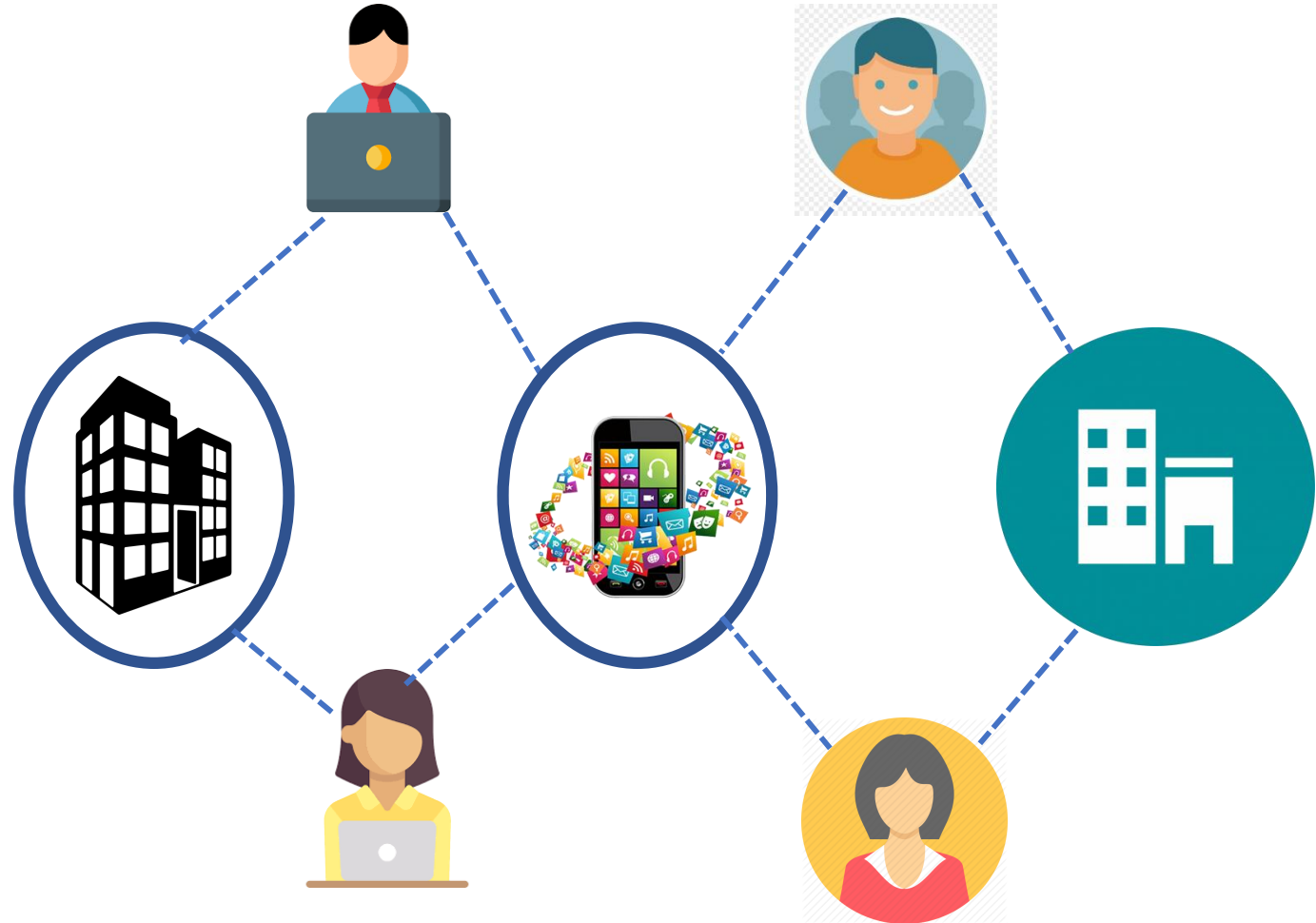


pastikan Keamanan **INFORMASI...**

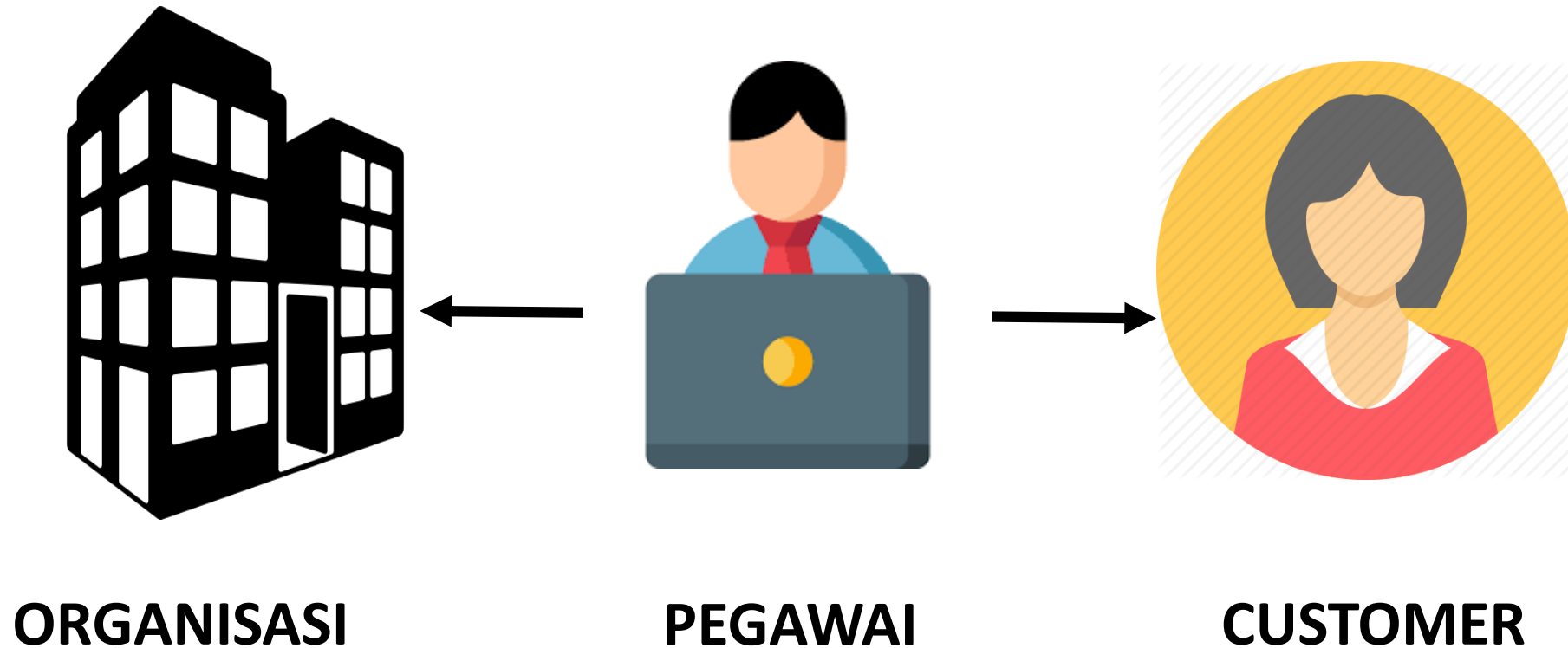
Kita mulai
darimana?

Dampak (Risiko / Value) Digital Transformasi

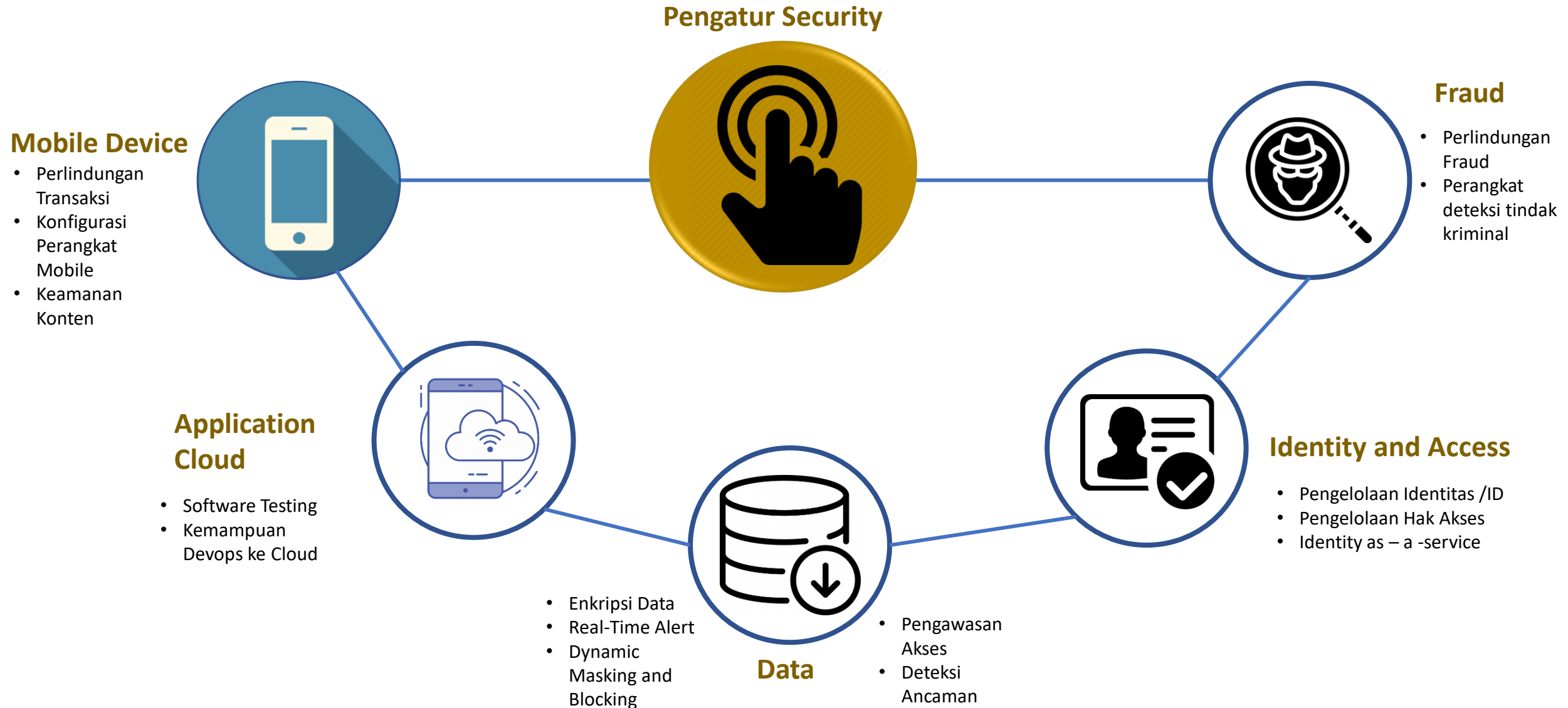
Semua terhubung dan terintegrasi (customer, pegawai dan organisasi)



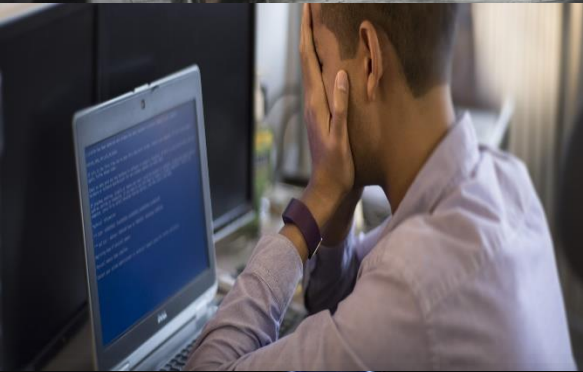
Pengamanan “End to End” Digital Transformasi



Cyber security “End to End” Digital Transformasi







RISIKO = ~~KETIDAKPASTIAN~~

**RISIKO = KETIDAKPASTIAN
UNTUK HAL YANG
PENTING**

**“DAMPAK DARI KETIDAKPASTIAN PADA
SUATU PENCAPAIAN SASARAN TERTENTU “**

[ISO 31000: 2009]

PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 5 TAHUN 2020
TENTANG
PEDOMAN MANAJEMEN RISIKO
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DUA DIMENSI RISIKO



KETIDAKPASTIAN

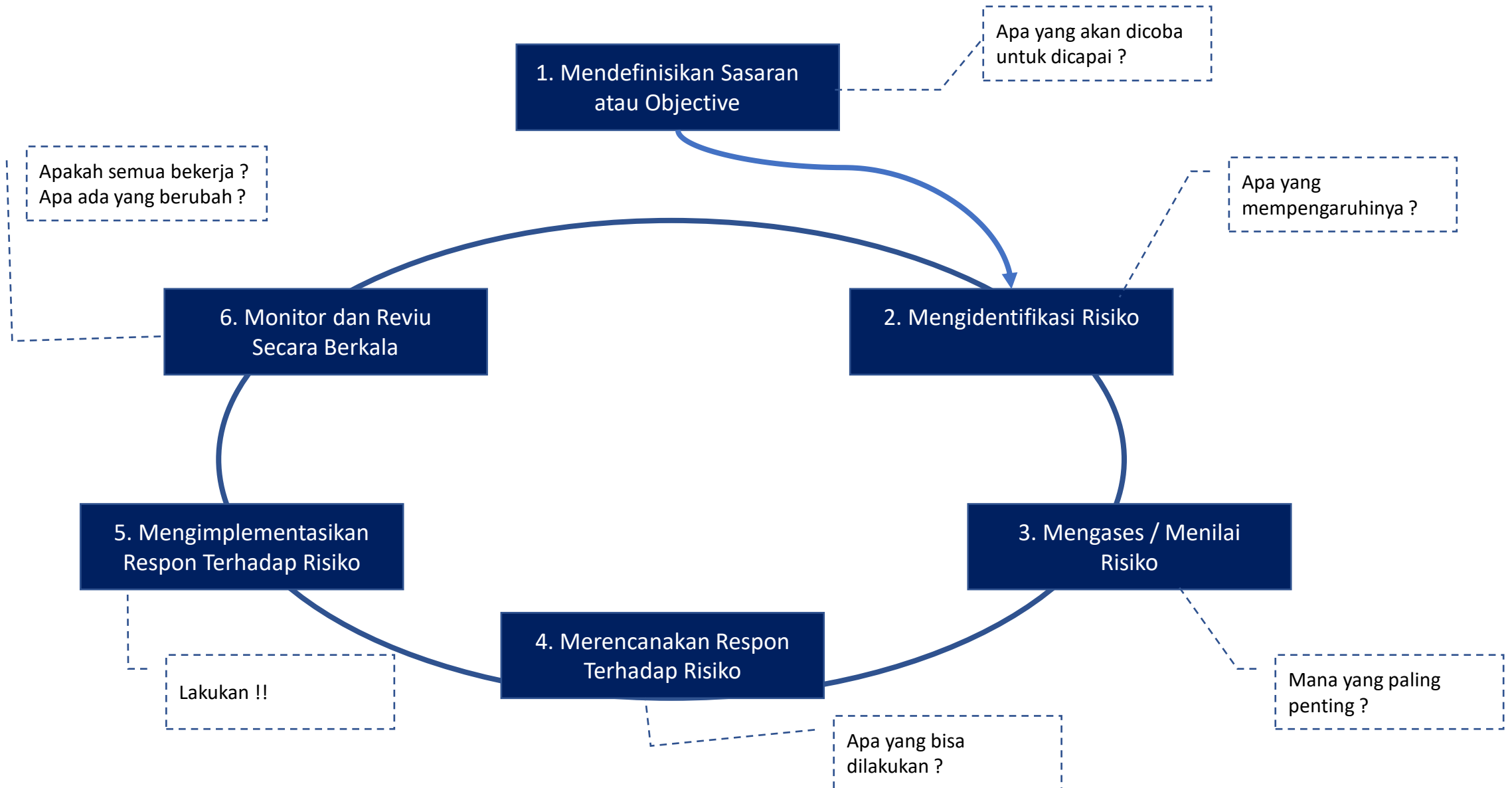
Sesuatu yang mungkin terjadi , namun
bisa jadi tidak terjadi

DAMPAK PADA SASARAN

Bisa berdampak positive , bisa juga
berdampak negative

Keduanya membutuhkan
pengelolaan secara proaktif

PROSES MANAJEMEN RISIKO



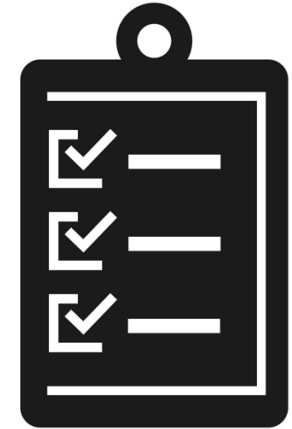
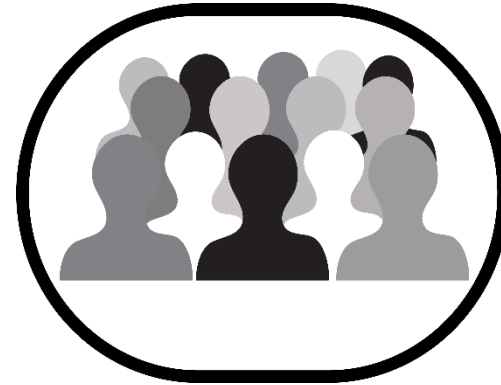
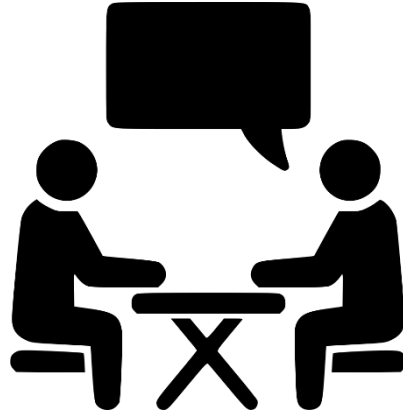
PROSES UTAMA RISIKO



IDENTIFIKASI RISIKO

CARA MENGIDENTIFIKASI

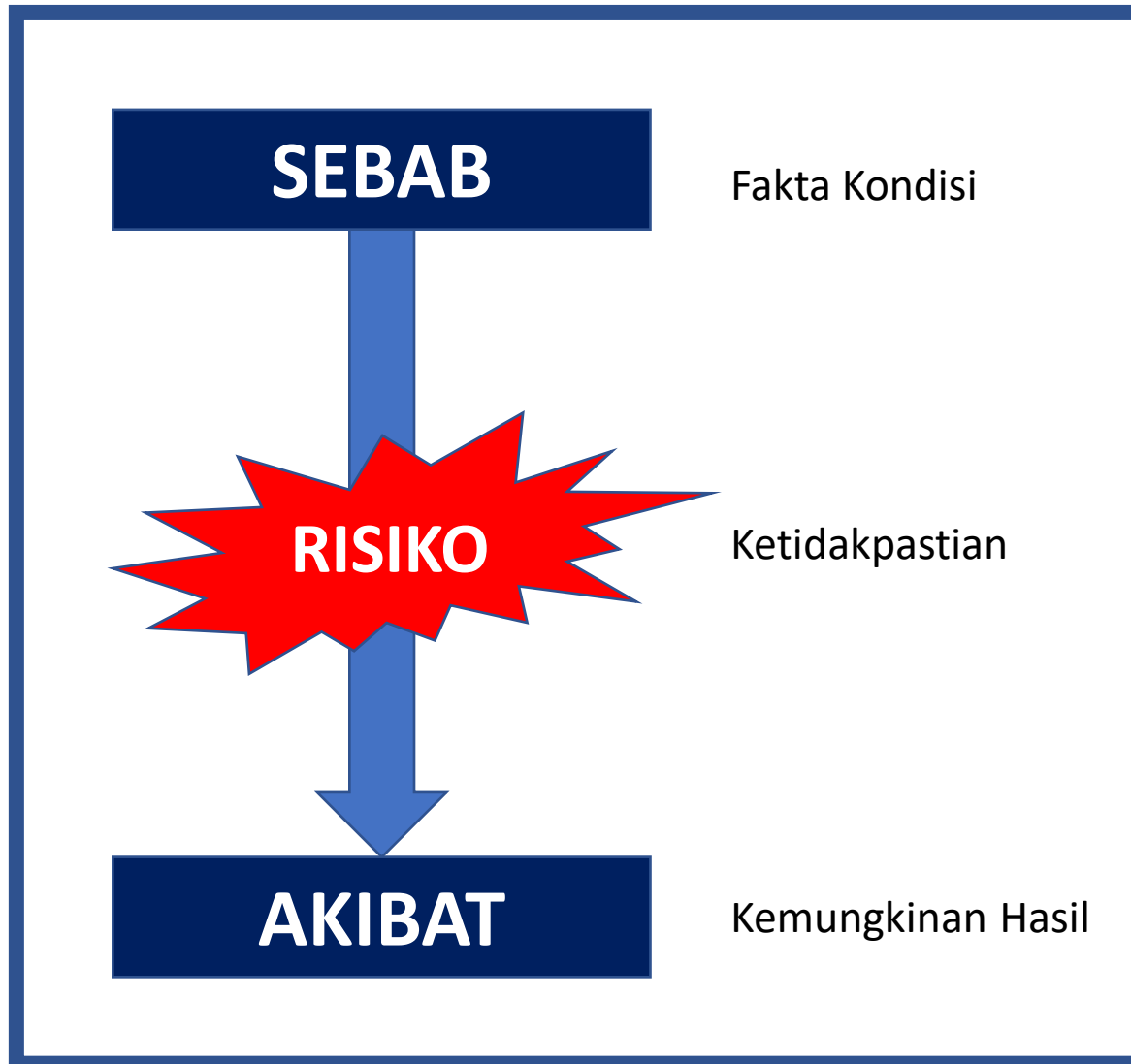
- Brainstorming / workshop
- Membuat check list
- Interview
- Kuesioner
- Pengamatan
- Asumsi



[RISIKO ATAU **BUKAN RISIKO**]



IDENTIFIKASI RISIKO



Struktur Bahasa pendefinisian Risiko sebaiknya memisahkan antara **sebab**, **risiko** dan **akibat /dampak**

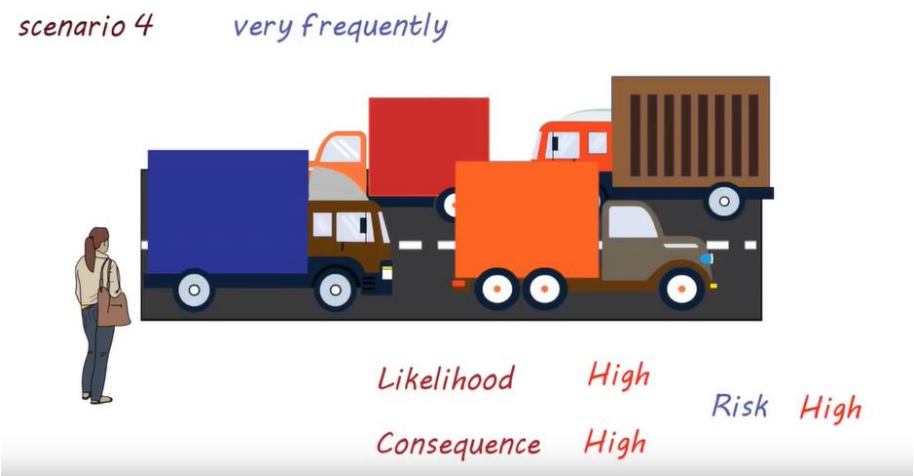
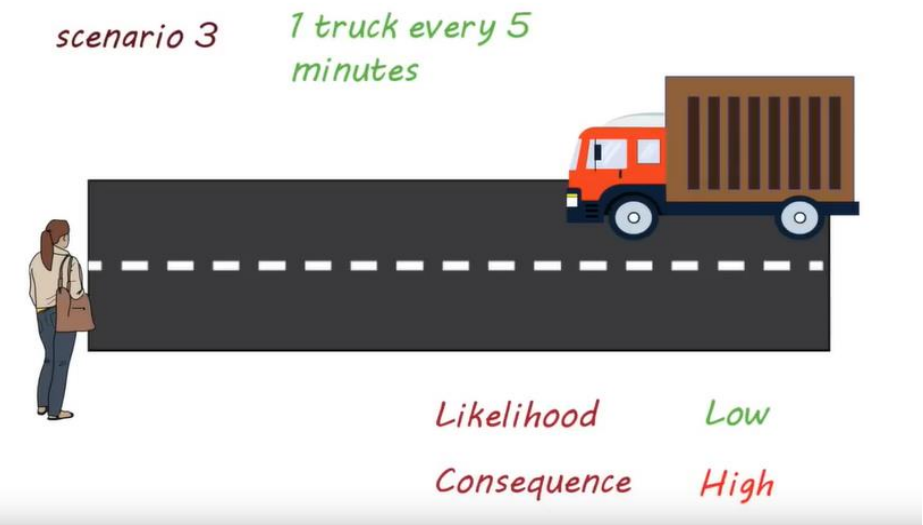
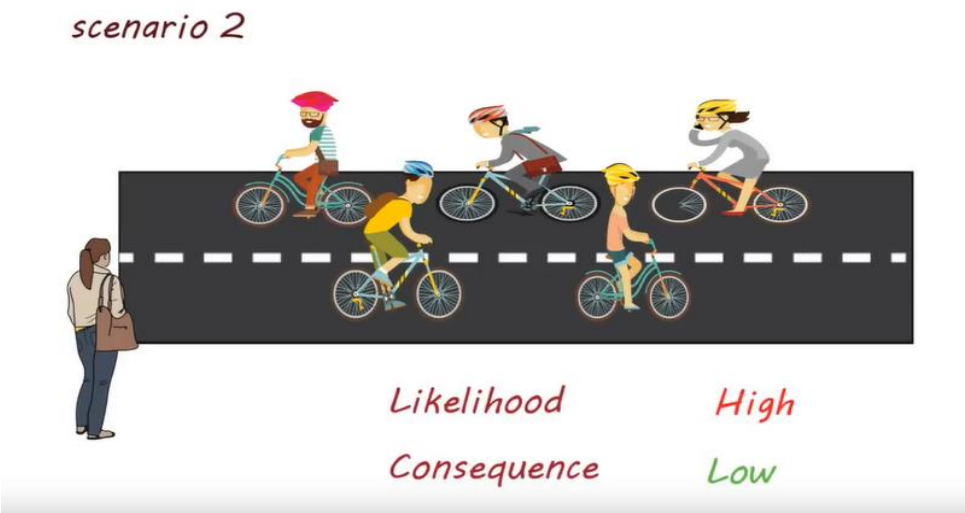
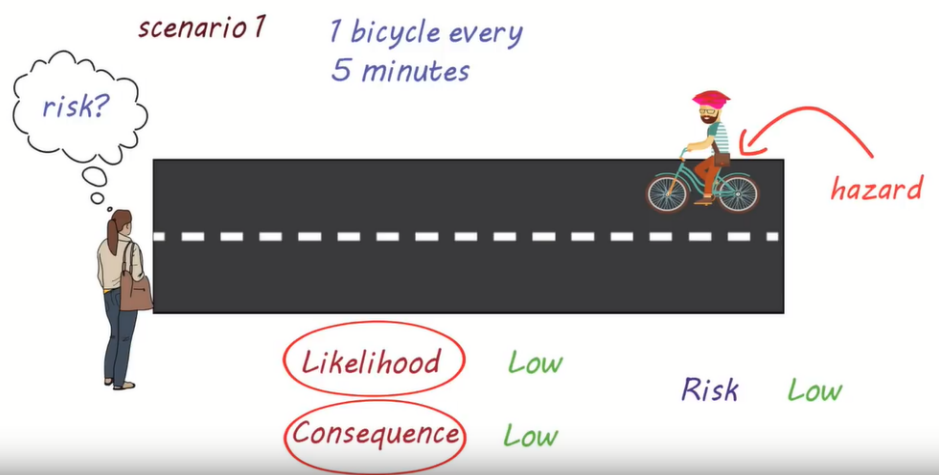
<1.kondisi terkini>, <2.kejadian tak terduga> dapat menyebabkan <3. dampak pada pencapaian sasaran>

“Hari ini cuaca cerah, namun tiba tiba mendung dan langsung hujan, sehingga kita tidak jadi bermain sepak bola di lapangan.”

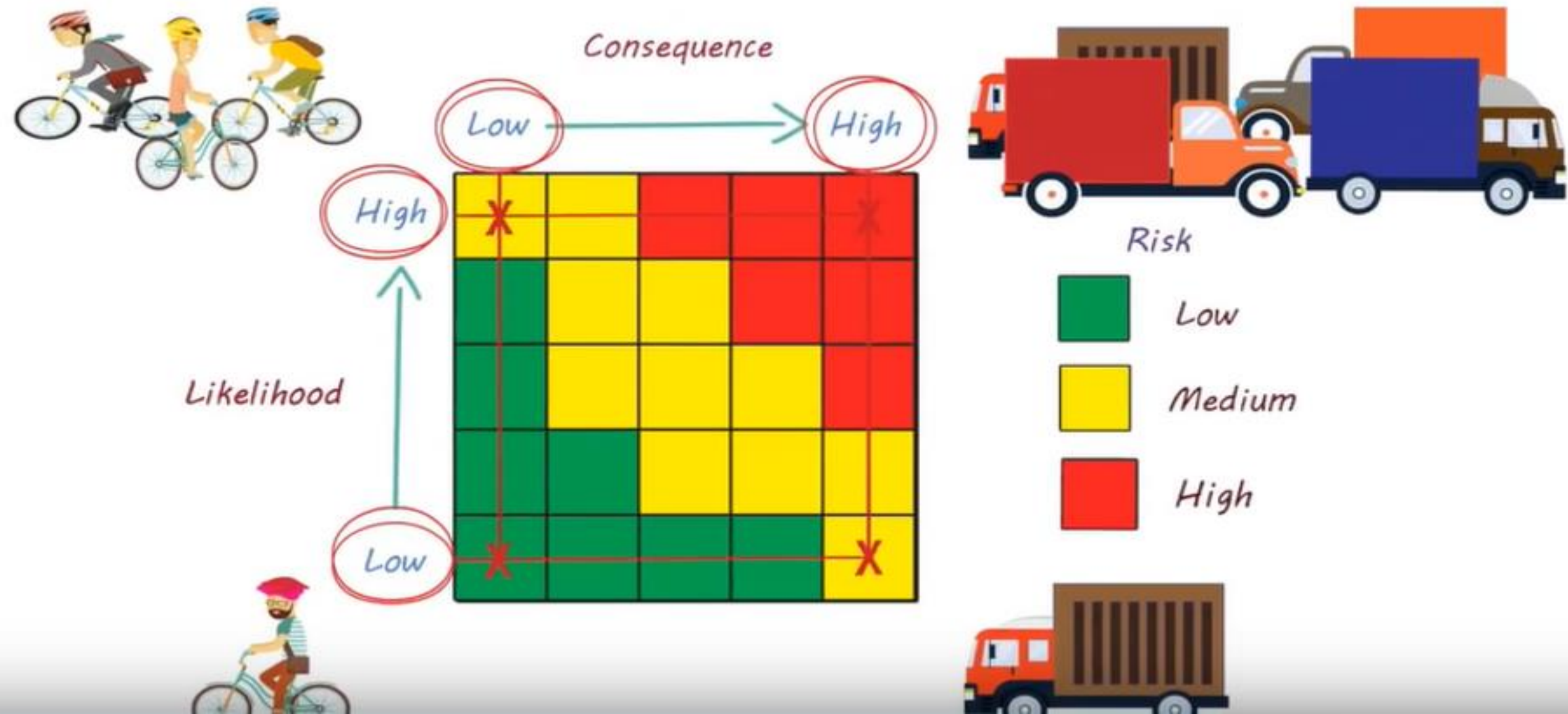
NILAI RISIKO



NILAI RISIKO



NILAI RISIKO



CONTOH NILAI RISIKO

DAMPAK

Deskripsi	Level	Kriteria Laba (Profit)	Kriteria Biaya Penanganan Insiden	Kriteria Pemenuhan <i>Requirement</i> Pelanggan
Dahsyat	5	Pengurangan laba > 1%	Biaya respon > Rp 150 juta	Pemenuhan requirement < 80%
Besar	4	0.5% < Pengurangan laba <= 1%	Rp 100 juta < Biaya respon <= Rp 150 juta	80% <= Pemenuhan requirement < 85%
Menengah / Sedang	3	0.3% < Pengurangan laba <= 0.5%	Rp 50 juta < Biaya respon <= Rp 100 juta	85% <= Pemenuhan requirement < 90%
Rendah	2	0.1% < Pengurangan laba <= 0.3%	Rp 20 juta < Biaya respon <= Rp 50 juta	90% <= Pemenuhan requirement < 95%
Sangat Rendah / Tidak Signifikan	1	Pengurangan laba <= 0.1%	Biaya respon <= Rp 20 juta	Pemenuhan requirement >= 95%

FREKUENSI

Deskripsi	Level	Kriteria Likelihood
Hampir Pasti Terjadi	5	Terjadi kejadian 4x atau lebih dalam setahun
Kemungkinan Besar Terjadi	4	Terjadi kejadian 3x dalam setahun
Kemungkinan Sedang Terjadi	3	Terjadi kejadian 2x dalam setahun
Kemungkinan Kecil Terjadi	2	Terjadi kejadian 1x dalam setahun
Jarang Terjadi	1	Terjadi kejadian kurang dari 1x dalam setahun

DAMPAK X FREKUENSI

CONTOH NILAI RISIKO

LIKELIHOOD						
	5	Sedang (5x1)	Tinggi (5x2)	Ekstrim (5x3)	Ekstrim (5x4)	Ekstrim (5x5)
	4	Sedang (4x1)	Tinggi (4x2)	Ekstrim (4x3)	Ekstrim (4x4)	Ekstrim (4x5)
	3	Rendah (3x1)	Sedang (3x2)	Tinggi (3x3)	Ekstrim (3x4)	Ekstrim (3x5)
	2	Rendah (2x1)	Sedang (2x2)	Sedang (2x3)	Tinggi (2x4)	Tinggi (2x5)
	1	Rendah (1x1)	Rendah (1x2)	Rendah (1x3)	Sedang (1x4)	Sedang (1x5)
		1	2	3	4	5
DAMPAK/KONSEKWENSI						

1-3

• RENDAH

4-6

• SEDANG

7-10

• TINGGI

11-25

• EKSTRIM

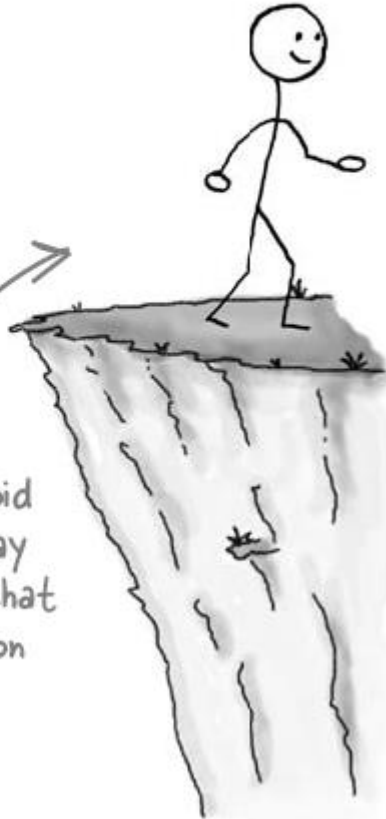
RESPON RISIKO

1

Avoid

The best thing that you can do with a risk is avoid it—if you can prevent it from happening, it definitely won't hurt your project.

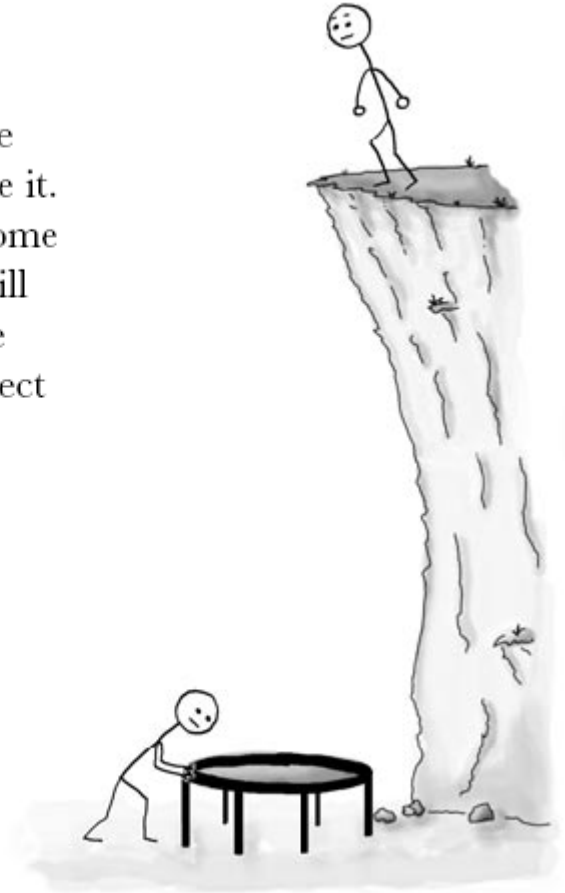
The easiest way to avoid this risk is to walk away from the cliff... but that may not be an option on this project.



2

Mitigate

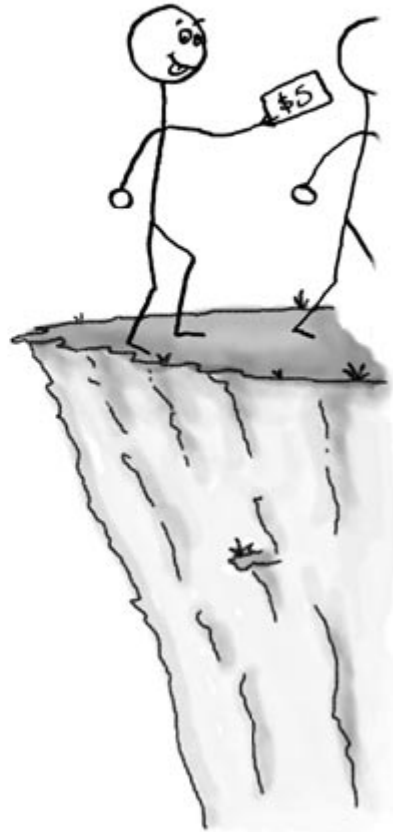
If you can't avoid the risk, you can mitigate it. This means taking some sort of action that will cause it to do as little damage to your project as possible.



RESPON RISIKO

3 Transfer

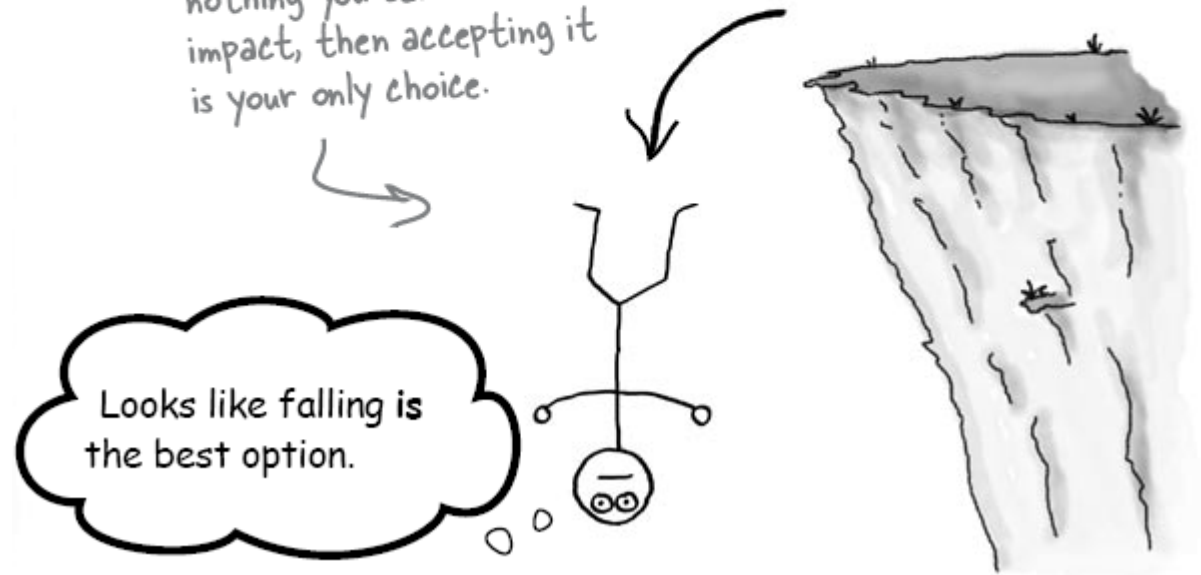
One effective way to deal with a risk is to pay someone else to accept it for you. The most common way to do this is to buy insurance.



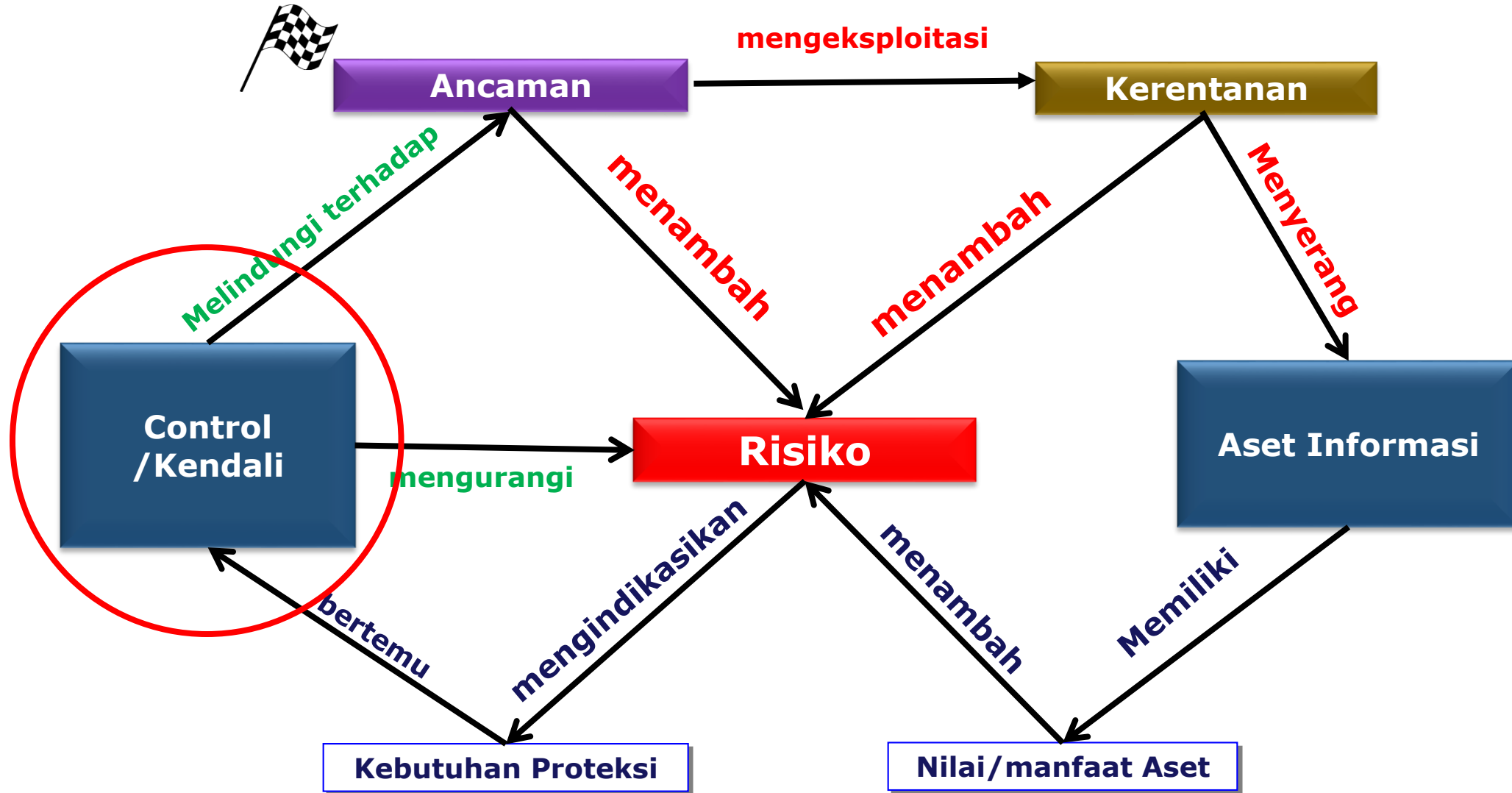
4 Accept

When you can't avoid, mitigate, or transfer a risk, then you have to accept it. But even when you accept a risk, at least you've looked at the alternatives and you know what will happen if it occurs.

If you can't avoid the risk, and there's nothing you can do to reduce its impact, then accepting it is your only choice.

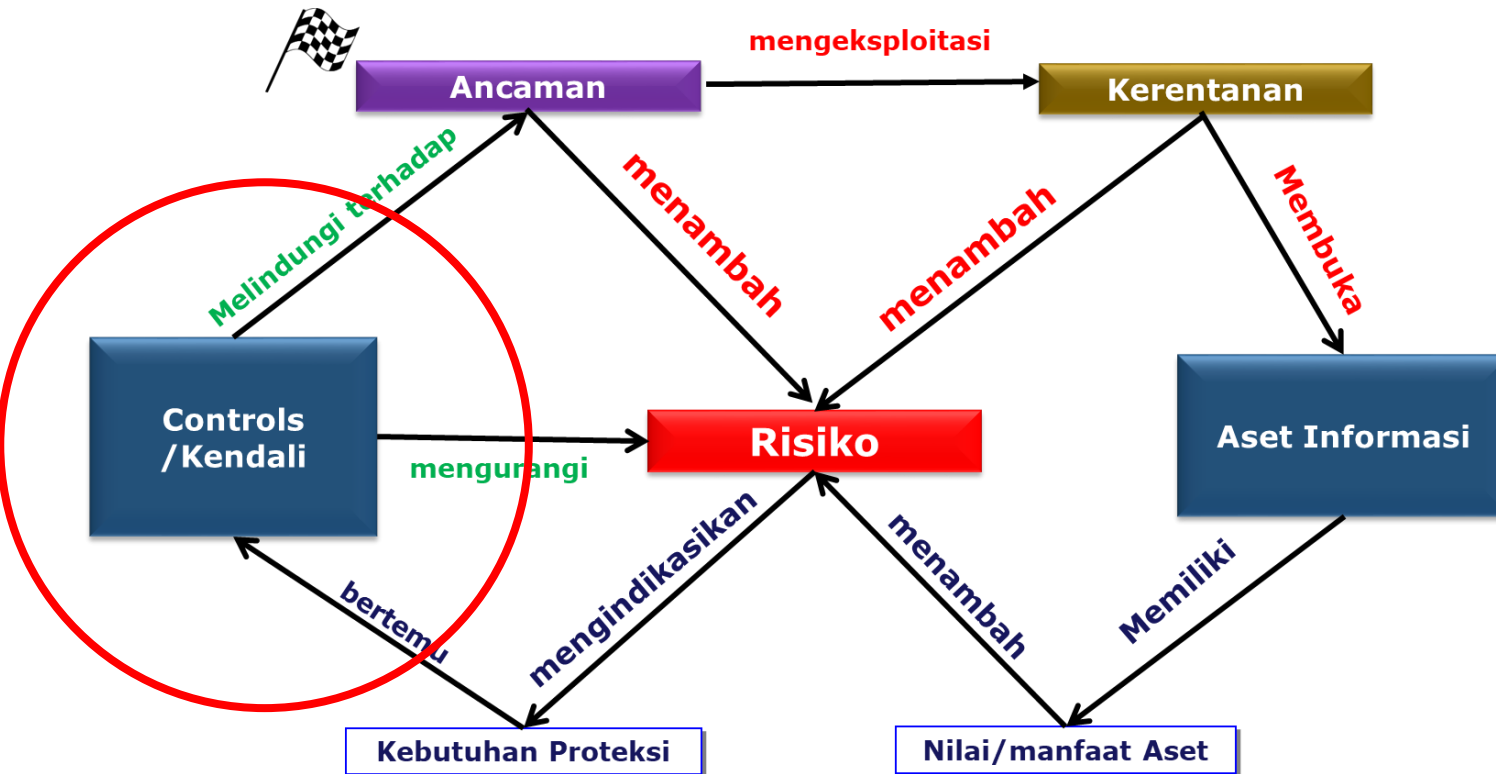


RESPON RISIKO



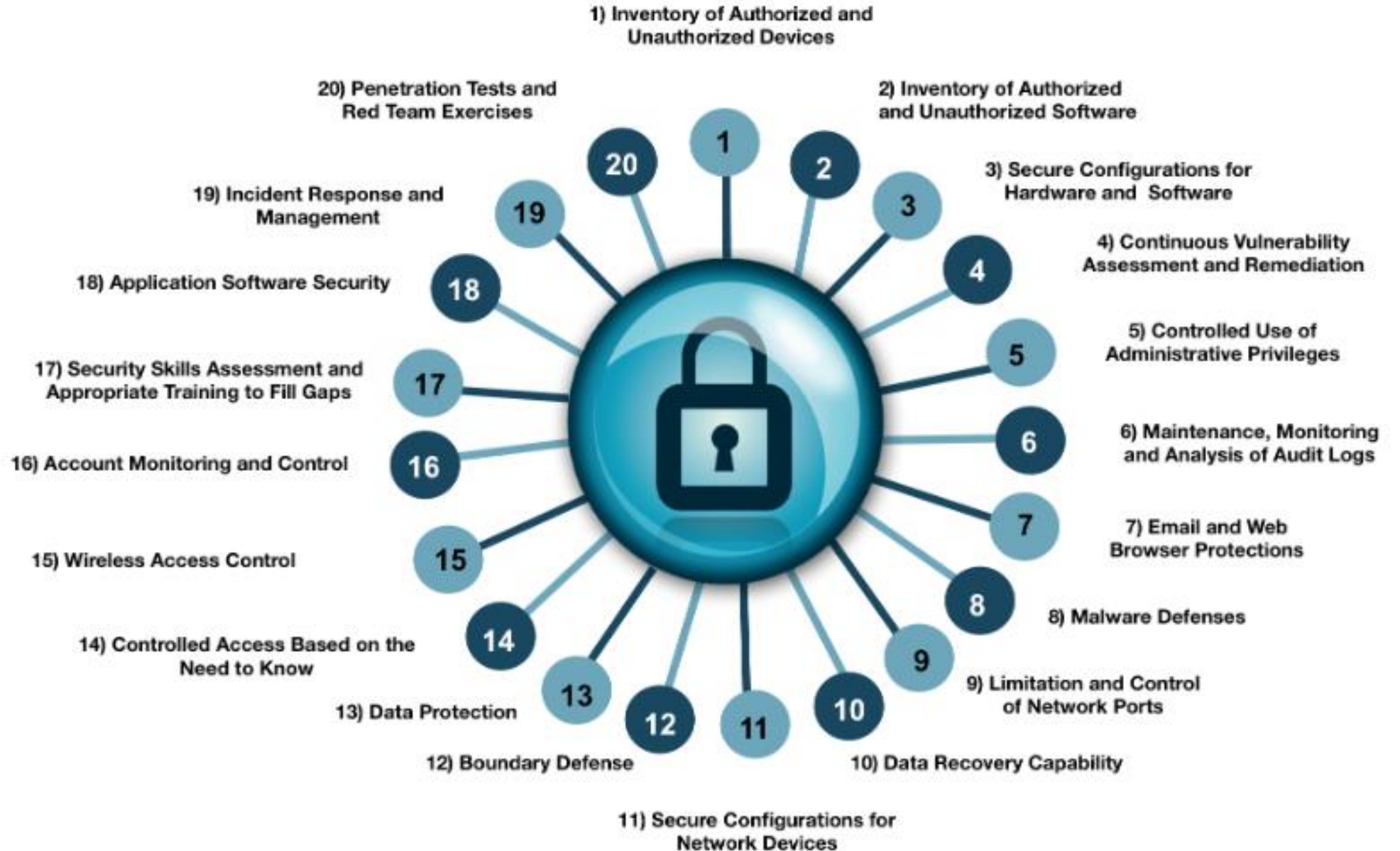
Control / Kendali : Aktivitas, prosedur atau mekanisme yang mengurangi risiko

Cyber security : Kendali (Controls)



Dengan
Ancaman
tadi ,
Kendali
atau
Controls nya
apa ?

CYBER SECURITY CONTROLS (CIS)



KUESIONER IDENTIFIKASI RISIKO

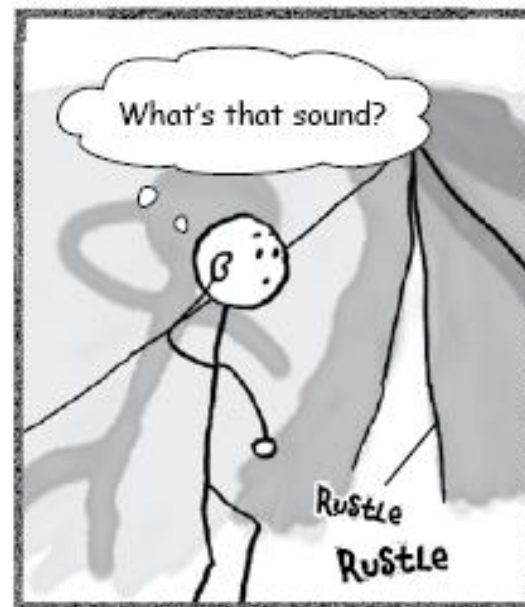


SKENARIO RISIKO

Formulir Aset TI Kritisal	
Direktorat	
Dinas	
Tanggal Pengisian Aset	
Nama Pengisi Aset	
Strategi, Tujuan dan Peran Dinas	
Deskripsi Proses Bisnis Inti Dinas (Core Business Process)	
Data/Informasi, Aplikasi, & Infrastruktur (Server, Storage, Jaringan) yang digunakan untuk mendukung Proses Bisnis Inti Dinas	1. 2. 3. 4. 5. 6. 7. 8. 9.
Tingkat Sensitivitas dan Tingkat Kritisalitas Data/Informasi yang digunakan untuk mendukung Proses Bisnis Inti Dinas	Tingkat Sensitivitas (Kerahasiaan) : PUBLIK / INTERNAL / RAHASIA Tingkat Kritisalitas (Keutuhan & Ketersediaan) : LOW / MEDIUM / HIGH
IT Service Dependency (Ketergantungan Layanan TI) lain yang penting untuk mendukung Proses Bisnis Inti Dinas	1. 2. 3. 4. 5. 6. 7. 8. 9.
Masalah TI yang menyebabkan Proses Bisnis Inti Dinas terganggu atau tidak berjalan dengan baik	1. 2. 3. 4. 5. 6. 7. 8.

Risk Register					
Part I—Ringkasan					
Kode Risiko					
Risk statement					
Tanggal Asesmen					
Level Risiko	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High		<input type="checkbox"/> Crisis
Risk response	<input type="checkbox"/> Accept	<input type="checkbox"/> Transfer	<input type="checkbox"/> Mitigate		<input type="checkbox"/> Avoid
Part II—Deskripsi					
Deskripsi Risiko					
Komponen Risiko	Actor	<input type="checkbox"/> Internal (staff, contractor) <input type="checkbox"/> External (Competitor, outsider, business partner, regulator, market)			
	Threat type	<input type="checkbox"/> Malicious <input type="checkbox"/> Accidental <input type="checkbox"/> Error		<input type="checkbox"/> Failure <input type="checkbox"/> Nature <input type="checkbox"/> External Requirement	
	Event	<input type="checkbox"/> Disclosure <input type="checkbox"/> Interruption <input type="checkbox"/> Modification <input type="checkbox"/> Theft <input type="checkbox"/> Destruction		<input type="checkbox"/> Ineffective design <input type="checkbox"/> Ineffective execution <input type="checkbox"/> Rules and Regulations <input type="checkbox"/> Inappropriate use	
	Asset/ resource	<input type="checkbox"/> People and Organization <input type="checkbox"/> Process <input type="checkbox"/> Infrastructure (facilities)		<input type="checkbox"/> IT Infrastructure <input type="checkbox"/> Information <input type="checkbox"/> Application	
	Timing	<input type="checkbox"/> Duration <input type="checkbox"/> Timing of occurrence (critical, non-critical) <input type="checkbox"/> Timing to detect			
Part III—Hasil Analisis					
Kemungkinan kejadian (<i>Likelihood</i>)	1	2	3	4	5
	RARE <input type="checkbox"/>	UNLIKELY <input type="checkbox"/>	POSSIBLE <input type="checkbox"/>	LIKELY <input type="checkbox"/>	CERTAIN <input type="checkbox"/>
Keterangan					
Dampak Bisnis	1	2	3	4	5
1. Kriteria Laba (<i>Profit</i>)					
Dampak Pengurangan Laba	INSIGNIFICANT <input type="checkbox"/>	MINOR <input type="checkbox"/>	MODERATE <input type="checkbox"/>	MAJOR <input type="checkbox"/>	CATASTROPHIC <input type="checkbox"/>
Keterangan					

1. Kriteria Biaya Penanganan Insiden (<i>Recovery</i>)					
Dampak biaya respon (dalam juta rupiah)	INSIGNIFICANT <input type="checkbox"/>	MINOR <input type="checkbox"/>	MODERATE <input type="checkbox"/>	MAJOR <input type="checkbox"/>	CATASTROPHIC <input type="checkbox"/>
Keterangan					
1. Kriteria Pemenuhan Requirement Pelanggan (<i>Service Level Agreement</i>)					
Dampak pemenuhan <i>requirement</i> dari pelanggan	INSIGNIFICANT <input type="checkbox"/>	MINOR <input type="checkbox"/>	MODERATE <input type="checkbox"/>	MAJOR <input type="checkbox"/>	CATASTROPHIC <input type="checkbox"/>
Keterangan					
Nilai akhir dampak bisnis (nilai terbesar) :					
Level Risiko	1–4 <input type="checkbox"/> Low	5–8 <input type="checkbox"/> MEDIUM	9–15 <input type="checkbox"/> HIGH	16–25 <input type="checkbox"/> CRISIS	
Part IV—Response					
Risk response	<input type="checkbox"/> Accept	<input type="checkbox"/> Transfer	<input type="checkbox"/> Mitigate	<input type="checkbox"/> Avoid	
Keterangan					
Deskripsi Respon / Control	Response Action Plan			Domain Annex A Control	
	1.				
	1.				
	1.				
	1.				
	1.				

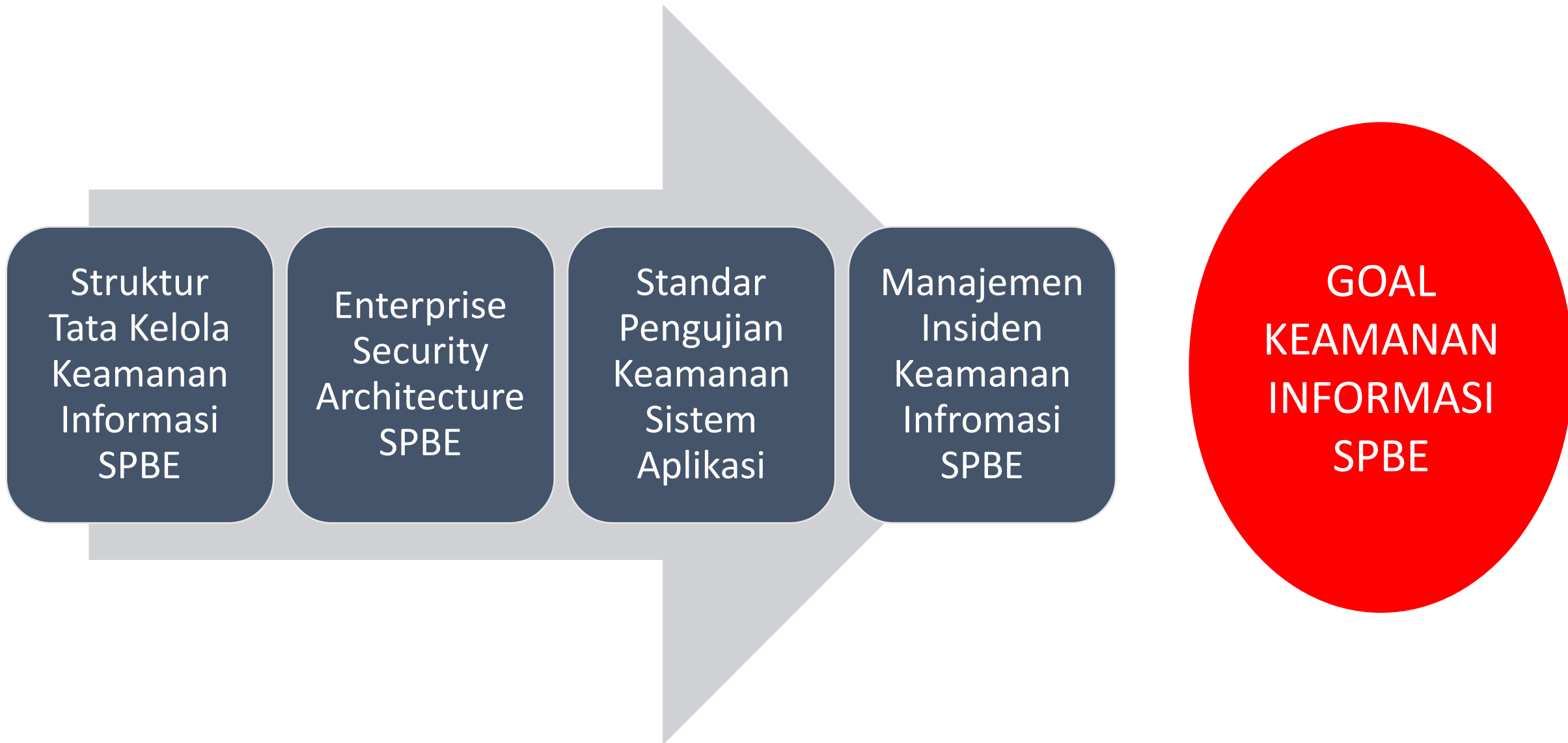








PERENCANAAN STRATEGIS KEAMANAN INFORMASI SPBE



Common Vulnerability Scoring System (CVSS 3)

LOW

MEDIUM

HIGH

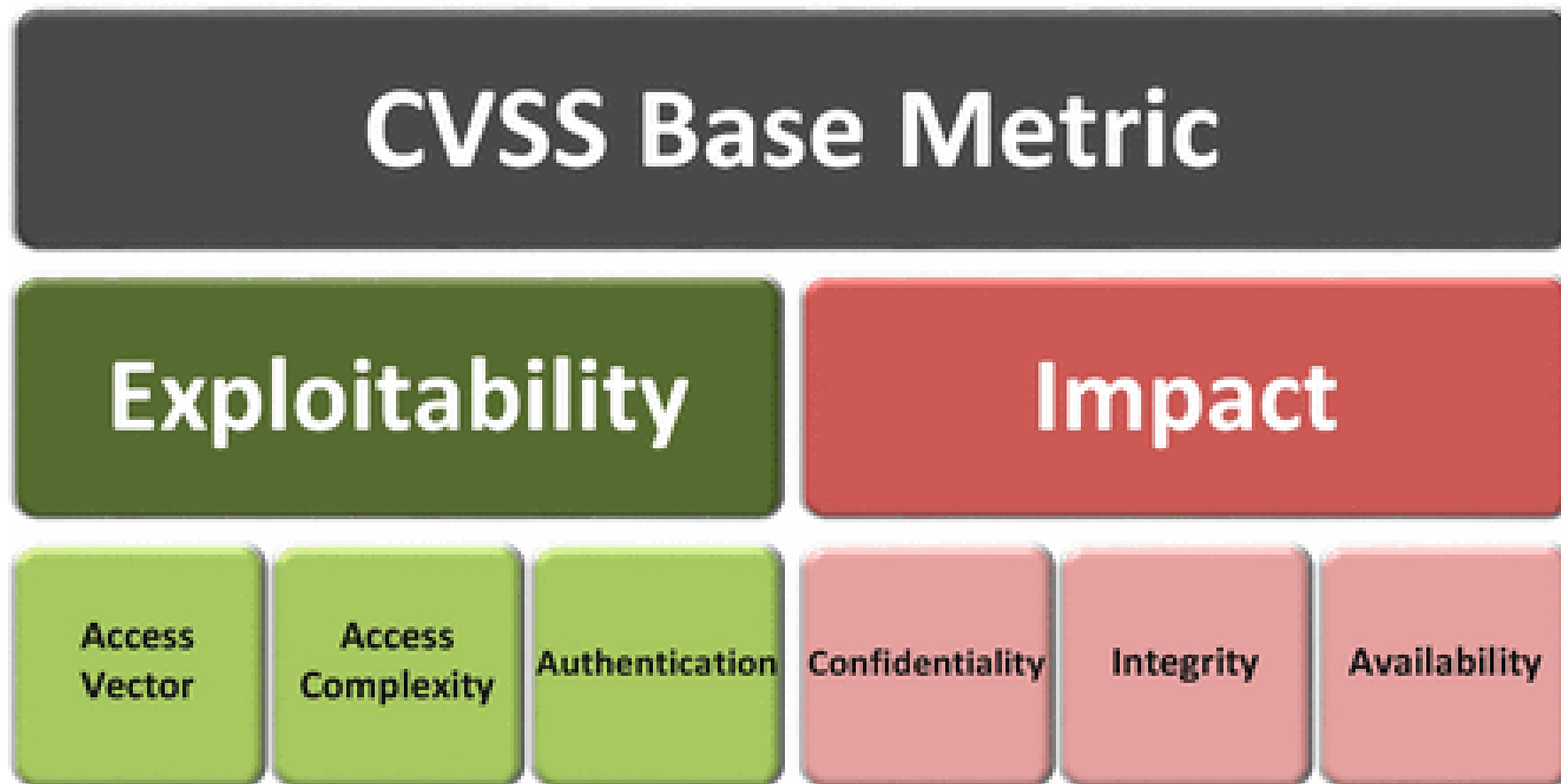
CRITICAL

Membantu Pemda untuk menilai dan memprioritaskan proses pengelolaan **kerentanan** secara tepat. Ketika terdapat hasil dengan kategori “**Tinggi**” atau **High**, maka secara otomatis aplikasi / layanan tersebut dinyatakan **tidak lulus ujian**



Common Vulnerability Scoring System

CVSS 3





EXPLOITABILITY

AV (ACCESS VECTOR)

Menunjukkan bagaimana sebuah **kerentanan**
/ vulnerability dapat di eksploitasi

Value	Description	Score
Local (L)	The attacker must either have physical access to the vulnerable system (e.g. firewire attacks) or a local account (e.g. a privilege escalation attack).	0.395
Adjacent Network (A)	The attacker must have access to the broadcast or collision domain of the vulnerable system (e.g. ARP spoofing , Bluetooth attacks).	0.646
Network (N)	The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service)	1.0

(AC) ACCESS COMPLEXITY

Menunjukkan seberapa mudah atau susah melakukan exploitasi terhadap kerentanan yang ditemukan

Value	Description	Score
High (H)	Specialised conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people.	0.35
Medium (M)	There are some additional requirements for the attack, such as a limit on the origin of the attack, or a requirement for the vulnerable system to be running with an uncommon, non-default configuration.	0.61
Low (L)	There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.	0.71

(AU) AUTHENTICATION

Menunjukkan **berapa kali** penyerang harus melakukan otentifikasi ke target untuk meng
exploitasi

Value	Description	Score
Multiple (M)	Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.	0.45
Single (S)	The attacker must authenticate once in order to exploit the vulnerability.	0.56
None (N)	There is no requirement for the attacker to authenticate.	0.704



impact

CONFIDENTIALITY (C)

Dampak pada **kerahasiaan data** yang diolah oleh sistem

Value	Description	Score
None (N)	There is no impact on the confidentiality of the system.	0.0
Partial (P)	There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.	0.275
Complete (C)	There is total information disclosure, providing access to any / all data on the system. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.	0.660

Integrity (I)

Dampak pada **integritas sistem** yang dieksploitasi.

Value	Description	Score
None (N)	There is no impact on the integrity of the system.	0.0
Partial (P)	Modification of some data or system files is possible, but the scope of the modification is limited.	0.275
Complete (C)	There is total loss of integrity; the attacker can modify any files or information on the target system.	0.660

Availability (A)

Dampak pada **ketersediaan sistem**. Serangan yang menghabiskan bandwidth jaringan, *processor cycles*, memori atau sumber daya lainnya mempengaruhi ketersediaan sistem

Value	Description	Score
None (N)	There is no impact on the availability of the system.	0.0
Partial (P)	There is reduced performance or loss of some functionality.	0.275
Complete (C)	There is total loss of availability of the attacked resource.	0.660



Security Awareness sebagai pribadi

HO

Handling dan Respon

AX





Orang mudah percaya informasi yang salah

Penyebaran fakta (kebenaran) untuk mempengaruhi sekarang lebih sulit dibanding masa-masa sebelumnya

KONTEN SEBAGAI SENJATA



Propaganda berbasis perilaku

Psikologi propaganda yang memanfaatkan otomasi manipulasi emosi dan analisa psikometrik



Targeting & retargeting

Mesin pintar yang mengincar sisi kepribadian target untuk menciptakan pergeseran opini individu dan publik

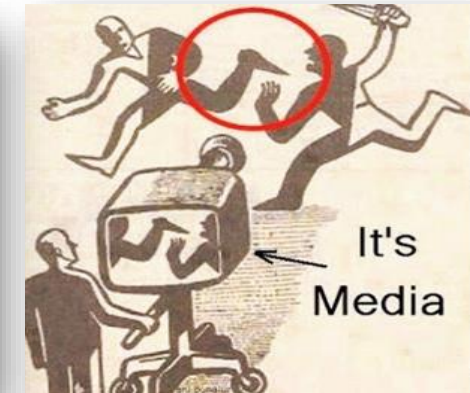
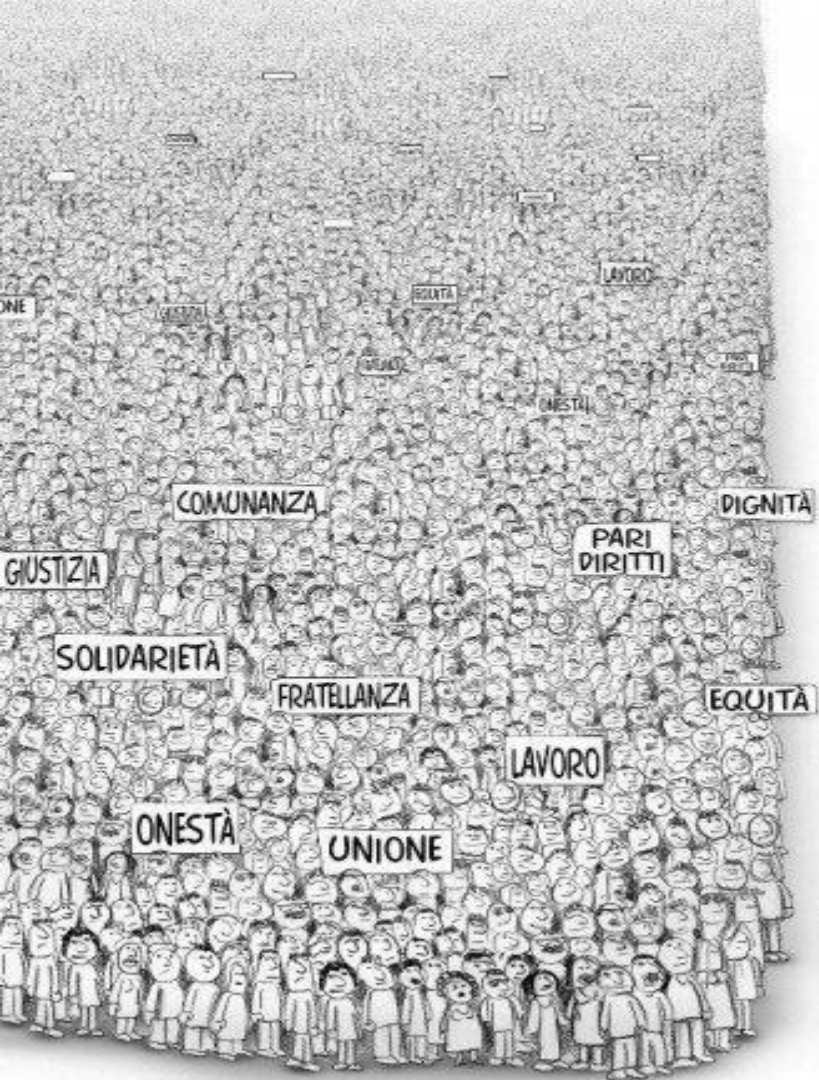


API, AI & MACHINE LEARNING

Konten yang anda sukai mengikuti anda kemanapun anda berkeliling di dunia maya/web

Media Framing

Diadopsi Di dunia maya dengan cepat & Fasih



Citizen Journalists

Liputan media mainstream dihasilkan langsung dari konten media sosial

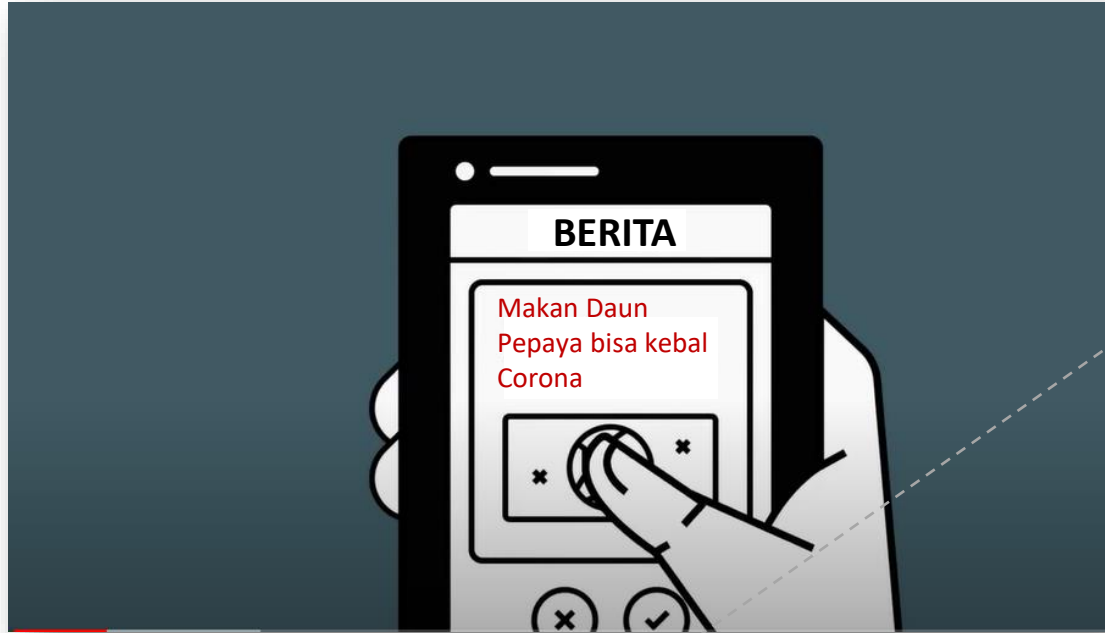
Kebenaran vs realita

Narasi online didominasi oleh siapa yang memiliki SEO terbaik

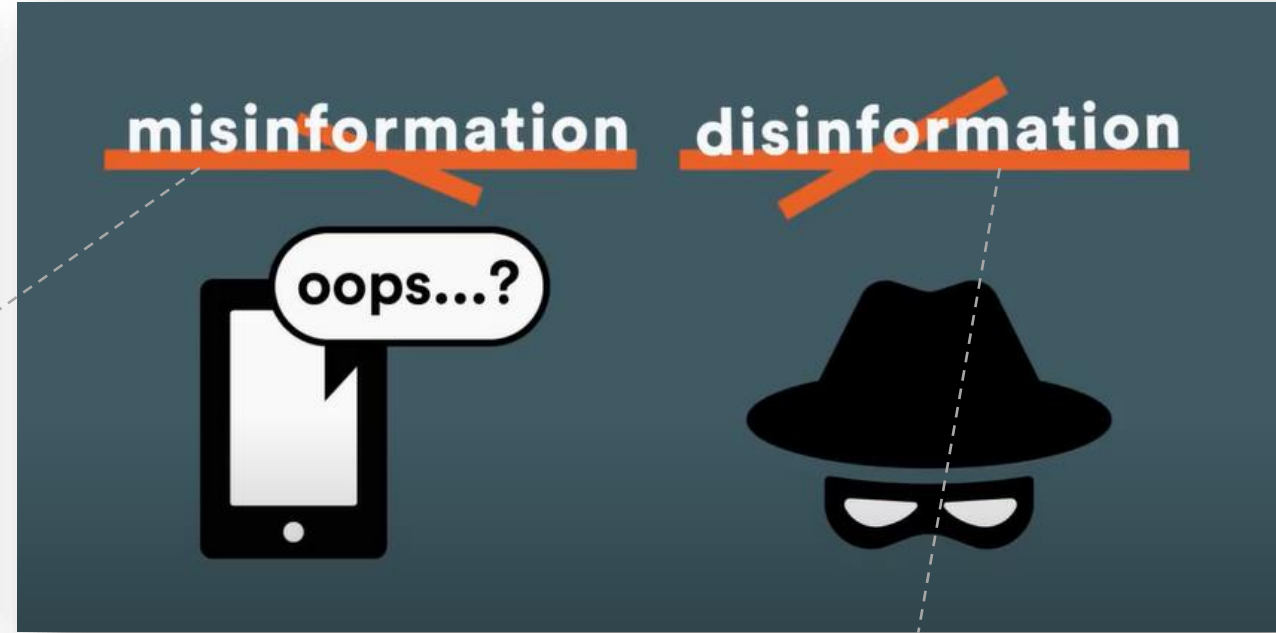
DOMINASI **CLICKBAIT**

Audiens lelah, kecewa & bingung, namun tetap mengklik.....





**Kebenaran berita dipelintir
sedemikian rupa sehingga
membentuk narasi yang
menyimpang dan
menyesatkan banyak orang**



**Informasi palsu yang sengaja
disebarkan untuk menipu atau
mereayasa dengan motif
tertentu**



DATA PRIBADI PENGGUNA PONSEL

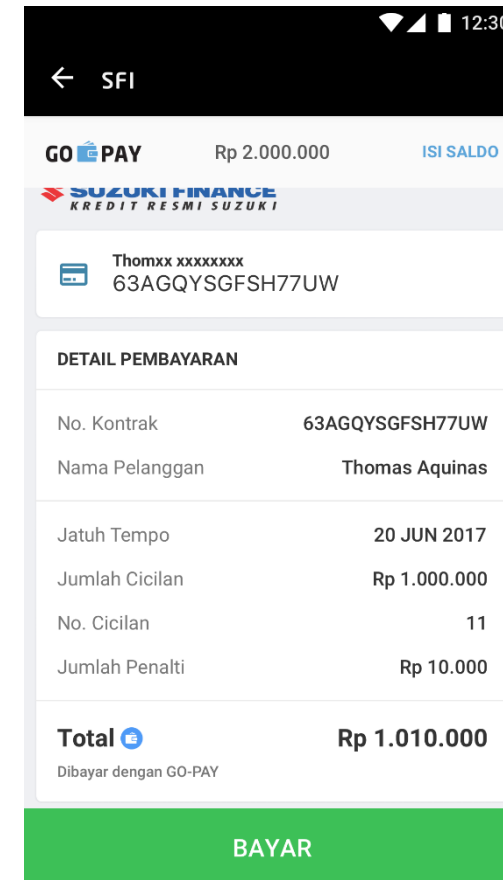
MENJAGA KEAMANAN DATA PRIBADI

1. Pastikan pengguna memberikan data kepada pihak yang tepat
2. Lakukan double checking di setiap transaksi
3. Periksa perijinan akses aplikasi
4. Baca Syarat dan ketentuan aplikasi



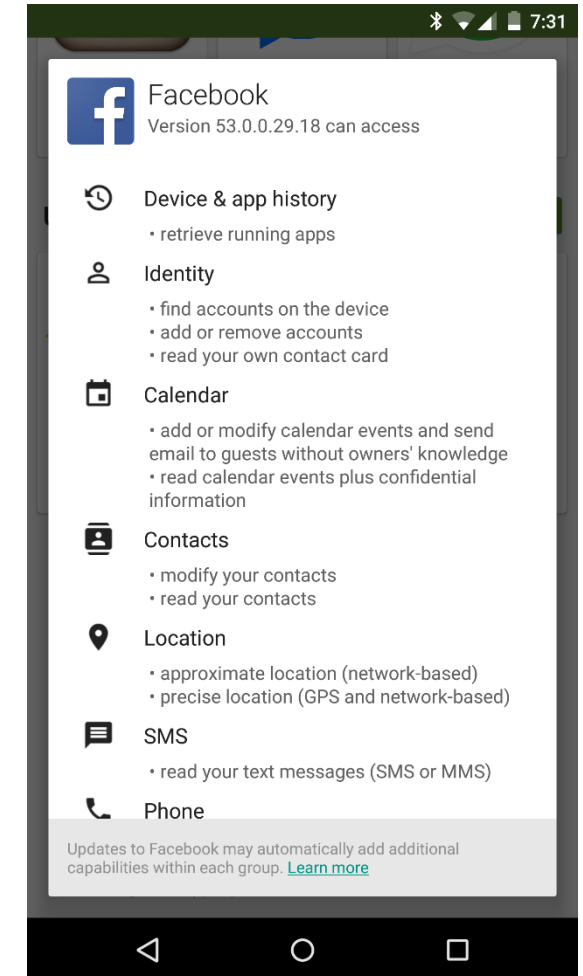
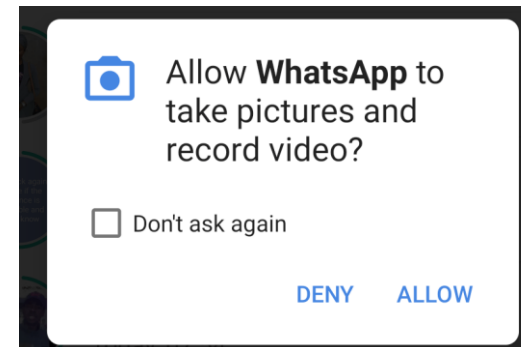
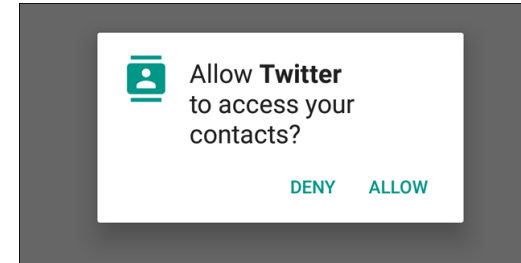
MENJAGA KEAMANAN DATA PRIBADI

1. Pastikan pengguna memberikan data kepada pihak yang tepat
2. Lakukan double checking di setiap transaksi
3. Periksa perijinan akses aplikasi
4. Baca Syarat dan ketentuan aplikasi



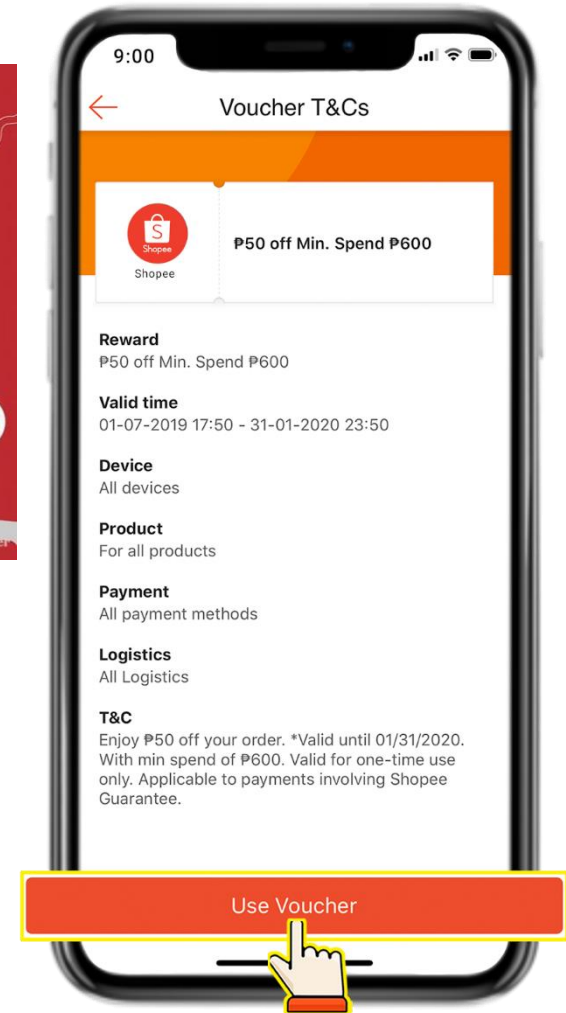
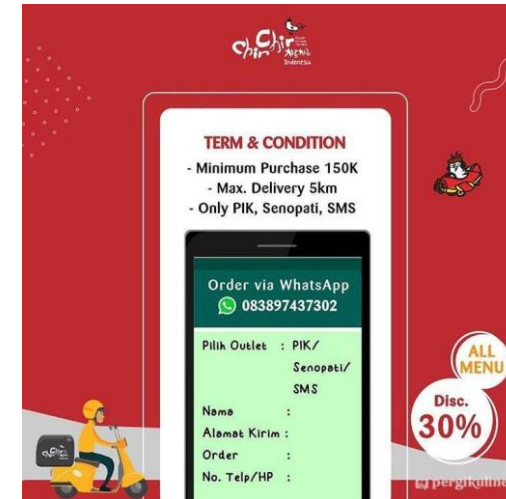
MENJAGA KEAMANAN DATA PRIBADI

1. Pastikan pengguna memberikan data kepada pihak yang tepat
2. Lakukan double checking di setiap transaksi
3. Periksa perijinan akses aplikasi
4. Baca Syarat dan ketentuan aplikasi



MENJAGA KEAMANAN DATA PRIBADI

1. Pastikan pengguna memberikan data kepada pihak yang tepat
2. Lakukan double checking di setiap transaksi
3. Periksa perijinan akses aplikasi
4. Baca Syarat dan ketentuan aplikasi



KEAMANAN

KENYAMANAN

