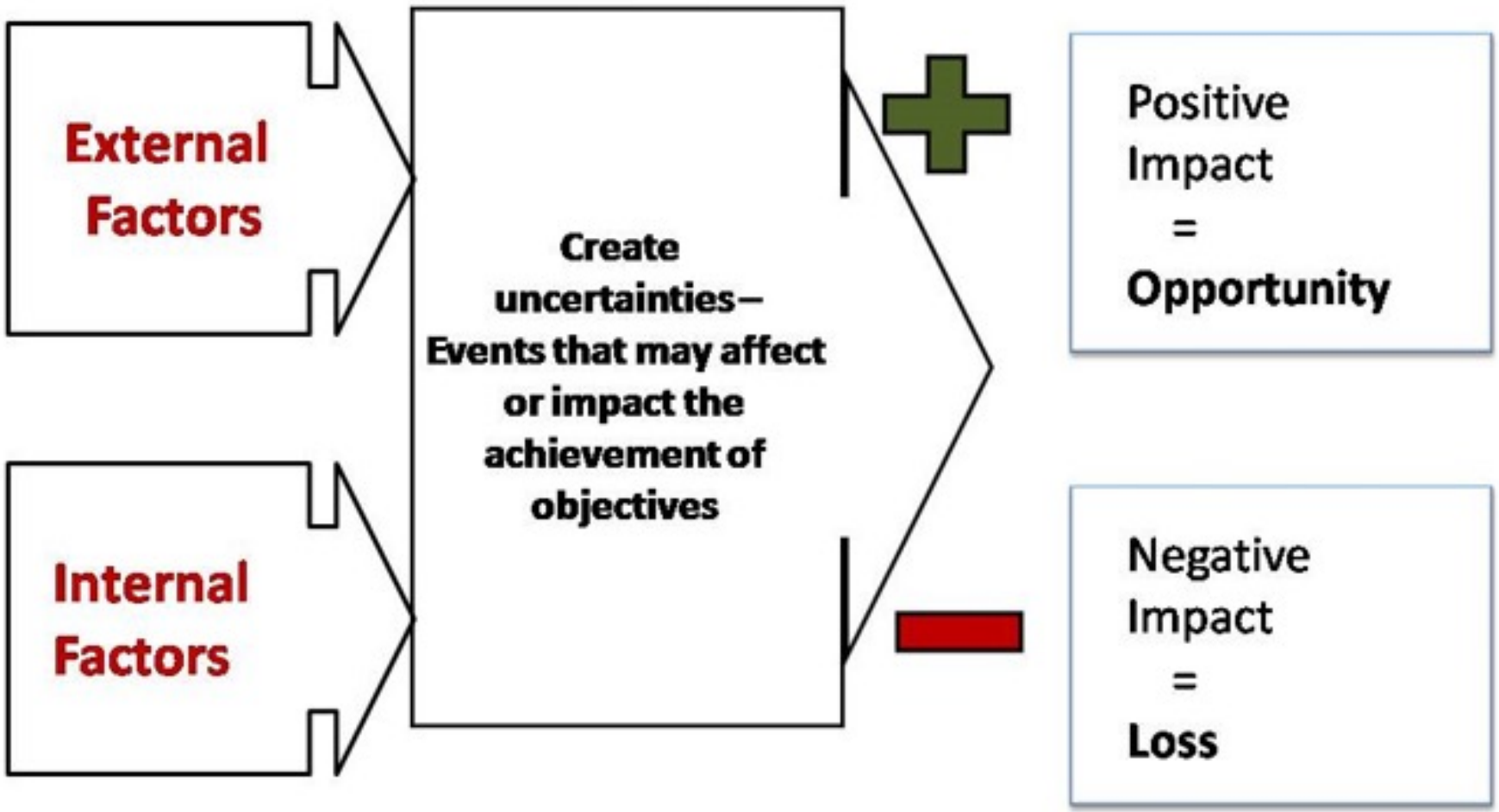
Manajemen Risiko

Guruh Prasetyo Putro, S.ST., M.Si (Han)

Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Badan Siber dan Sandi Negara
2022

Prinsip Risiko

- Risiko adalah potensi terjadinya suatu peristiwa/kejadian, baik yang dapat diperkirakan maupun yang tidak dapat diperkirakan, yang dapat menimbulkan dampak negatif bagi pencapaian visi, misi, tujuan/sasaran.
- Risiko adalah suatu ketidakpastian dari suatu kejadian/peristiwa, yang berpotensi memberikan dampak (negatif) terhadap pencapaian tujuan organisasi.


External Factors
Internal Factors
Create uncertainties– Events that may affect or impact the achievement of objectives
Positive Impact = Opportunity
Negative Impact = Loss

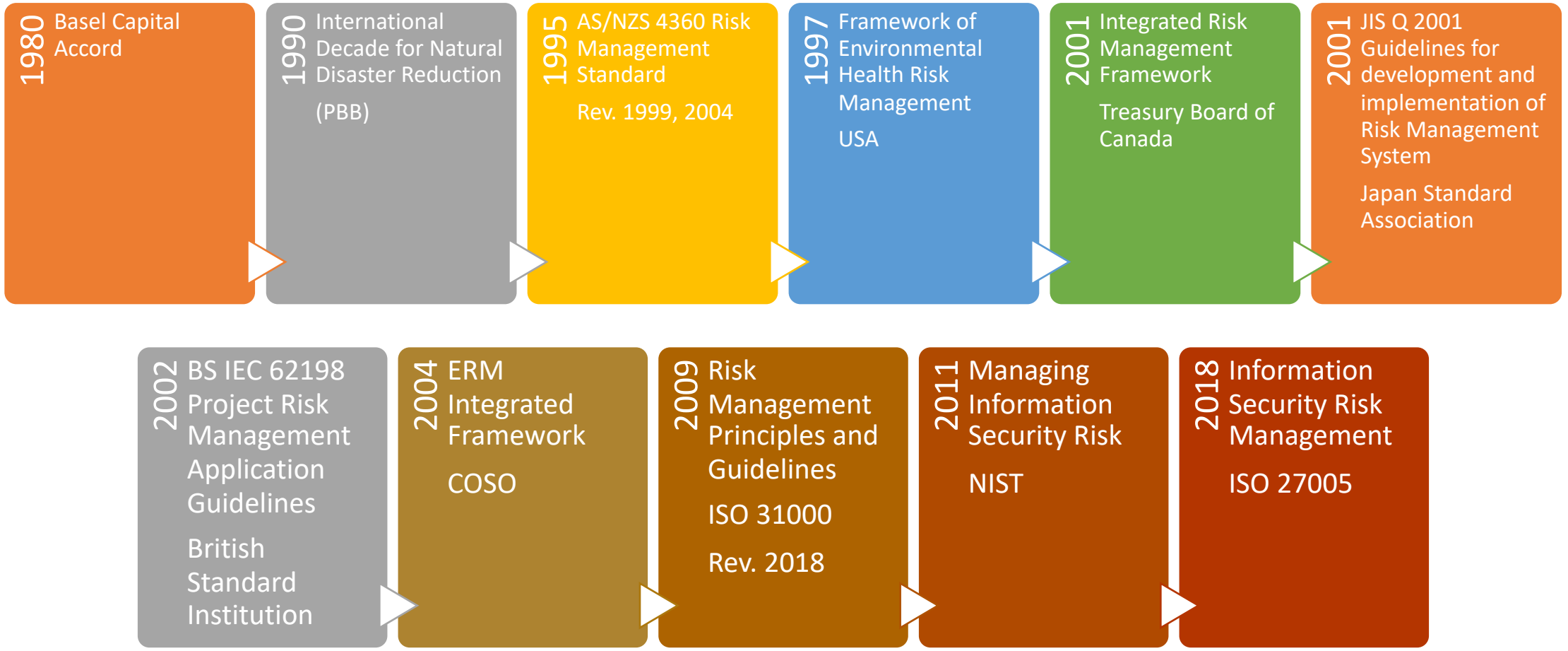
Mengapa Perlu Manajemen Risiko

- Seringkali ditafsirkan bahwa manajemen risiko adalah menghilangkan risiko.
- Tujuan manajemen risiko adalah mengenali seberapa besar risiko yang dihadapi dan bagaimana mengelolanya – kepastian organisasi untuk mencapai tujuannya tanpa terekspos pada risiko yang berlebihan –
- Manajemen risiko bukan berarti harus menghindari risiko, namun kita harus melakukan perhitungan (kuantifikasi) risiko sehingga hasil yang diperoleh setara dengan risiko yang dihadapi

Manajemen Risiko

- Serangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, mengendalikan dan memantau risiko yang muncul dari kegiatan operasional.
- Suatu proses pengelolaan secara proaktif atas risiko dengan memitigasi risiko yang menjadi ancaman tercapainya tujuan organisasi.
- Suatu tindakan mengidentifikasi risiko-risiko secara terencana dan terukur, dan mempersiapkan berbagai pendekatan untuk mengendalikan agar tujuan dapat dicapai.

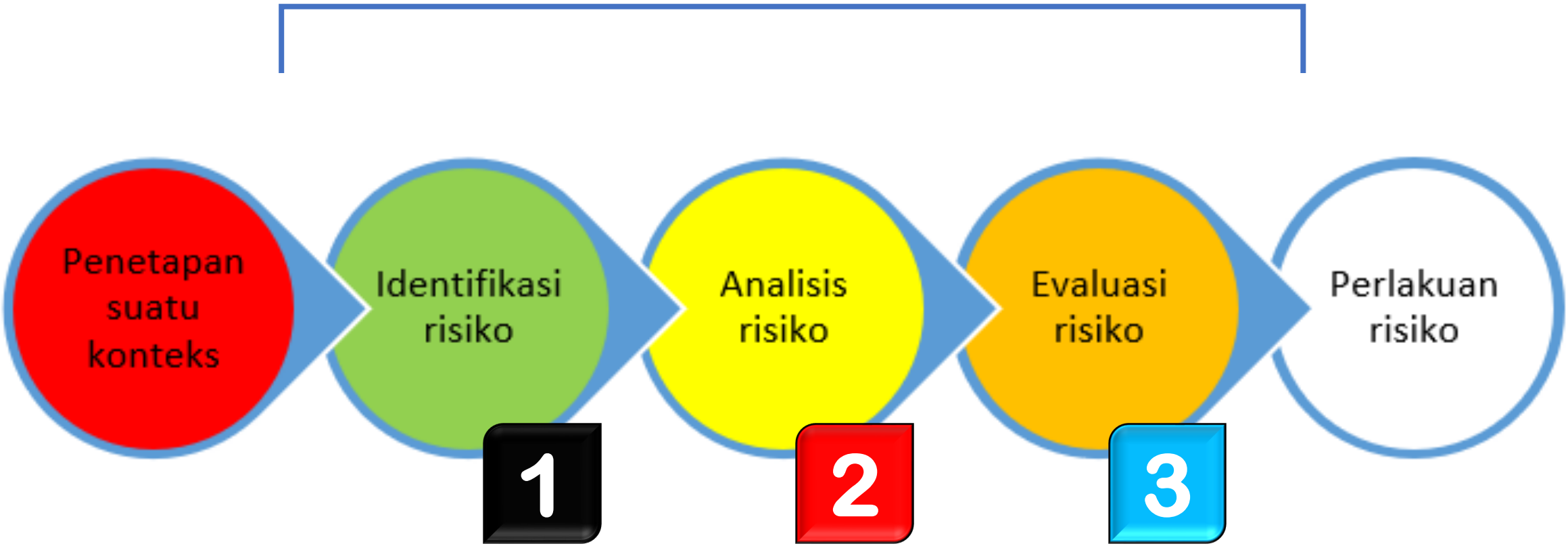
Sejarah Manajemen Risiko



Hirarki Manajemen Risiko

- Risiko berkaitan erat dengan kejelasan sasaran.
- Pemilik risiko adalah pemilik sasaran, dan pada dasarnya hal ini berlaku disemua level organisasi.
- Risiko terdapat pada seluruh tingkat organisasi.
- Risiko juga terdapat pada seluruh proses bisnis organisasi.
- Setiap orang dalam organisasi memiliki sasaran kerja.

Proses Manajemen Risiko



Prinsip Manajemen Risiko SNI/ISO 31000

Proses Manajemen Risiko

Identifikasi Risiko	Pengukuran Risiko	Evaluasi/Pemetaan Risiko	Respon Risiko	Monitoring dan Review
• Daftar Risiko • Jenis Risiko	• Probabilitas Risiko • Dampak Risiko • Level Risiko	• Profil Risiko • Prioritas Penanganan Risiko	• Desain awal Penanganan Risiko • Keputusan cara Penanganan Risiko	• Efektifitas Penanganan Risikio • Perbaikan Pengawasan • Perbaikan Pedoman Manajemen Risiko • dll

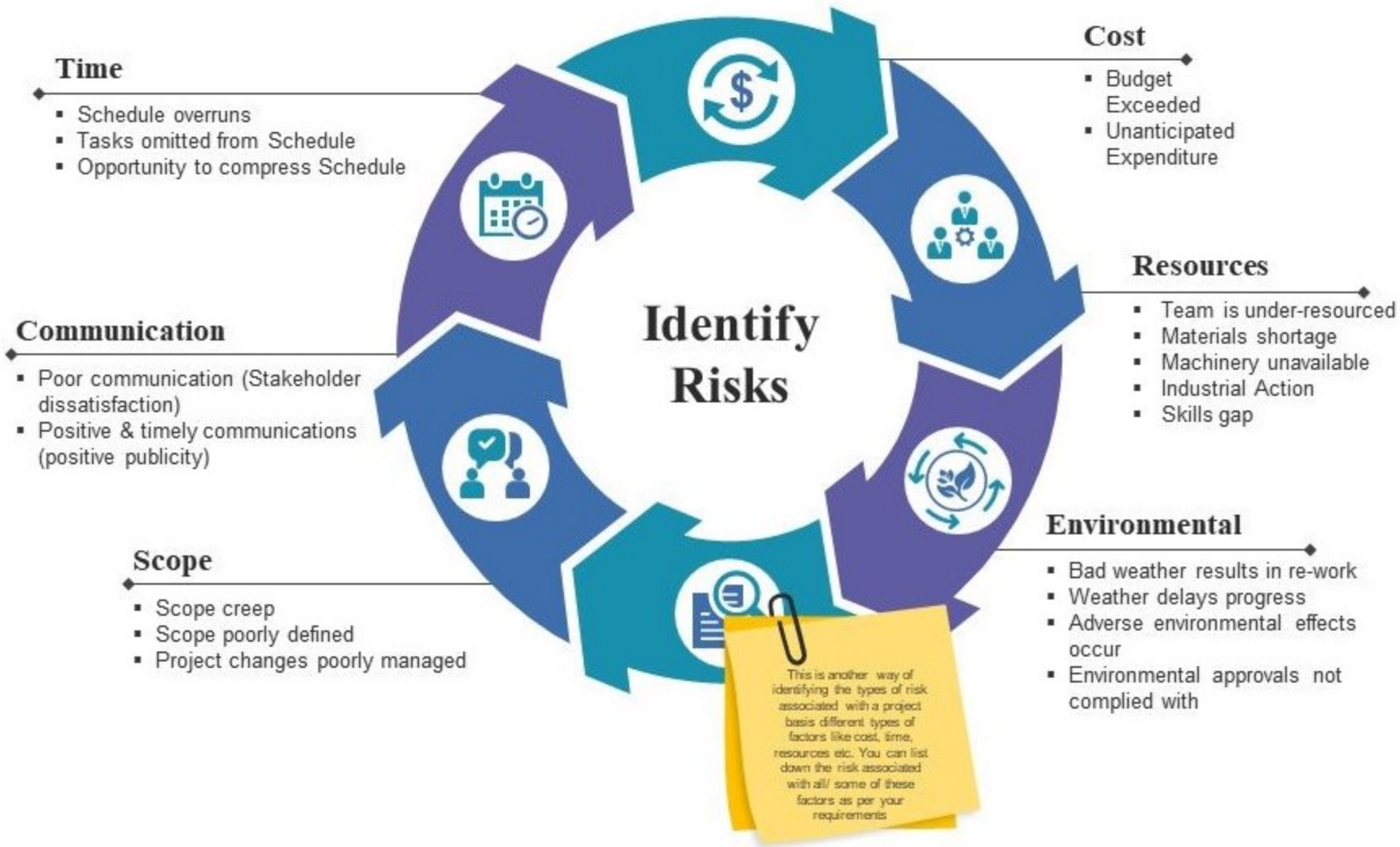
1 2 3

Risk Assessment

- RA terdiri dari Risk Identification – Risk Analysis – Risk Evaluation
- Proses RA dapat dilakukan pada setiap level organisasi, departemen, proyek, aktivitas individu atau risiko yang lebih spesifik.
- RA dilakukan untuk mendapatkan:
  - Risiko dan dampak terhadap tujuan organisasi.
  - Kapan suatu keputusan/aktivitas harus dilakukan.
  - Bagaimana memaksimalkan peluang.
  - Kapan risiko harus dikelola.
  - Memilih opsi keputusan.
  - Mencari prioritas opsi risk treatment.
  - Bahan dukungan informasi untuk pimpinan.

Identifikasi Risiko

1

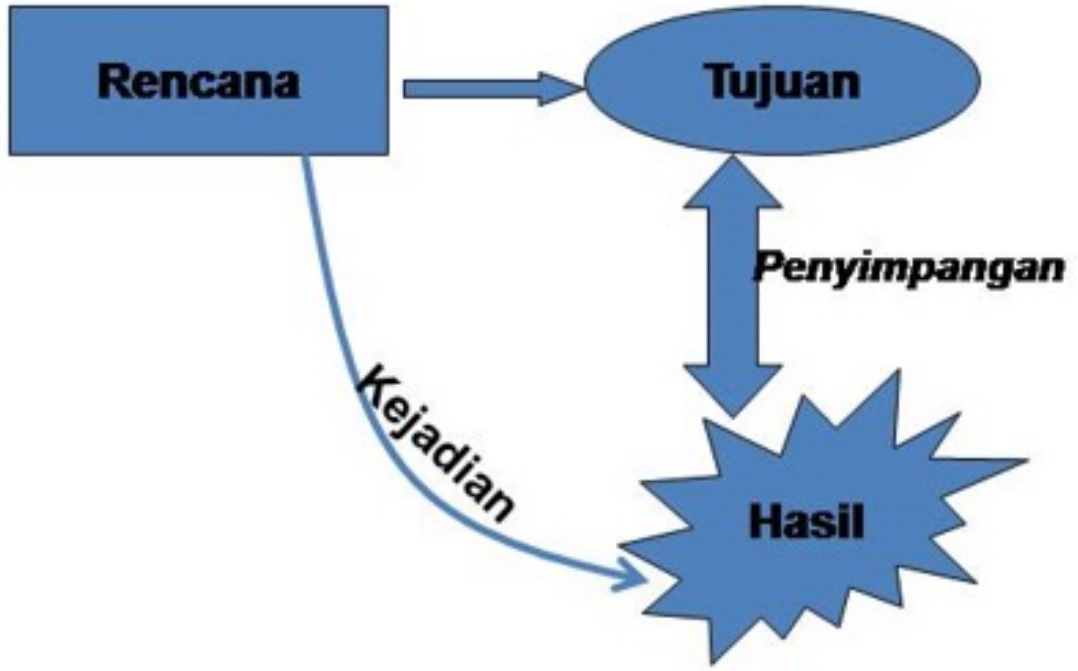


Identifikasi Risiko

Melakukan identifikasi atas kejadian maupun potensi kejadian yang apabila terjadi akan mempengaruhi pencapaian tujuan organisasi (berpotensi merugikan).

Identifikasi Risiko bertujuan:

Mengenali seluruh potensi risiko yang melekat (inherent risk) pada setiap aktifitas fungsional/operasional



Kata kunci dalam identifikasi risiko:

1. Kejadian tidak direncanakan
2. Tujuan
3. Penyimpangan

Identifikasi Risiko

Dalam melakukan identifikasi risiko harus mempertimbangkan faktor sumber/penyebab risiko (risk cause)

Faktor Internal	Faktor Ekstenal
• Infrastruktur • Aset • Proses • Personil • Teknologi	• Politik • Lingkungan • Ekonomi • Sosial • Regulasi • Masyarakat

Teknik Identifikasi

Retrospective

- Past organizational experience
- Historical records (loss event database)
- Post event reports / Audit reports
- Wawancara
- Financial reports

Prospective

- Expert judgement
- Change analysis result (what-if)
- FGD / Brainstorming
- Process flow analysis
- Benchmarking
- Threat scenario

Contoh Teknik Identifikasi Risiko

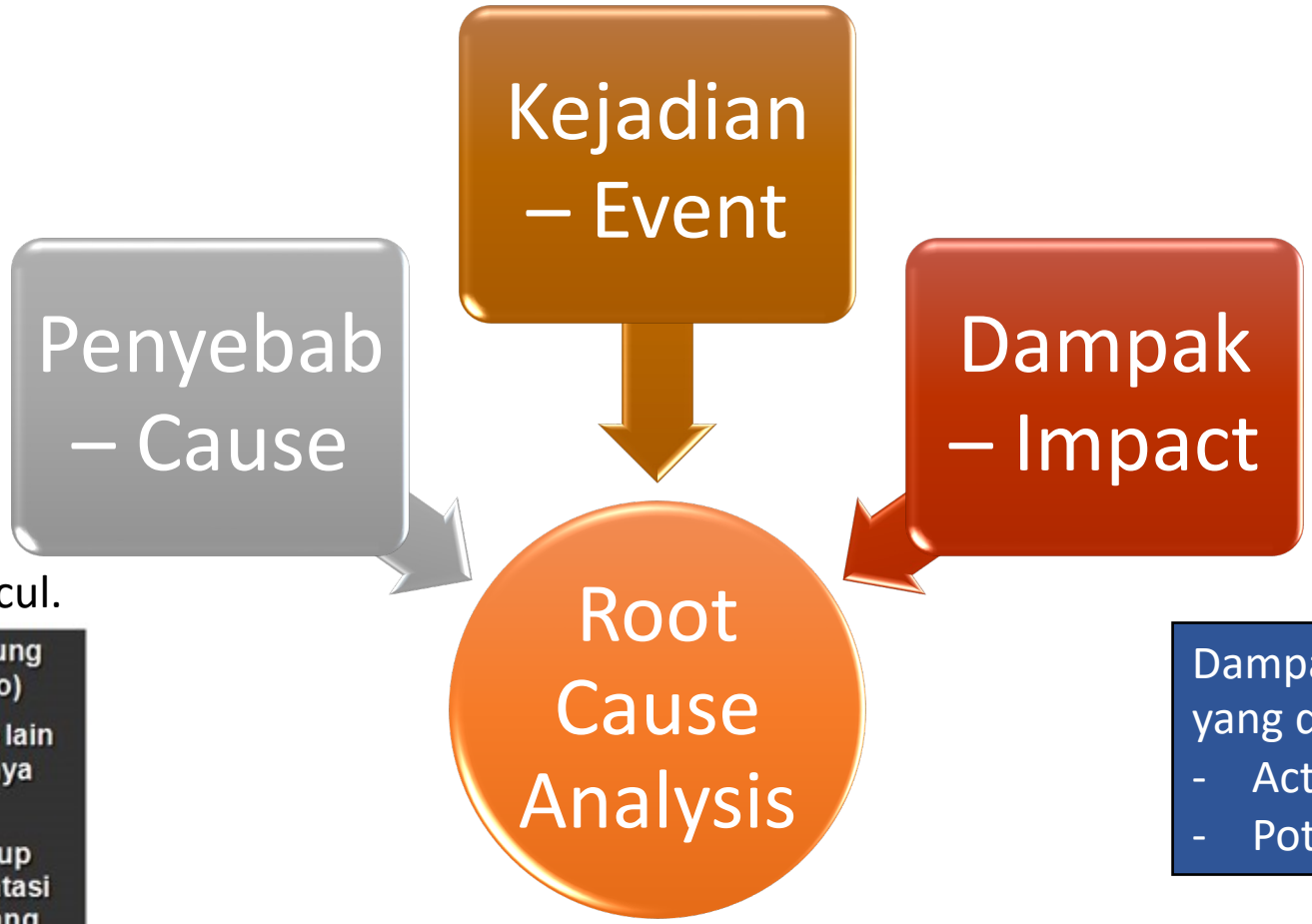
Pendekatan Historis	*-Gunakan pengalaman yang sejenis* *-Identifikasi risiko yang pernah terjadi* *-Proyeksikan ke situasi saat ini* *-Tetapkan risiko yang bisa terjadi*
Pendekatan FGD/Brainstorming	*- Analisis situasi yang Anda hadapi* *-Identifikasi risiko yang bisa terjadi* *-Proyeksikan ke situasi saat ini* *-Tetapkan risiko yang bisa terjadi*
Pendekatan Benchmark	*-Identifikasi institusi lain sebagai benchmark* *-Identifikasi risiko yang dialami* *-Proyeksikan ke situasi saat ini* *-Tetapkan risiko yang bisa terjadi*
Pendekatan Pendapat Ahli	*-Tetapkan beberapa orang sebagai ahli* *-Wawancara mengenai risiko* *-Tetapkan risiko yang bisa terjadi*

Kunci Identifikasi Risiko

Signifikan	Pilih risiko yang mempunyai dampak signifikan terhadap pencapaian tujuan organsiasi.
Efektif dan sederhana	Pilih risiko yang dapat menggambarkan risiko inheren yang terjadi atau mungkin terjadi.
Prioritas	Prioritaskan pada risiko-risiko yang berdampak langsung kepada tujuan organisasi.
Risk cause	Periksa sumber informasi yang dapat digunakan untuk mengidentifikasi faktor-faktor risiko.
Opsional	Gunakan lebih dari satu macam teknik identifikasi untuk mendapatkan risiko sebanyak mungkin.

Root Cause Analysis

What issue?



Kenapa dan Bagaimana kemungkinan risiko muncul.

1. Direct Cause (penyebab langsung yg menimbulkan kejadian risiko)
2. Contributing Cause (penyebab lain yang turut mendukung terjadinya suatu kejadian risiko)
3. Penyebab Risiko bisa saja cukup banyak, namun sebaiknya dibatasi menjadi beberapa penyebab yang paling relevan dan significan

Dampak/kerugian yang ditimbulkan.

- Actual loss
- Potential loss

Asking "why" five times

1. Q. Why did the machine stop?
   A. There was an overload and the fuse blew.

2. Q. Why was there an overload?
   A. The bearing was not sufficiently lubricated.

3. Q. Why was it not sufficiently lubricated?
   A. The lubrication pump was not pumping sufficiently.

4. Q. Why was it not pumping sufficiently?
   A. The shaft of the pump was worn and rattling.

5. Q. Why was the shaft worn?
   A. There was no strainer and metal scrap got in.

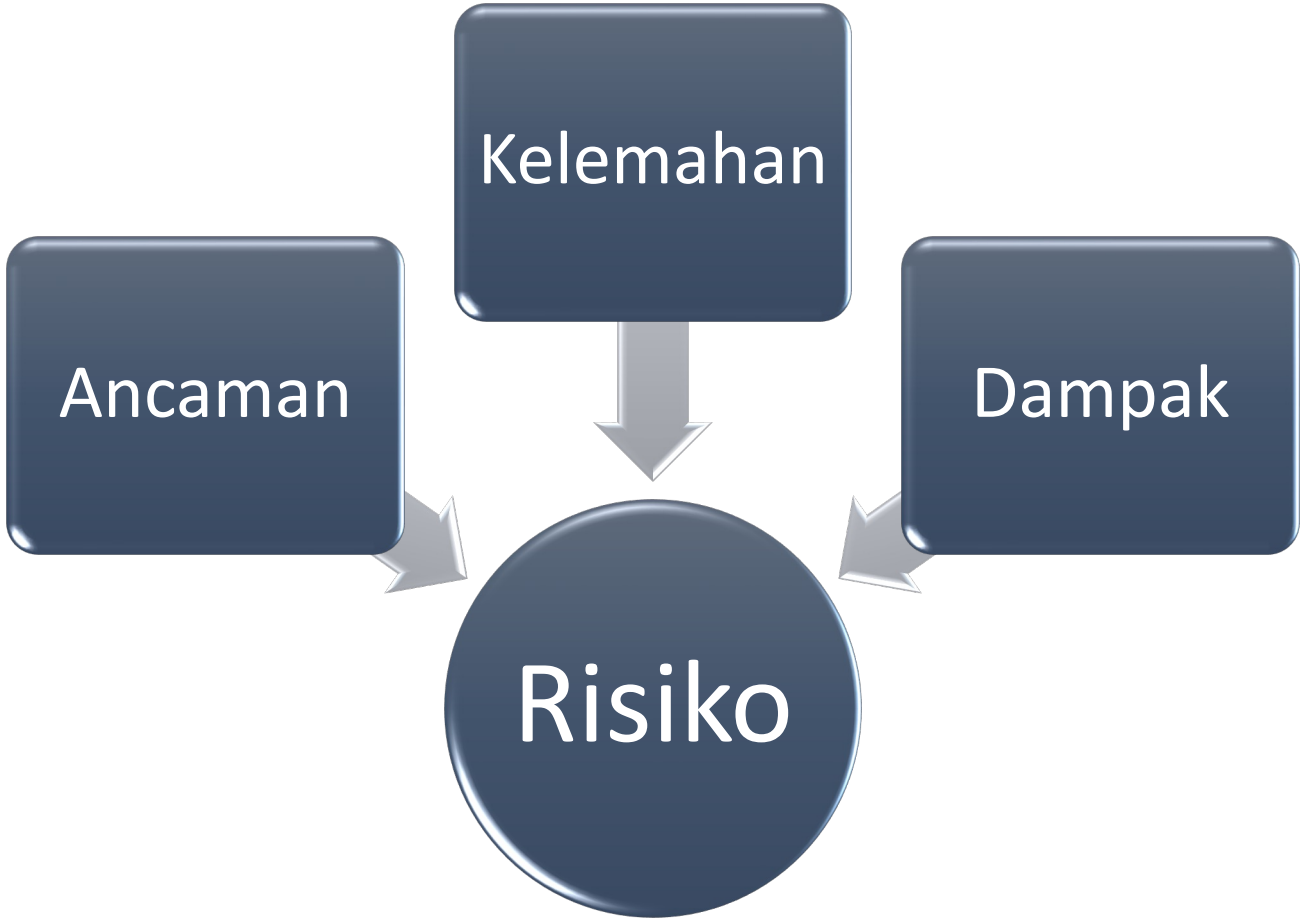
Repeating why five times like this can help uncover the root problem and correct it. If this procedure were not carried through, one might simply replace the fuse or the pump shaft. In that case the problem would reoccur in a few months.

Taiichi Ohno
Toyota Production System

Contoh.


PENYEBAB
KEJADIAN
KERUGIAN
Masa berlaku perizinan Tidak terpantau
Pengurusan Perizinan Perusahaan terlambat
Proyek Tertunda
Sistem pengamanan aset yang kurang baik
Kehilangan computer
Data hilang dan harus membeli computer
Teknologi/ alat yang sudah usang
Gangguan Jaringan
Kerusakan image

Elemen Manajemen Risiko



Woman Standing On Edge Of Rock is a photograph by Vitor Marigo which was uploaded on January 21st, 2018.

Faktor yang berperan dalam risiko

- Kelemahan
  - *People*
  - *Process*
  - *Technology & Infrastructure*
- Ancaman
  - Nilai Aset
  - Aktor
  - Motivasi
  - Sumber Daya Pendukung
  - Faktor Alam
  - Teknologi
  - [Perkembangan Teknologi >< Kebutuhan Hidup]
  - Kondisi tertentu terkait waktu

Ancaman Karena Faktor Manusia

Bomb Attack

Computer Crime

Network/application Backdoor

Un-authorized Network/System Access

Viruses

DDoS

Trojans

Fraud

Human Error

Un-authorized Scan

Terrorist

Malicious Code

Network/application Time bomb

Un-intentional DDoS

Tailgating to gain Un-authorized Access

Sabotage

Robbery

Worm

Vandalism

Bomb Threat

Ancaman Karena Faktor Teknis

Power Fluctuations

DNS Failure

Application software Failure

HVAC Failure

Hardware Failure

CPU Malfunction Failure

Telecommunication Failure

Power Failure

Software Defect

System software Failure

Contoh Kelemahan dan Ancaman

	KELEMAHAN	ANCAMAN
Hardware	Proses pemeliharaan yang tidak layak	Kerusakan
	Storage tidak disimpan dengan baik	Hilang atau dicuri
	Ceroboh dalam mengelola pemusnahan media	Pencurian media
Software	Pemgujian *software* tidak dilakukan	Penyalahgunaan akses
	Tidak *logout* saat meninggalkan komputer	Penyalahgunaan akses
	Penghapusan/penghancuran media tidak sempurna	Penyalahgunaan akses
	Jejak audit tidak tersedia	Penyalahgunaan akses
	Kesalahan alokasi hak akses	Penyalahgunaan akses
Network	*Password* tidak disimpan dengan aman	Penyalahgunaan akses
	Koneksi jaringan publik tidak telindungi	Penggunaan perangkat secara tidak berwenang
SDM	Pelatihan keamanan kurang memadai	Kesalahan penggunaan TI
	Pemantauan tidak dilakukan	Pelanggaran kebijakan keamanan

Analisis Risiko

Pengukuran Risiko

2

Pengukuran risiko dilakukan untuk menentukan Level of Risk (tingkat eksposur risiko) dengan melihat dua perspektif, yaitu

Likelihood/ Probability/ Kemungkinan	Adalah peluang atau kemungkinan terjadinya risiko
Impact/ Consequencies/ Dampak	Adalah besarnya kerugian (severity) saat peristiwa risiko terjadi. Aspek keuangan, SDM, Reputasi, Output, dll

Asesmen pertama kali dilakukan terhadap inherent risk (risiko tanpa kontrol)

Inherent Risk vs Residual Risk

- Inherent risk adalah risiko yang terjadi apabila organisasi tidak melakukan suatu Tindakan baik dari sisi perhitungan dampak maupun kemungkinannya.
- Residual risk adalah risiko yang masih muncul setelah dilakukan Tindakan/kontrol baik terhadap sisi perhitungan dampak maupun kemungkinannya.
- Kontrol adalah aspek/faktor positif yang dapat memodifikasi risiko, dapat berupa suatu kebijakan, SOP, peralatan, instruksi kerja, surat edaran, dll.

Inherent Risk
Control
Residual Risk
Mitigant
Treated Risk
Current Risk Exposure
Risk Tolerance Line

Informasi yang dibutuhkan dalam RA

Past Records

Practice and Relevant Experience

Market Research

Experiments and Prototypes

Relevant published literature

Dampak

- Dampak merupakan tingkat kerugian dan/atau potensi kerugian yang terjadi dari satu kejadian/event berdasarkan pengalaman historis dan/atau kemungkinan di masa depan.
- Dapat bersifat kualitatif dan kuantitatif, contoh:
  - Kerugian Rp.50 juta
  - Gugatan pihak ketiga
  - Kehilangan pelanggan
  - Reputasi buruk organisasi
- Tabel dampak dibuat sebagai pedoman untuk menentukan kriteria dampak dari masing-masing kejadian/event. – Finansial, Operasional, SDM, Reputasi, dll –
- Penentuan table dampak dilakukan oleh Top Management.

Dampak

- Ketika pertama kali mengukur nilai dampak sebuah risiko, dimungkinkan memiliki lebih dari satu dampak. Risk owner dapat memilih satu dampak saja yang paling dominan, signifikan, dan/atu mempunyai bobot yang tertinggi.

Kemungkinan

- Likelihood merupakan tingkat kemungkinan sebuah risiko terjadi dibandingkan seluruh aktivitas dan/atau periode waktu tertentu, berdasarkan pada pengalaman historis dan/atau kemungkinan di masa depan.
- Seberapa besar kemungkinan Risiko AKAN/DAPAT terjadi.
- Contoh:
  - Kesalahan prosedur 5 kali dalam sebulan
  - Kegagalan sistem 2 kali dalam setahun
  - dll

- Tabel kemungkinan dibuat sebagai pedoman untuk menentukan Kriteria Kemungkinan dari masing-masing kejadian/event.
- Penentuan tabel kemungkinan pertama kali dilakukan oleh Top Management.

Kemungkinan (*Probability*)	Uraian
Sangat Jarang	Risiko terjadi sekali dalam waktu >5 tahun
Jarang	Risiko dapat terjadi sekali antara 1 – 5 tahun
Sedang	Risiko mungkin terjadi 1-6 kali setahun
Sering	Risiko mungkin terjadi rata-rata 1 kali setiap bulan
Sangat Sering	Risiko terjadi minimum seminggu 1 kali

Dampak (*Impact*)	Uraian
Tidak Signifikan	Dampak dapat diatasi dengan kegiatan rutin atau tidak menimbulkan kerugian berarti (<10 juta)
Minor	Dampak bisa mengganggu pekerjaan selama maksimum 4 jam atau kemungkinan kerugiannya antara Rp 10 – 50 juta
Menengah	Dampak bisa mengganggu pekerjaan selama maksimum 24 jam atau kemungkinan kerugiannya di atas Rp 50 maksimum 100 juta
Besar	Dampak bisa mengganggu pekerjaan selama lebih dari 24 jam, maksimum 3 x24 jam atau kemungkinan kerugiannya di atas Rp 100, Maksimum 250 juta
Sangat Besar	Dampak bisa mengganggu pekerjaan selama lebih dari 3x24 jam atau kemungkinan kerugiannya di atas Rp 250 juta

Contoh Lain Nilai Dampak

Dampak	Uraian
Sangat Besar	Risiko mengakibatkan keseluruhan proses bisnis utama tidak berjalan lebih dari 1 hari
Besar	Risiko mengakibatkan seluruh aktivitas bisnis utama mengalami penundaan selama 4-8 jam
Menengah	Risiko mengakibatkan sebagian aktivitas bisnis utama mengalami penundaan selama <4 jam
Minor	Diskripsi risiko mengakibatkan gangguan aktivitas bisnis utama <2 jam
Tidak Signifikan	Diskripsi risiko tidak menyebabkan gangguan proses bisnis utama

Contoh Lain Kriteria *Probability– Impact*

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

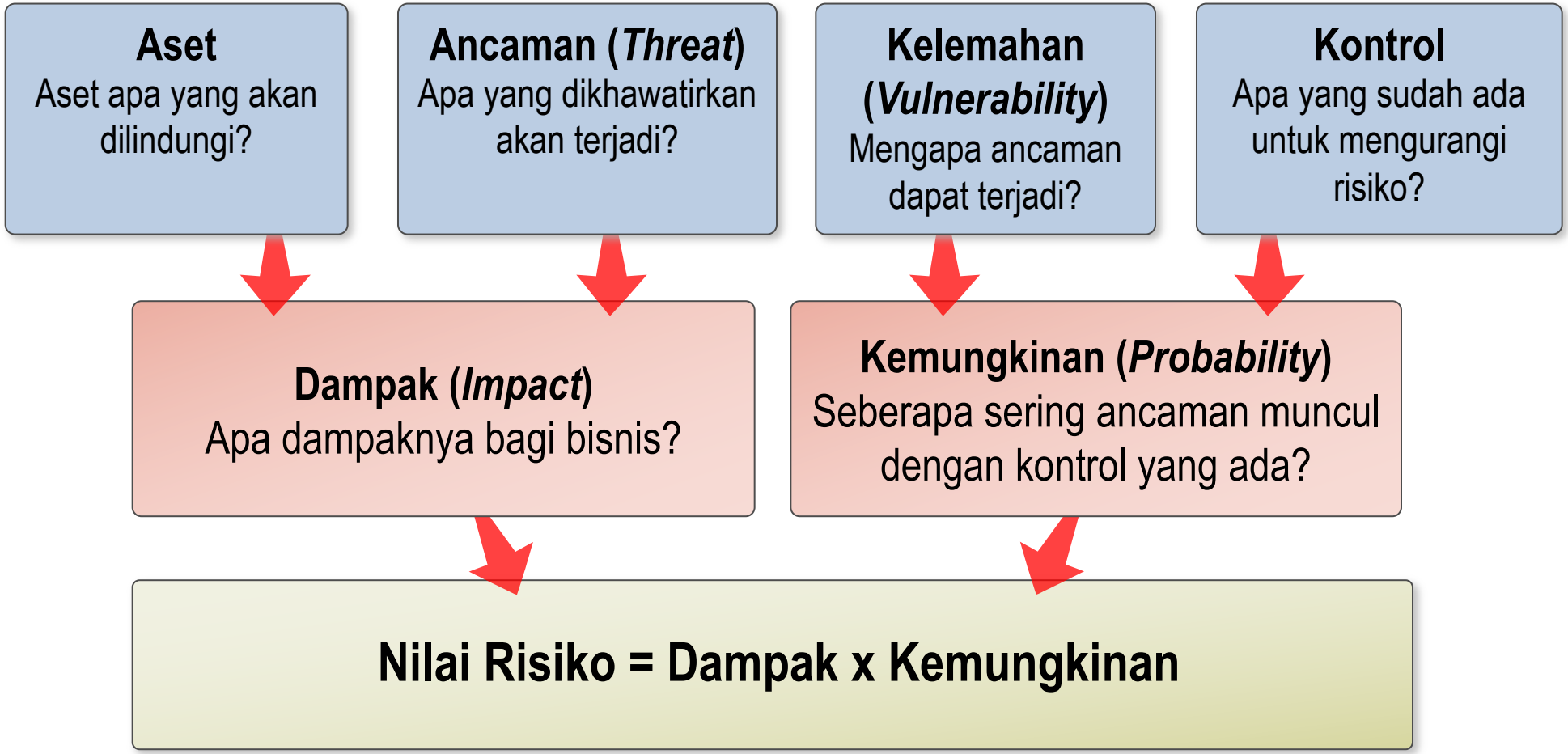
Matriks Risiko

Kemungkinan (*Probability*)	DAMPAK (*IMPACT*)				
	Tidak Signifikan (1)	Minor (10)	Menengah (50)	Besar (100)	Sangat Besar (200)
Sangat Jarang (1)	1	10	50	100	200
Jarang (2)	2	20	100	200	400
Sedang (4)	4	40	200	400	800
Sering (8)	8	80	400	800	1600
Sangat Sering (10)	10	100	500	1000	2000

Kriteria Nilai Risiko: RENDAH (1-50); SEDANG (>50 – 200); TINGGI (>200 – 500); SANGAT TINGGI (>500 – 2000)

RENDAH SEDANG TINGGI SANGAT TINGGI

Metode Penilaian Risiko



Evaluasi Risiko

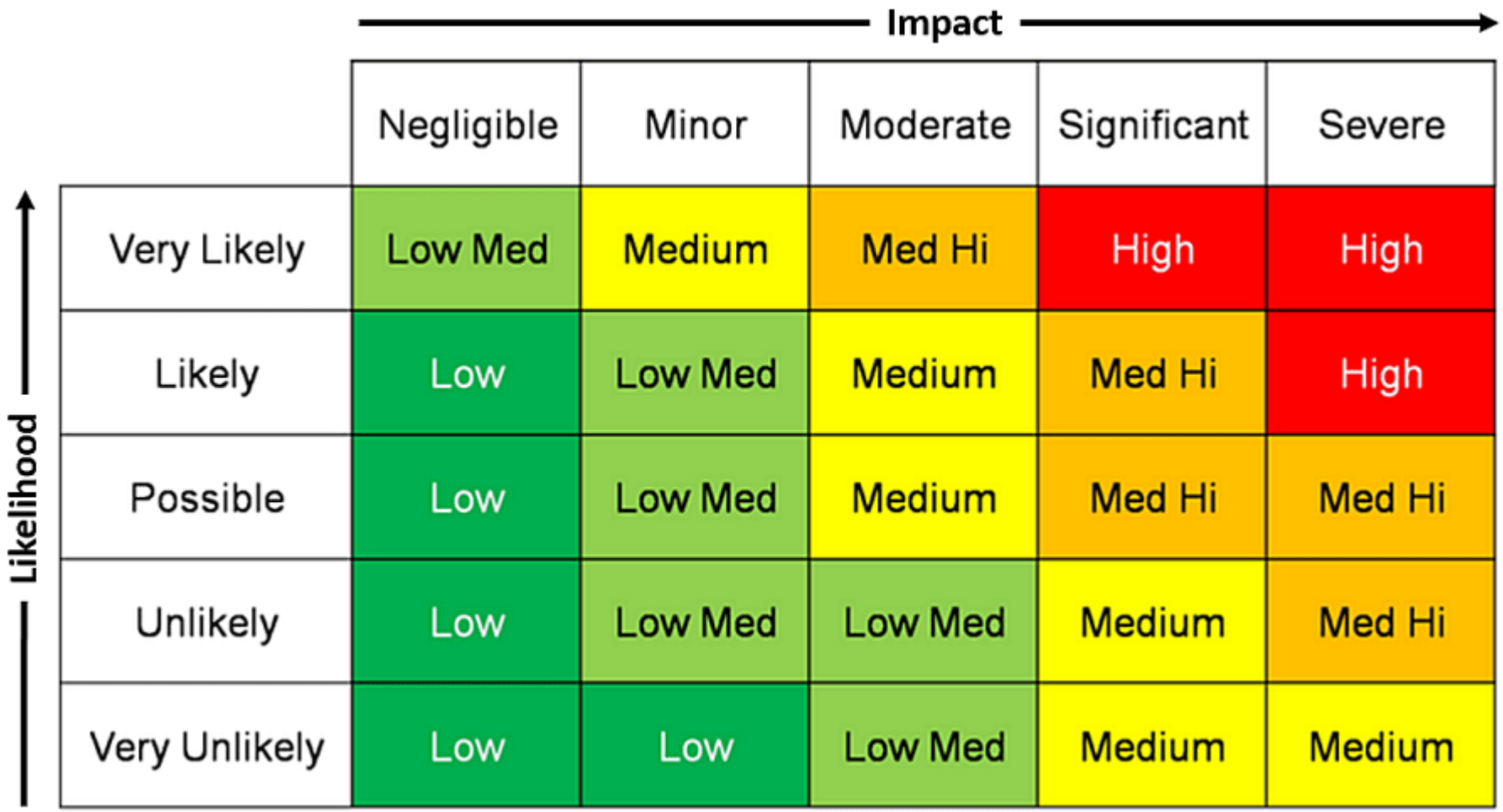
3

- Evaluasi risiko mengacu pada penetapan apakah risiko tersebut melampaui toleransi risiko organisasi atau tidak.
- Evaluasi risiko juga mengurutkan prioritas risiko untuk rencana penanganan risiko (risk treatment plan).
- Output dari evaluasi risiko
    1. Peta Risiko
    2. Daftar Prioritas Risiko

Peta Risiko

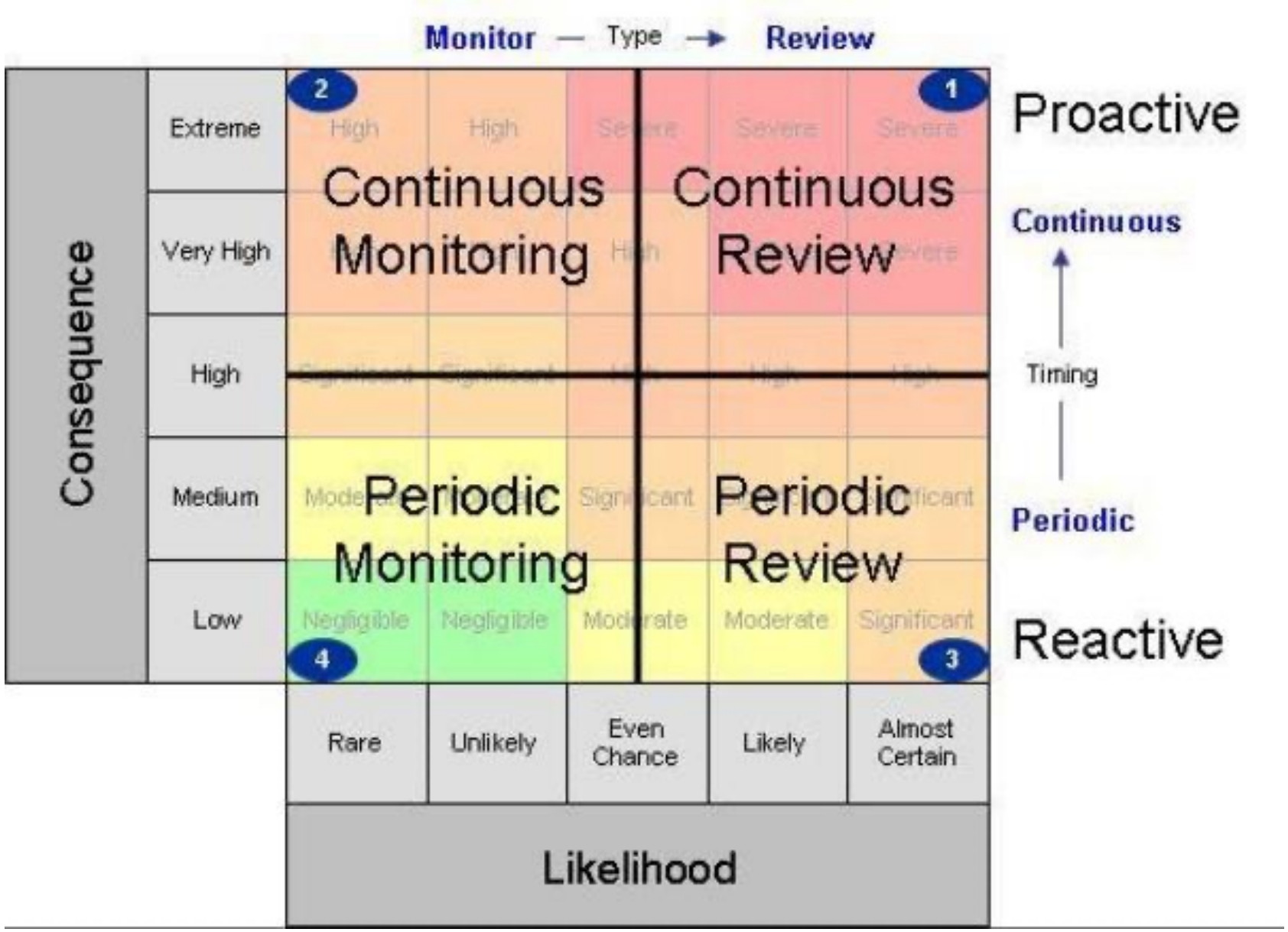
- Representasi grafis dari kejadian risiko atas dasar tingkatan dampak dan kemungkinan dalam suatu unit bisnis tertentu.
- Digunakan untuk menunjukkan posisi risiko dan menentukan prioritas respon risiko.
- Peta risiko dapat dibuat berupa peta risiko inheren dan/atau peta risiko residual, disesuaikan dengan kebutuhan masing-masing organisasi.

Risk Heat Map

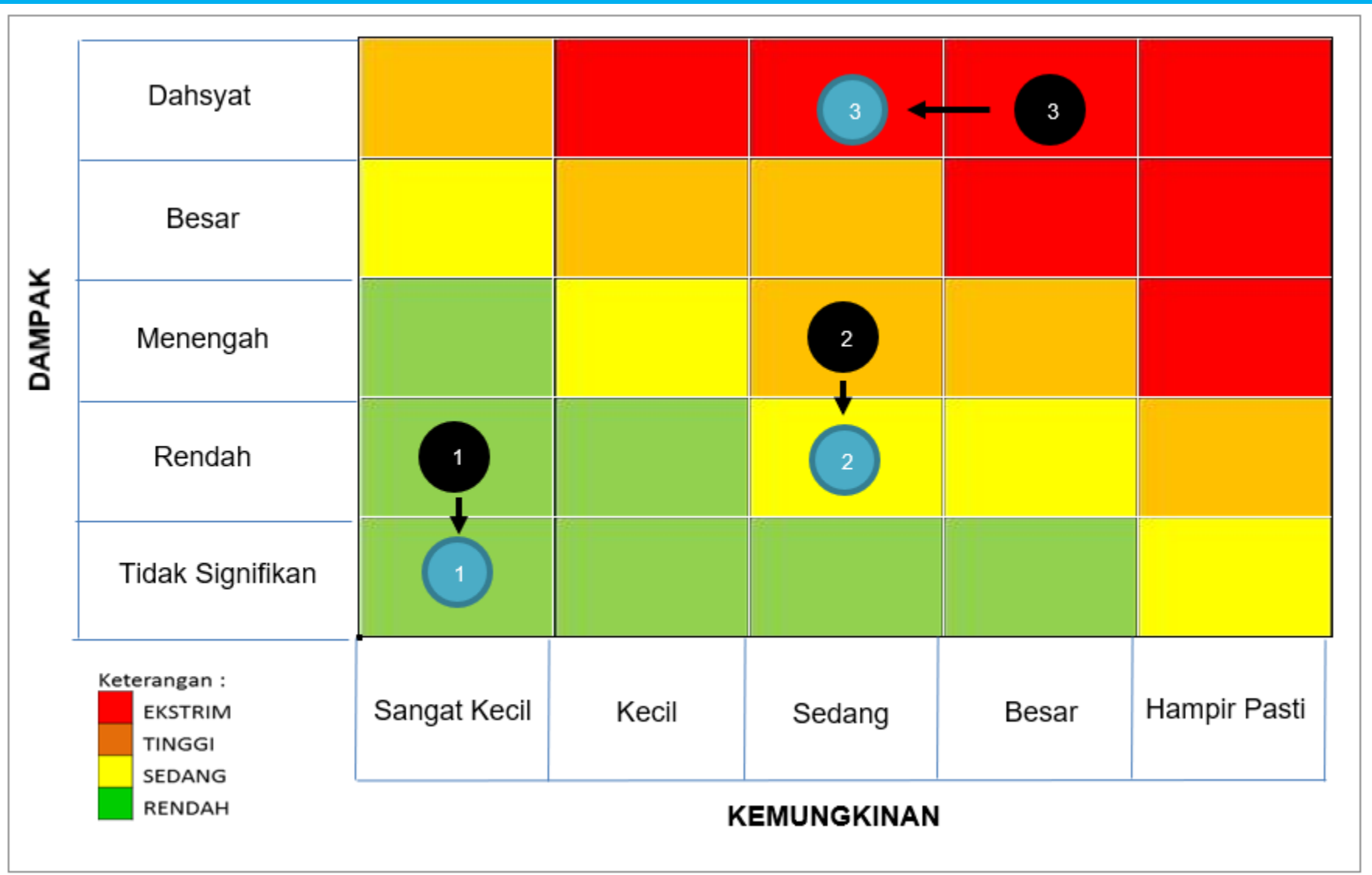


Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Heat Map



Peta Penanganan Risiko

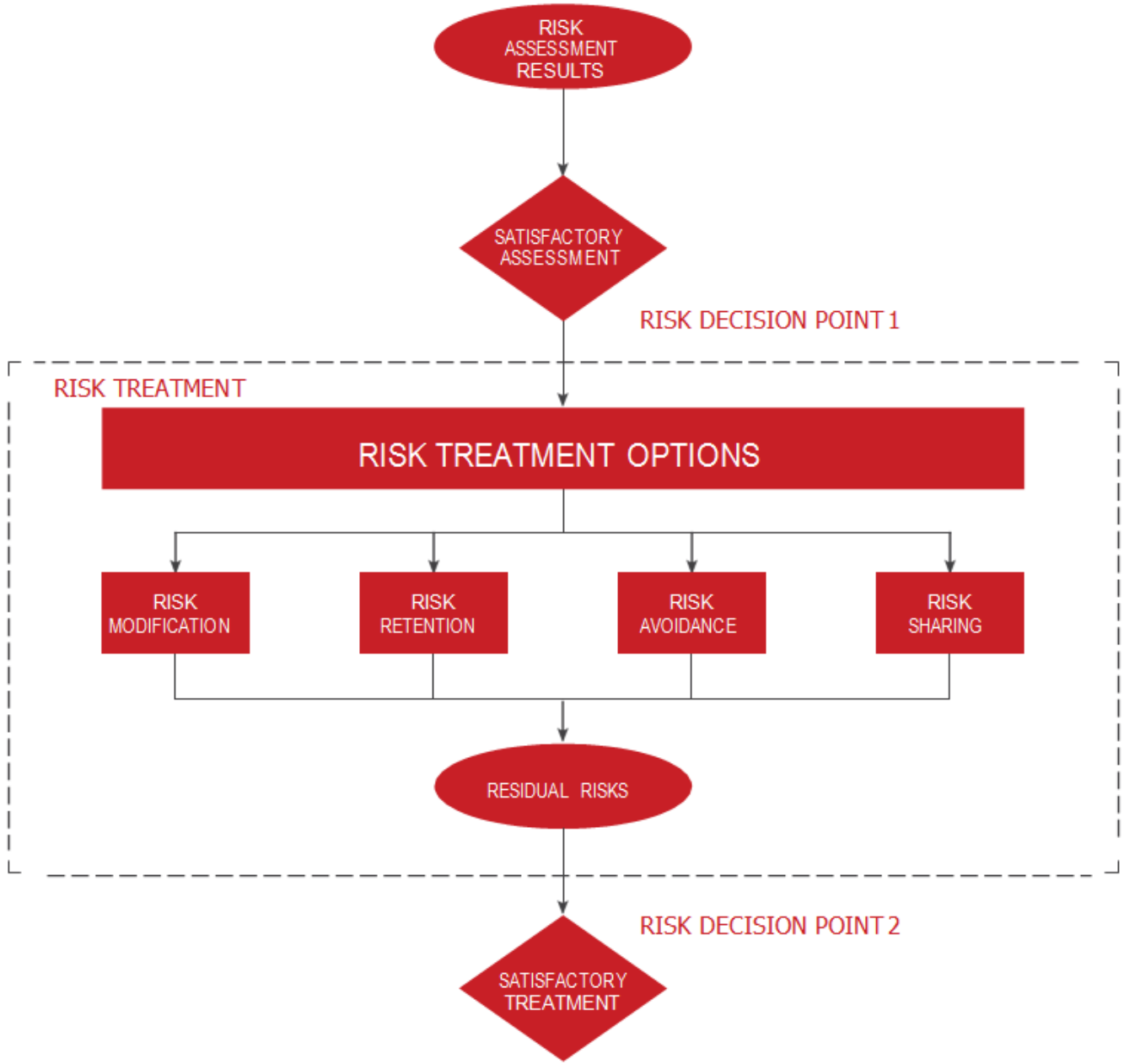


Risk Response / Risk Treatment

- Tindakan/kontrol yang diambil manajemen untuk mengurangi risiko sampai pada tingkat residual risk yang dapat diterima, sesuai dengan risk apetite/risk tolerance organisasi.
- Terdapat 4 kategori
  - Accept/terima
  - Share/berbagi
  - Reduce/kurangi
  - Avoid/hindari

Risk Response / Risk Treatment

Accept	• Menerima risiko yang terjadi (dalam batas toleransi risiko) dan mempertahankannya untuk tidak berkembang ke tingkat yang lebih tinggi.
Share	• Membagi risiko dengan pihak lain, misalnya: asuransi, penjaminan kredit, outsourcing, partnership, leasing, dll.
Reduce	• Mengurangi kemungkinan dan/atau dampak suatu risiko, misalnya: memperbaiki prosedur, membuat kebijakan baru, mengganti peralatan, diversifikasi produk, pelatihan, dll • Khusus untuk mengurangi dampak dilakukan dengan contingency plan, BCM/BCP.
Avoid	• Menghindari risiko dengan tidak melakukan aktivitas atau berhenti melakukan aktivitas yang menaikkan risiko.

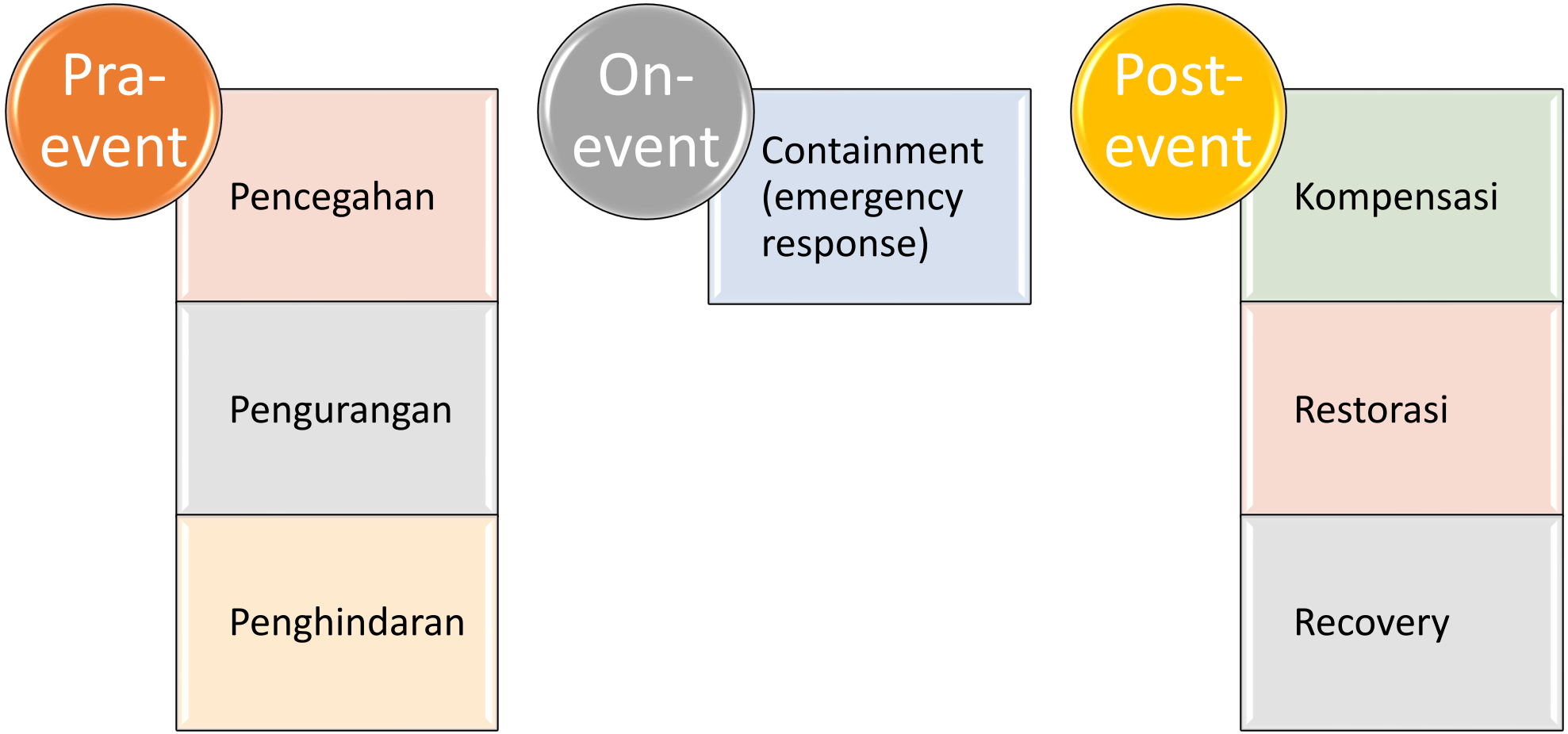

RISK ASSESSMENT RESULTS
SATISFACTORY ASSESSMENT
RISK DECISION POINT 1
RISK TREATMENT
RISK TREATMENT OPTIONS
RISK MODIFICATION
RISK RETENTION
RISK AVOIDANCE
RISK SHARING
RESIDUAL RISKS
RISK DECISION POINT 2
SATISFACTORY TREATMENT

Kunci Risk Response

Evaluasi pemilihan respon risiko mempertimbangkan :

1. Besaran risk appetite dan risk tolerance
2. Efektifitas
3. Cost and benefit
4. Kecukupan sumber daya
5. Dampak risiko paling minimum

Risk Response



Langkah Risk Response

Risiko telah ditentukan peringkatnya dan tingkat signifikansinya.

Melakukan identifikasi opsi penanganan risiko : menerima risiko, menurunkan tingkat risiko, membagi/mengalihkan risiko, dan menghindari risiko.

Melakukan kajian manfaat dan biaya (cost-benefit analysis) atas opsi penanganan risiko yang dipilih.

Melakukan persiapan untuk pelaksanaan penanganan risiko, rencana kerja mitigasi termasuk diantaranya menyusun alternatif back-up mitigasi.

Implementasi rencana penanganan risiko, diikuti dokumentasi yang lengkap, review dan monitoring secara berkala.

Monitoring Risiko

5

Apa yang dipantau?

- Pemantauan rutin terhadap kinerja actual penerapan manajemen risiko terhadap rencana awalnya.
- Memastikan cara pengendalian risiko berjalan efektif.
- Mengidentifikasikan setiap risiko-risiko baru yang muncul.
- Fokus kepada risiko-risiko yang tinggi dan kritis.
- Mengawasi risiko rendah untuk memastikan tetap dalam kategori rendah.
- Mengawasi penyimpangan dari langkah-langkah proses manajemen risiko.

Monitoring Risiko

Siapa yang melakukan pemantauan?

- Pemantauan dilakukan pada setiap jenjang organisasi.
- Metodenya :
  - On-going Monitoring

    Day-to-day review yang dilakukan oleh risk owner, risk agent dan atasan langsung. Pemantauan bersifat berkesinambungan, sehingga disiplin memonitor, mencatat, dan melaporkan ke atasan.
  - Separate Evaluations

    Dilakukan secara periodic oleh internal atau eksternal audit untuk menjaga validitas dari sistem manajemen risiko yang telah diterapkan.

Contoh Monitoring Worksheet

NO	RISK EVENT	RENCANA MITIGASI	WAKTU PELAKSANAAN MITIGASI & REALISASI MITIGASI												EVIDENCE
			TRIWULAN I 2014			TRIWULAN II 2014			TRIWULAN III 2014			TRIWULAN IV 2014			
			JAN	FEB	MAR	APR	MEI	JUN	JUL	AGU	SEPT	OKT	NOV	DES	
1	AAAAA	XXXXXX													
		XXXXXXX													
2	ZZZZZ	XXXXX													
		XXXXXX													

RENCANA MITIGASI

PELAKSANAAN MITIGASI

Output

- Terdapat proses pembelajaran
- Penyesuaian terhadap toleransi risiko, anggaran dan target organisasi
- Penyempurnaan proses manajemen risiko
- Perbaikan kerangka kerja manajemen risiko
- Meningkatkan kepatuhan terhadap regulasi
- Meningkatkan efektifitas pengendalian risiko
- Mengidentifikasi risiko-risiko baru
- Update proses bisnis
- Mendapatkan informasi yang relevan, dipercaya, dan tepat waktu

Pelaporan

6

- Pelaporan kegiatan manajemen risiko disebut dengan profil risiko.
- Berisi (minimal) :
  - Peta risiko
  - Laporan risiko-risiko signifikan/prioritas utama
  - Laporan pelaksanaan dan progres mitigasi (mengutamakan kegagalan bila ada)
  - Perubahan tingkat eksposur risiko
  - Laporan adanya risiko-risiko baru
  - Laporan pelanggaran terhadap risk tolerance
  - Laporan kekurangan dan kelemahan sistem pengendalian internal (bila ada)
  - Laporan temuan kelemahan pada tiap proses manajemen risiko (bila ada)

Terima Kasih

BADAN SIBER DAN SANDI NEGARA

Manajemen Risiko Keamanan Informasi ISO/IEC 27005 – Contoh Kasus

Direktorat Keamanan Siber dan Sandi Pemerintah Daerah

@Guruh Prasetyo Putro, S.ST., M.Si (Han)

Identifikasi Risiko di Ruang Server

- Observasi situasi pada gambar berikut.
- Identifikasikan potensi risiko (ancaman, kelemahan, dampak) yang Anda kenali!
- Template Risk Register

  https://drive.bssn.go.id/s/yeeK59akqo7nQDc