

# **Pengantar Jaminan Informasi**

Capaian Pembelajaran : Mahasiswa mampu menjelaskan konsep trust (kepercayaan) dan trustworthiness(amanah), trusted-computing(komputasi terpercaya) termasuk trusted-computing-base dan permukaan serangan, serta prinsip meminimalkan trusted-computing-base.

# Pengantar jaminan informasi (Information Assurance = IA)

- Banyak organisasi yang menghadapi tugas untuk mengimplementasikan perlindungan data dan langkah keamanan data untuk memenuhi berbagai kebutuhan.
- perlindungan ini menangani elemen yang disajikan dalam bentuk daftar pemeriksaan keamanan.
- Namun, kepatuhan individu yang hilang melatar belakangi dasar dalam jaminan informasi sebagai tindakan cepat untuk masalah perlindungan ini.
- Jaminan Informasi adalah tentang memastikan bahwa pengguna yang berwenang memiliki akses ke informasi resmi pada saat yang sah. Tidak peduli apakah informasi dalam penyimpanan, pengolahan, atau transit, dan apakah terancam oleh kedengkian atau kecelakaan.
- Sesi ini memberikan pengenalan jaminan informasi serta rincian yang akan membantu personil penyimpanan lebih memahami penerapannya di lingkungan mereka sendiri.

# Apakah Jaminan Informasi itu?

- Tindakan yang melindungi dan membela informasi dan sistem informasi dengan memastikan **ketersediaan**, **integritas**, **autentikasi**, **kerahasiaan**, dan **nonrepudiasi**.
- Langkah ini termasuk menyediakan untuk restorasi sistem informasi dengan memasukkan kemampuan **perlindungan**, **deteksi**, dan **reaksi**.

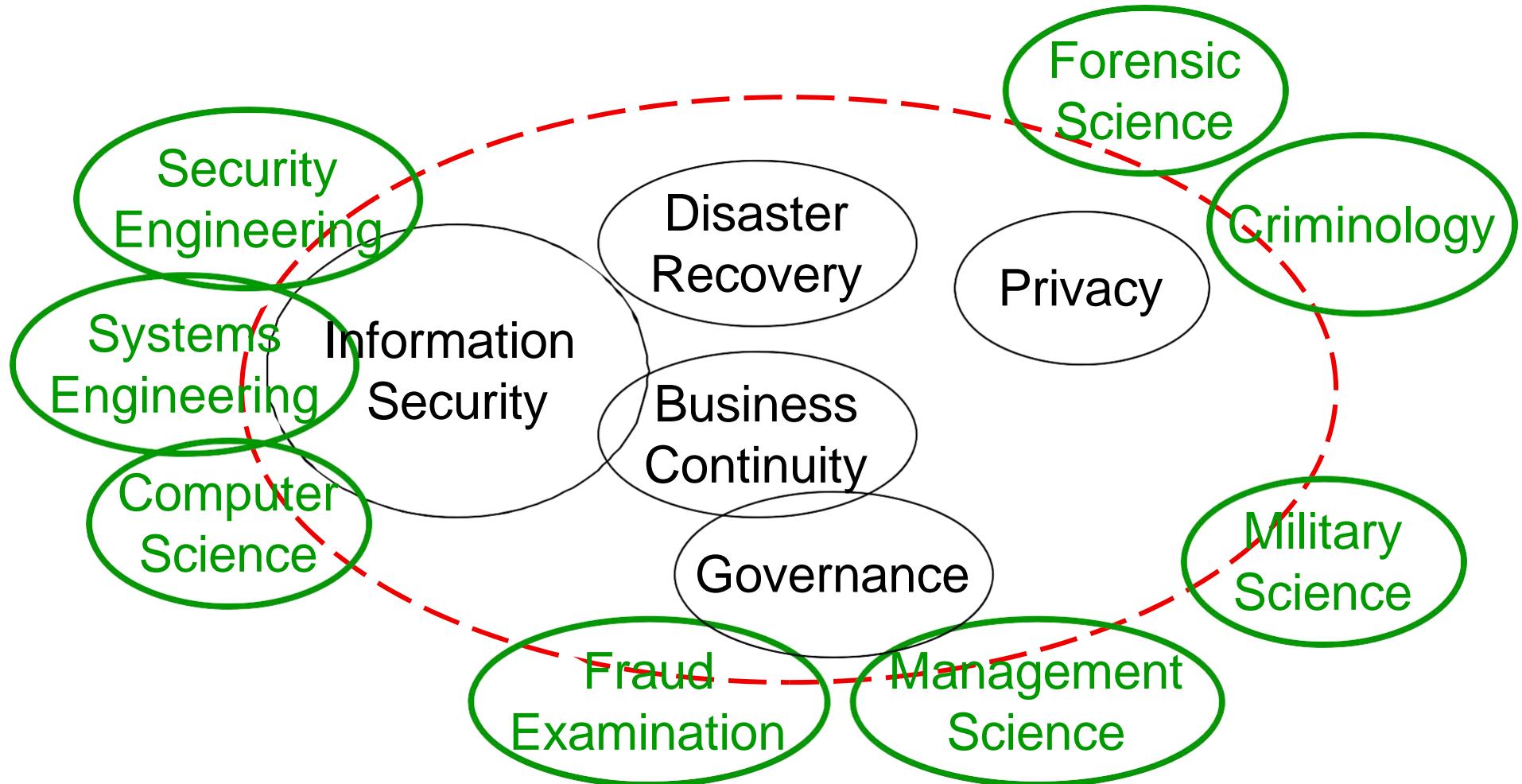
SOURCE: National Information Assurance Glossary (CNSS Instruction No. 4009)

# Apakah Jaminan Informasi itu?

- Jaminan informasi mendefinisikan dan menerapkan kumpulan kebijakan, standar, metodologi, Layanan, dan mekanisme untuk menjaga integritas misi sehubungan dengan orang, proses, teknologi, informasi, dan infrastruktur pendukung.
- Jaminan informasi menyediakan kerahasiaan, integritas, ketersediaan, kepemilikan, utilitas, keaslian, nonrepudiasi, penggunaan yang berwenang, dan privasi informasi dalam segala bentuk dan selama pertukaran.

Source: Information Assurance Architecture, Keith D. Willett, 2008, CRC Press, ISBN: 978-0-8493-8067-9

# Aspek aspek dari Jaminan Informasi



# Prinsip inti dari Jaminan Informasi

- » **Confidentiality** - untuk memastikan pengungkapan informasi hanya kepada orang yang memiliki wewenang untuk melihatnya.
- » **Integrity** - memastikan bahwa informasi tetap dalam bentuk aslinya; informasi tetap berlaku untuk maksud pencipta
- » **Availability** - informasi atau sumber informasi siap digunakan dalam parameter operasional yang tercantum
- » **Possession** - sumber informasi atau informasi tetap dalam pengawasan personel berwenang
- » **Authenticity** - sumber informasi atau informasi yang sesuai dengan kenyataan; itu tidak disalahartikan sebagai sesuatu yang tidak

# Prinsip inti dari Jaminan Informasi(lanj.)

- **Utility** - informasi tersebut sesuai untuk suatu tujuan dan dalam kondisi
- **Privacy** - memastikan perlindungan informasi pribadi dari pengamatan atau intrusi serta kepatuhan terhadap kepatuhan privasi yang relevan
- **Authorized Use** - memastikan layanan yang memakan biaya hanya tersedia bagi personil yang berwenang
- **Nonrepudiation** - memastikan pencetus pesan atau transaksi tidak mungkin menyangkal tindakannya dikemudian hari

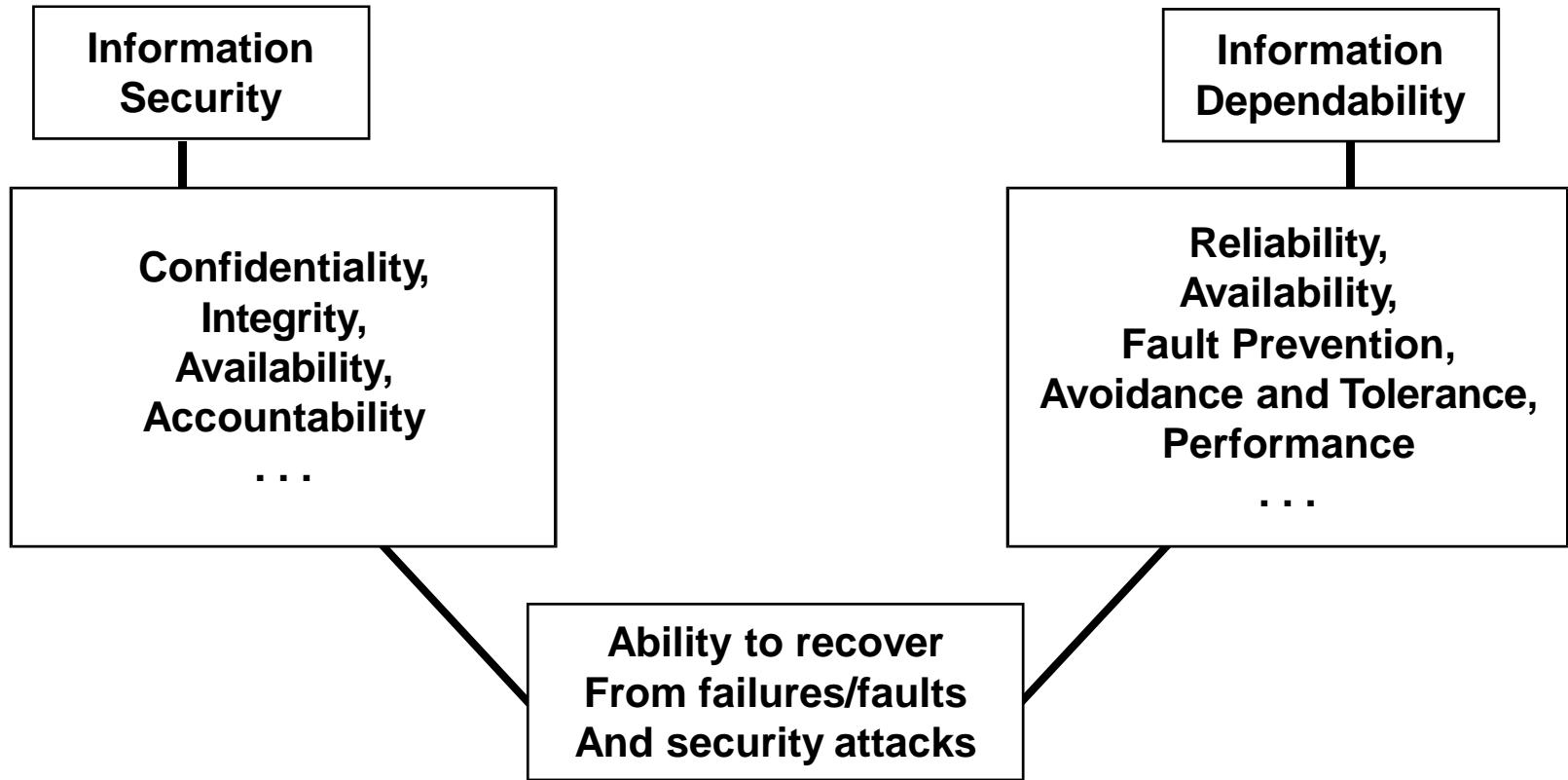
# Kerangka Kerja Arsitektur Jaminan Informasi

- Dasar struktur konseptual untuk mendefinisikan dan menggambarkan arsitektur jaminan informasi
- Risiko (driver root) dapat diungkapkan dalam hal driver bisnis dan driver teknis
- Enam tampilan arsitektural: orang, kebijakan, proses bisnis, sistem dan aplikasi, informasi/data, dan infrastruktur
- Sebuah pernyataan risiko tunggal dapat dinyatakan dari sudut pandang sembilan prinsip inti IA, masing-masing dari salah satu dari enam tampilan yang berbeda, atau 54 perspektif pada risiko tunggal.

# Proses Jaminan Informasi

- Enumerasi dan klasifikasi aset informasi (misalnya data/teknologi informasi dan nilai)
- Penilaian resiko (kerentanan dan ancaman)
- Analisis resiko (probabilitas/kemungkinan dan dampak) manajemen resiko (pengobatan)
- Uji dan Tinjau kembali
- Ulangi...

# Jaminan Informasi



Source: *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

**Beberapa kata di  
keamanan informasi**

# Jaminan Informasi vs. Keamanan Informasi (InfoSec)

- keduanya melibatkan orang, proses, teknik, dan teknologi (yaitu, administratif, teknis, dan kontrol fisik)
- Jaminan informasi dan keamanan informasi sering digunakan secara bergantian (salah)
- InfoSec difokuskan pada kerahasiaan, integritas, dan ketersediaan informasi (elektronik dan non-elektronik)
- IA memiliki konotasi yang lebih luas dan secara eksplisit mencakup keandalan, kontrol akses, dan nonrepudiasi serta penekanan yang kuat pada manajemen risiko strategis
- Standar manajemen keamanan informasi ISO (ISMS) lebih erat selaras dengan IA

# Kerangka Kerja “Keamanan” umum

- ISO/IEC 27002:2005 *The Code of Practice for Information Security Management* & ISO/IEC 27001:2006 *Information Security Management - Requirements*
- IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.1
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- Federal Financial Institutions Examination Council (FFIEC)
- National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems (Special Publication 800-53)
- Canadian Institute of Chartered Accountants (CICA), Information Technology Control Guidelines (ITCG)
- UK Office of Government Commerce (OGC), Information Technology Infrastructure Library (ITIL), Security Management

# Paradigma Keamanan

- Prinsip 1: Hacker yang menerobos sistem Anda mungkin merupakan seseorang yang Anda tahu
- Prinsip 2: Percayalah tidak satu, atau berhati-hatilah tentang siapa Anda disyaratkan untuk percaya
- Prinsip 3: Membuat penyusup percaya mereka akan tertangkap
- Prinsip 4: Lindungi di lapisan/layer
- Prinsip 5: Sementara perencanaan strategi keamanan Anda, menganggap lengkap kegagalan setiap lapisan keamanan tunggal
- Prinsip 6: Jadikan keamanan sebagai bagian dari desain awal
- Prinsip 7: Nonaktifkan layanan, paket, dan fitur yang tidak dibutuhkan
- Prinsip 8: Sebelum menyambungkan, pahami dan pastikan aman
- Prinsip 9: persiapan untuk yang terburuk

SOURCE: Peter H. Gregory, *Solaris™ Security*, © 2000 by Prentice Hall PTR, ISBN 0-13-096053-5

# Konsep dan Prinsip Keamanan Dasar

## ➤ Keamanan memerlukan

- Auditabilitas & akuntabilitas
- Kontrol akses integritas
- kerahasiaan
- Ketersediaan aset

➤ Keamanan harus hemat biaya

## ➤ Keamanan juga memerlukan

- Manajemen risiko
- Pendekatan komprehensif dan terpadu
- Manajemen siklus hidup

## ➤ Keamanan adalah elemen Integral dari menegemen suara

➤ Tanggung jawab keamanan dan akuntabilitas harus dibuat eksplisit

# Konsep dan Prinsip Keamanan Dasar

- Keamanan membutuhkan
  - pelatihan dan kesadaran
  - terus-menerus
- Keamanan harus menghormati hak etika dan Demokrasi
- Prinsip keamanan dasar lainnya
  - Titik choke
  - Konsistensi
  - Kontrol dari pinggiran pertahanan secara mendalam
  - Deny atas kegagalan
  - keragaman pertahanan
  - interdependensi
  - Override
  - Keandalan
  - kesederhanaan
  - ketepatan waktu
  - Penerapan/partisipasi Universal
  - Link paling lemah

# Pendekatan untuk menerapkan prinsip

- *Strategi Keamanan oleh Obscurity*
  - Premis dasar adalah siluman/bersembunyi
- *Strategi pertahanan perimeter*
  - Lebih dari upaya terkonsentrasi pertahanan
  - pertahanan antara "Insiders" dan "orang luar"
- *Strategi pertahanan di kedalaman (Recommended)*
  - Mempekerjakan sejumlah operasional dioperasikan dan saling melengkapi teknis dan non-teknis lapisan pertahanan
  - Dapat menggunakan kantong untuk lebih kuat daerah pertahanan

# Keamanan adalah masalah berbasis orang

Jika Anda berpikir teknologi dapat memecahkan masalah keamanan Anda, maka Anda tidak mengerti masalah dan Anda tidak mengerti teknologi.

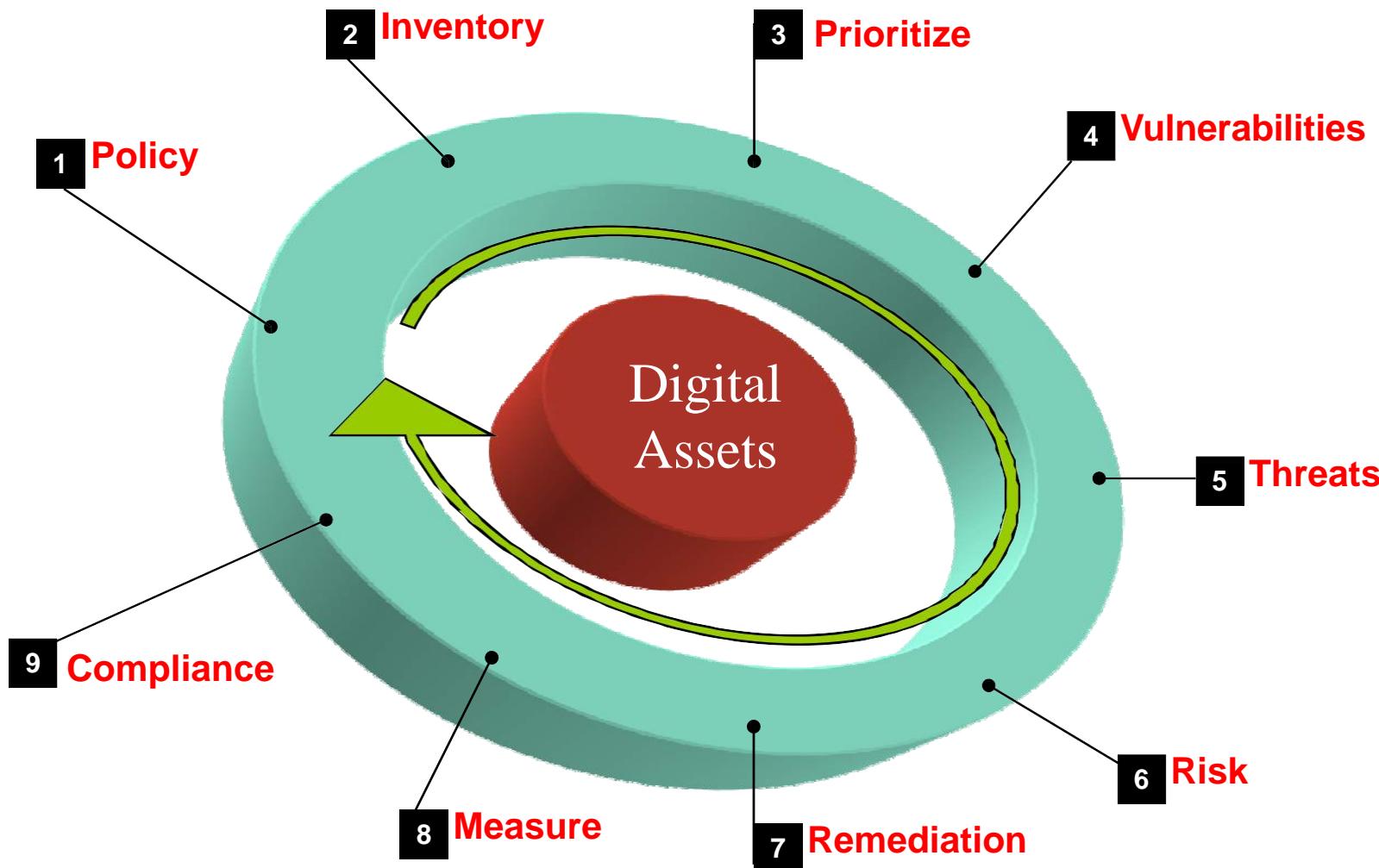
... itu jauh lebih efektif untuk memikirkan keamanan sebagai proses yang berkelanjutan dari "Risk Management" yang mencakup tidak hanya perlindungan, tetapi juga Deteksi dan mekanisme reaksi

Bruce Schneier, *Secrets & Lies*

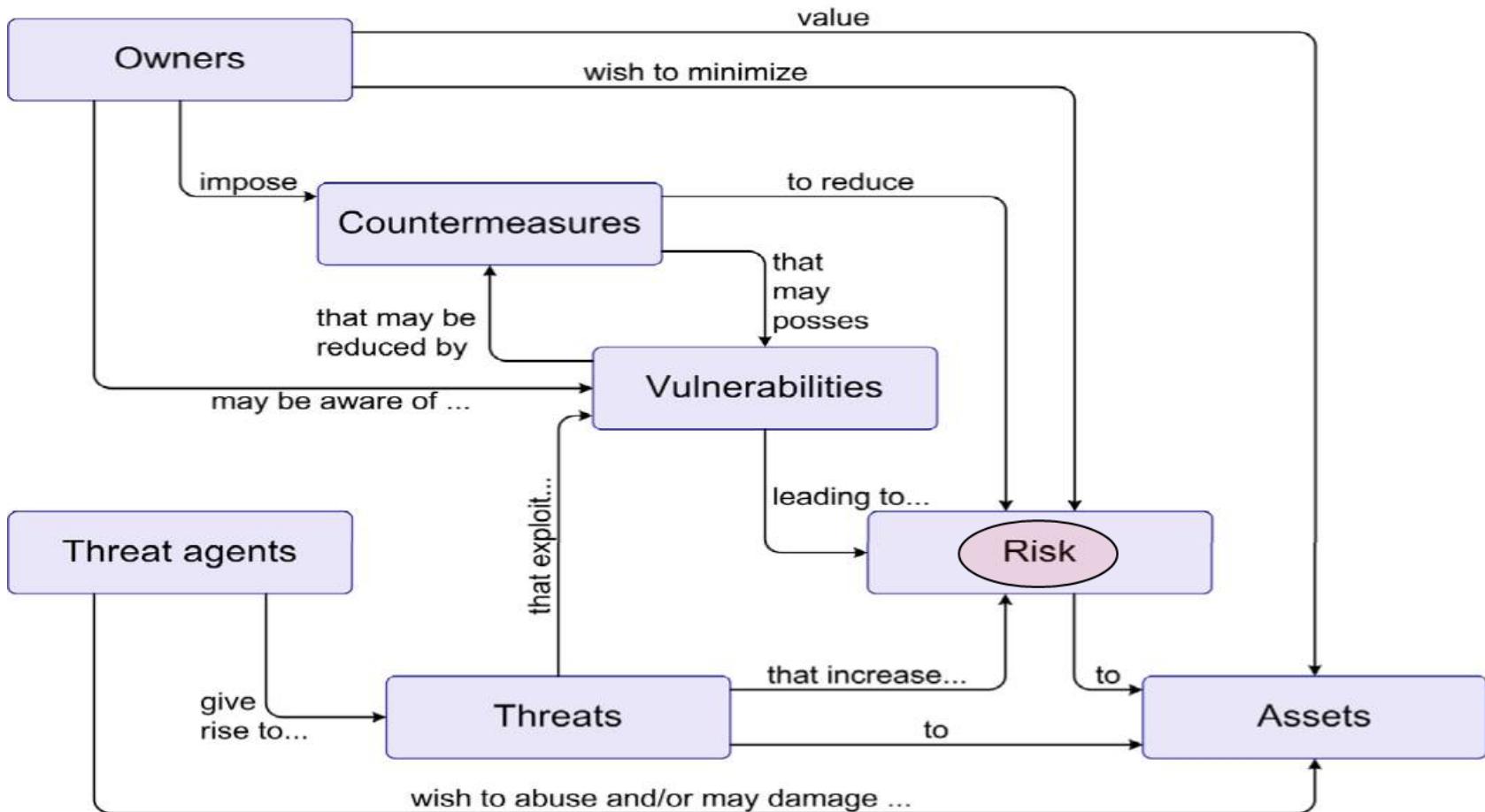
ISBN 0-471-25311-1

# **Sekilas tentang Risiko**

# Siklus hidup manajemen risiko

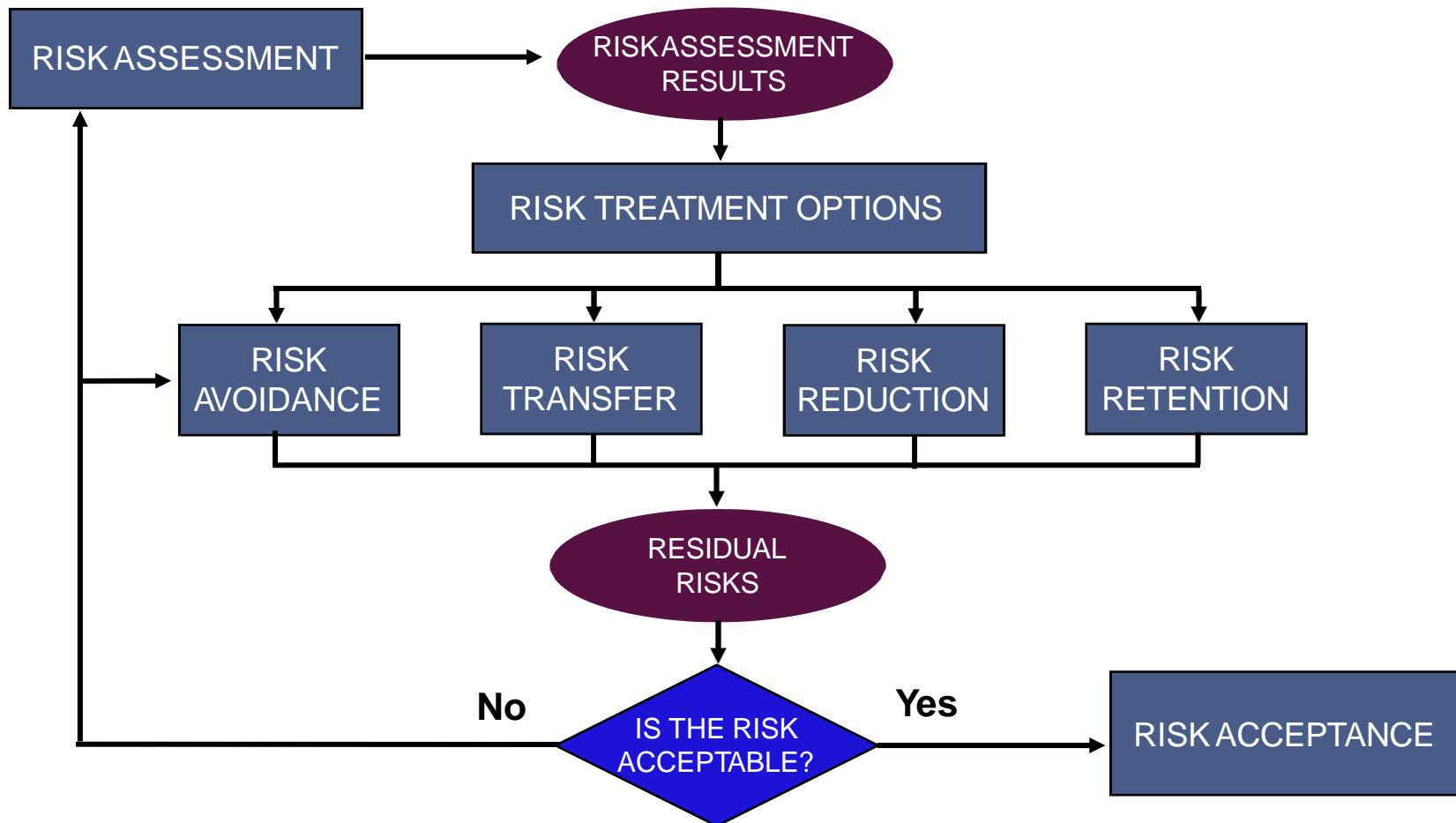


# The Security “Big Picture”



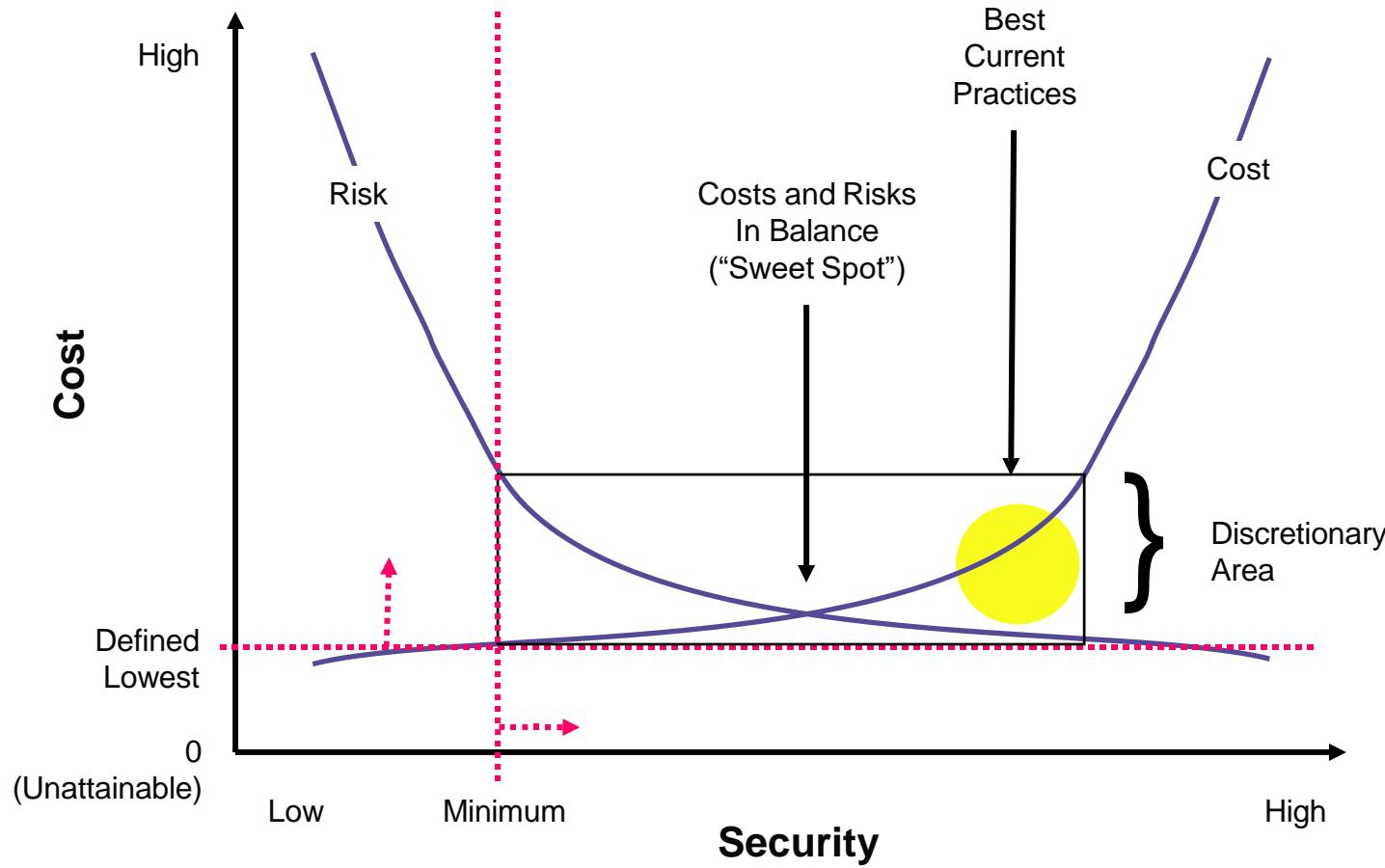
**SOURCE:** ISO/IEC 15408-1:2005, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, Common Criteria v2.3, <http://www.iso.ch>

# Proses pengambilan keputusan risiko



BASED ON: ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, <http://www.iso.ch>

# Keseimbangan Biaya dan Resiko



© 1996 – 2000 Ray Kaplan All Rights Reserved

Source: Ray Kaplan, CISSP, *A Matter of Trust*, Information Security Management Handbook, 5<sup>th</sup> Edition. Tipton & Krause, editors.

# **Final Thoughts**

# Rangkuman Jaminan Informasi

- Akar masalah di belakang Jaminan Informasi adalah risiko
- Jaminan informasi yang efektif memerlukan integrasi dari awal dan bukan setelah terjadi masalah
- Praktik bisnis yang baik harus dilengkapi dengan kebutuhan kepatuhan

# Security Versus Compliance



## Data Security

- Proaktif
- pertahanan-mendalam
- Area kontrol fisik, teknis, dan administratif
- Jenis kontrol preventif, detektif, dan korektif

## Compliance

- Reaktif
- Akuntabilitas
- Kemampuan telusuran
- Monitoring & pelaporan
- Managemen resiko
- Sering bergerak untuk keamanan

# Penutup

- Link yang lemah dalam rantai keamanan yang paling sering elemen manusia. Keamanan adalah masalah orang!
- Mengelola risiko atau mengurangi konsekuensi
- Sebuah pendekatan holistik keamanan termasuk orang, organisasi, pemerintahan, proses dan, terakhir, teknologi.
- Harapan program keamanan-menjaga organisasi dari masalah dan keluar dari Headline, sementara melakukannya untuk sesedikit mungkin uang
- Mengimplementasikan sistem firewall dan pengerasan tidak masalah keamanan lagi tetapi masalah operasional

# SNIA Security

## ➤ SNIA Security Technical Work Group (TWG)

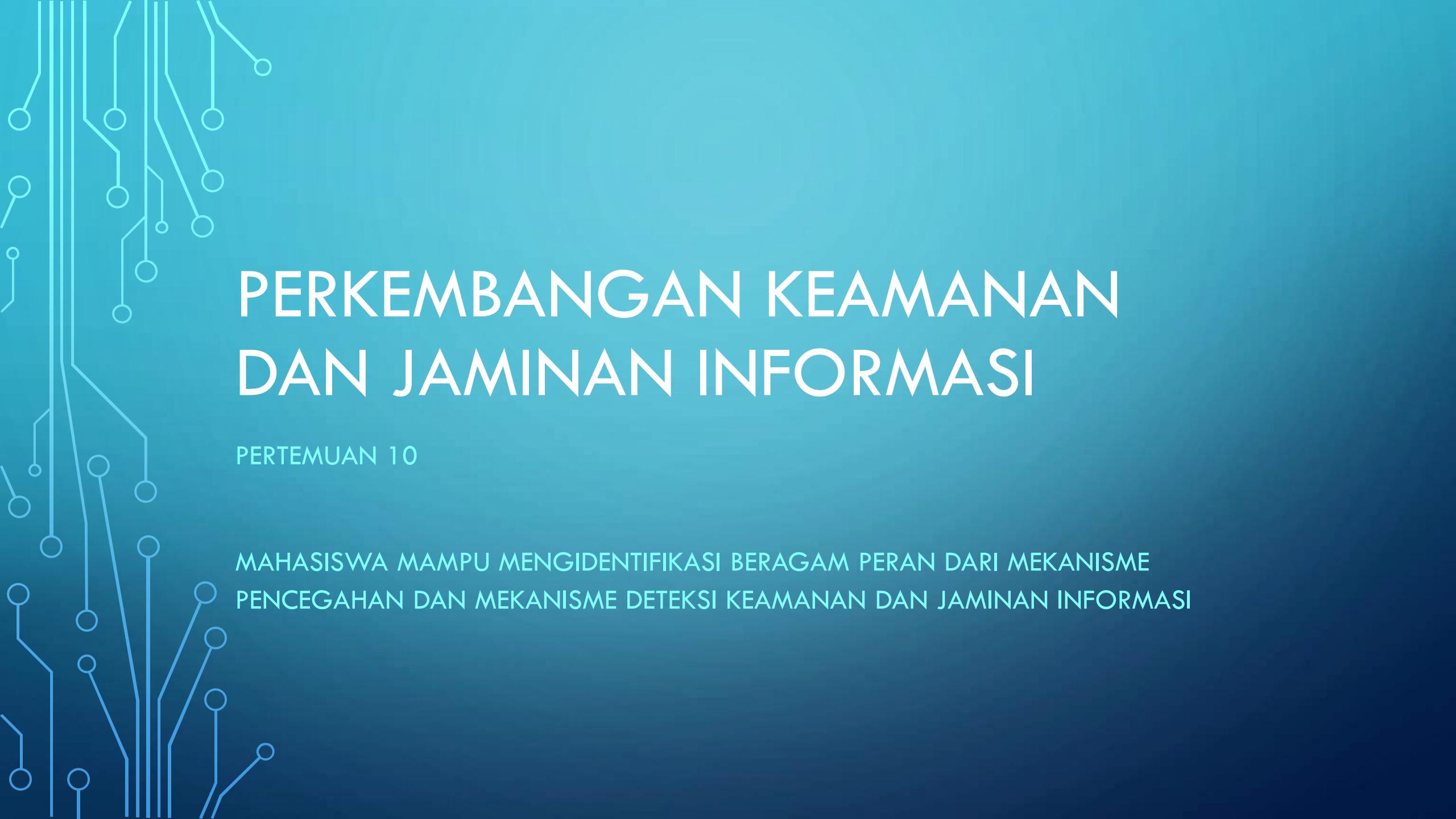
- ◆ Focus: Persyaratan, arsitektur, antarmuka, praktik, teknologi, materi pendidikan, dan terminologi untuk jaringan penyimpanan.
- ◆ ...[http://www.snia.org/tech\\_activities/workgroups/security/](http://www.snia.org/tech_activities/workgroups/security/)

## ➤ Storage Security Industry Forum (SSIF)

- ◆ Focus: Jaminan pemasaran, materi edukasi, kebutuhan pelanggan, Whitepapers, dan praktik terbaik untuk keamanan Penyimpanan.
- ◆ <http://www.snia.org/ssif>

# Useful Printed Resources

- *Information Assurance Architecture*, Keith D. Willett, 2008, CRC Press, ISBN: 978-0-8493-8067-9
- *Information Assurance - Managing Organizational IT Security Risks*, Joseph G. Boyce and Dan W. Jennings, 2002, Butterworth Heinemann, ISBN: 0-7506-7327-3
- *Information Assurance - Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, Morgan Kaufmann, ISBN: 978-0-12-373566-9.
- *A Practical Guide to Security Engineering and Information Assurance*, Debra S. Herrmann, 2001, Auerbach Publications, ISBN: 978-0-8493-1163-5
- *Information Security Architecture - An Integrated Approach to Security in the Organization*, Jan Killmeyer Tudor, 2001, AUERBACH, ISBN: 978-0-8493-9988-6
- *Enterprise Security Architecture - A Business-Driven Approach*, Sherwood, Clark, Lynas, 2005, CPM Books ,ISBN: 978-1-57820-318-5



# PERKEMBANGAN KEAMANAN DAN JAMINAN INFORMASI

PERTEMUAN 10

MAHASISWA MAMPU MENGIDENTIFIKASI BERAGAM PERAN DARI MEKANISME  
PENCEGAHAN DAN MEKANISME DETEKSI KEAMANAN DAN JAMINAN INFORMASI

# TINJAUAN PENDEKATAN HISTORIS UNTUK KEAMANAN INFORMASI DAN JAMINAN INFORMASI, KHUSUSNYA PENDEKATAN UNTUK

- Keamanan sistem,
- Keselamatan,
- keandalan dicapai,
- Keterbatasan terhadap teknologi

# PENDEKATAN SEJARAHINI TERBAGI DALAM TUJUH KATEGORI UTAMA:

- 1. keamanan fisik
- 2. Keamanan komunikasi (COMSEC)
- 3. keamanan komputer (COMPUSEC)
- 4. keamanan informasi (INFOSEC)
- 5. keamanan operasi (OPSEC)
- 6. keamanan sistem
- 7. keandalan sistem

# KEAMANAN FISIK

Keamanan fisik didefinisikan sebagai: perlindungan pada

- ✓ perangkat keras,
- ✓ perangkat lunak, dan
- ✓ data

terhadap ancaman fisik untuk mengurangi atau mencegah gangguan pada operasi dan layanan dan/atau hilangnya aset.

# TUJUAN DARI KEAMANAN FISIK

adalah untuk melindungi sumber daya sistem fisik (sebagai lawan dari sumber daya sistem Logis) dari

- (1) kerusakan fisik yang dapat mengganggu operasi dan
- (2) pencurian.

# SECARA HISTORIS, RENCANA KEAMANAN FISIK DIFOKUSKAN PADA EMPAT TANTANGAN UTAMA:

- melindungi sumber daya komputer dan komunikasi dari kerusakan akibat kebakaran, air, radiasi, gempa bumi, atau bencana alam lainnya
- menjaga suhu, kelembaban, debu, dan tingkat getaran yang sesuai
- memberikan tingkat daya yang berkelanjutan meskipun lonjakan sementara, brownouts, dan kegagalan daya
- mengontrol akses fisik ke komputer dan sumber daya komunikasi untuk personil resmi yang dikenal

# KEAMANAN KOMUNIKASI (COMSEC)

- adalah kumpulan kegiatan rekayasa yang dilakukan untuk melindungi kerahasiaan, integritas, dan ketersediaan data sensitif saat sedang ditransmisikan antara sistem dan jaringan.
- Kerahasiaan memastikan bahwa hanya penerima yang dituju yang menerima dan dapat menafsirkan data yang ditransmisikan.

# AKIBAT YANG HARUS DIMINIMALKAN TERKAIT KOMUNIKASI KEAMANAN:

- potensi kerugian dari pencurian informasi,
- kerugian finansial,
- hilangnya keunggulan kompetitif,
- hilangnya kepercayaan publik,
- hilangnya privasi,
- pencemaran nama baik,
- kompromi keamanan nasional,
- dan hilangnya hak kekayaan intelektual.

# INTEGRITAS

- integritas memastikan bahwa data yang diterima adalah representasi akurat dari data yang dikirim.
- Ketersediaan memastikan bahwa data yang diterima dalam waktu transmisi yang ditentukan, ditambah atau minus faktor toleransi Reasonable.

# DOD 5200,28-M MENERAPKAN PRINSIP COMSEC UNTUK

- saluran komunikasi dan link,
- Multiplexer,
- switch pesan,
- jaringan telekomunikasi dan antarmuka,
- Kontrol emanasi

# COMSEC BERFOKUS PADA PERLINDUNGAN TRANSMISI DATA END-TO-END

- Data yang meninggalkan pusat komputer adalah multiplexed dan dienkripsi, kadang-kadang lebih dari sekali.
- Sistem kunci rahasia digunakan, dan kunci diubah secara bersamaan pada kedua ujung link komunikasi secara teratur.
- Algoritma enkripsi dapat diimplementasikan dalam perangkat keras atau perangkat lunak.

# INFORMASI TERBARU TENTANG PERKEMBANGAN PKCS DAPAT DITEMUKAN DI: [WWW.RSA.COM](http://WWW.RSA.COM)

- PKCS #1 v 2.1 — RSA cryptography Standard, (draft) September 17, 1999
- PKCS #3 v 1.4 — standar perjanjian kunci Diffie-Hellman, 1 November, 1993
- PKCS #5 v 2.0 — standar kriptografi berbasis kata sandi, 25 Maret 1999
- PKCS #6 v 1.5-diperpanjang sertifikat sintaks standar, 1 November 1993
- PKCS #7 v 1.5 — sintaks pesan kriptografi standar, 1 November 1993
- PKCS #8 v 1.2 — sintaks informasi kunci privat standar, 1 November 1993
- PKCS #9 v 2.0 — kelas objek yang dipilih dan jenis atribut, 25 Februari 2000
- PKCS #10 v 1.7 — sintaks permintaan sertifikasi standar, 26 Mei 2000
- PKCS #11 v 2.11 — kriptografi token interface Standard, (draft) November 2000
- PKCS #12 v 1.0 — sintaks pertukaran informasi pribadi, 24 Juni 1999
- PKCS #13 (proposal) — standar kriptografi Curve Elliptic, 7 Oktober 1998
- PKCS #15 v 1.1 — kriptografi token informasi sintaks standar, 6 Juni 2000

# PRINSIP COMSEC: KEBUTUHAN UNTUK KERAHASIAAN DATA, INTEGRITAS, DAN KETERSEDIAAN SELAMA TRANSMISI TETAP.

## PADA MASA LALU

- diterapkan pada end-to-end link communication yang ditransmisikan textual, suara (teknologi STU), dan data gambar secara terpisah.

## PADA SAATINI

- diterapkan pada data audio, video, Gambar, dan textual yang ditransmisikan bersama di berbagai jenis jaringan dan topologi, seperti ISDN, ATM, SONET, frame relay, vpn, dan wireless.

## SCHNEIER MENGUTIP BEBERAPA KELEMAHAN UMUM DALAM MENGIMPLEMENTASIKAN ALGORITMA ENKRIPSI

- Tidak merusak plaintext setelah enkripsi
- Penggunaan file swapping sementara atau virtual
- Buffer meluap
- Deteksi/koreksi kesalahan lemah
- Akun escrow kunci
- Penggunaan parameter default
- Kemampuan untuk merekayasa balik produk

# TIGA KEKHAWATIRAN HARUS DIATASI SAAT MENGIMPLEMENTASIKAN ENKRIPSI:

- waktu dan sumber daya sistem yang dikonsumsi untuk melakukan enkripsi dan dekripsi
- Kapan melakukan enkripsi; yaitu, apa lapisan dalam protokol komunikasi suite
- algoritma enkripsi apa yang digunakan atau apa kekuatan enkripsi/tingkat perlindungan yang diperlukan

# KEAMANAN KOMPUTER (COMPUSEC)

- Keamanan komputer didefinisikan sebagai:  
mencegah, mendekksi, dan meminimalkan konsekuensi  
dari tindakan yang tidak sah oleh pengguna (berwenang  
dan tidak sah) dari sistem komputer.

# PENGGUNA

- pengguna yang berwenang, atau orang dalam yang berusaha untuk melakukan sesuatu yang mereka tidak memiliki izin,
- pengguna unauthorized, atau orang luar, yang mencoba untuk masuk ke sistem

# ISTILAH "SISTEM KOMPUTER"

- berlaku untuk setiap jenis atau konfigurasi perangkat keras dan perangkat lunak, termasuk pemrosesan terdistribusi, aplikasi klien/server, perangkat lunak tertanam, dan aplikasi internet.

# COMPUSEC TERUTAMA BERKAITAN DENGAN MELINDUNGI DATA SAAT DIPROSES DAN DISIMPAN

## BEBERAPA ANCAMAN TERHADAP DATA YANG DISIMPAN

### ANCAMAN AKTIF

- Menimpa
- Memodifikasi
- Menyisipkan
- Menghapus
- Memblokir akses untuk

### ANCAMAN PASIF

- browsing
- agregasi dan inferensi
- memutar
- Kebocoran
- menyalin dan mendistribusikan

## MODE SISTEM YANG AMAN DIOPERASIKAN:

- Mode Keamanan Terkontrol
- Mode Keamanan Khusus.
- Mode keamanan multi-level
- Mode keamanan tinggi.

## MODE KEAMANAN TERKONTROL.

Beberapa pengguna dengan akses ke sistem tidak memiliki izin keamanan atau kebutuhan-untuk-tahu untuk semua materi diklasifikasikan terkandung dalam sistem. Pemisahan dan kontrol pengguna dan bahan diklasifikasikan atas dasar izin keamanan dan kelas keamanan tidak di bawah kontrol sistem operasi

## MODE KEAMANAN KHUSUS.

Sistem komputer dan semua periferal secara eksklusif digunakan dan dikontrol oleh pengguna atau kelompok pengguna tertentu yang memiliki izin keamanan dan perlu tahu untuk memproses kategori tertentu dan jenis materi rahasia.

## MODE KEAMANAN MULTI-LEVEL.

Sistem memungkinkan berbagai kategori dan jenis bahan diklasifikasikan untuk secara bersamaan disimpan dan diproses dan akses selektif ke materi tersebut secara bersamaan oleh pengguna dibiarkan dan pengguna memiliki keamanan yang berbeda izin dan perlu tahu. Pemisahan personil dan bahan atas dasar izin keamanan dan perlu untuk tahu dicapai oleh sistem operasi dan perangkat lunak sistem terkait.

## MODE KEAMANAN TINGGI.

Semua komponen sistem dilindungi sesuai dengan persyaratan untuk kategori klasifikasi tertinggi dan jenis bahan yang terkandung dalam sistem. Semua personil yang memiliki akses ke sistem memiliki izin keamanan tetapi tidak harus kebutuhan-untuk-tahu untuk semua materi yang terkandung dalam sistem. Desain dan pengoperasian sistem harus menyediakan untuk pengendalian secara bersamaan tersedia bahan diklasifikasikan berdasarkan kebutuhan-untuk-tahu.

# PERSYARATAN STANDAR COMPUSEC PERTAMA DIKENAKAN PADA SISTEM KOMPUTER

- memastikan bahwa dua atau lebih kontrol independen harus mal-fungsi secara bersamaan untuk pelanggaran sistem keamanan terjadi (pertahanan secara mendalam)
- memonitor perlindungan variabel keadaan untuk mengontrol pelaksanaan operasi dan mencegah operasi illegal
- mengontrol akses ke lokasi memori
- memastikan terjemahan yang dapat diprediksi ke dalam kode objek
- melindungi register melalui deteksi kesalahan dan redundansi cek
- melakukan pemeriksaan paritas dan memeriksa alamat terikat semua Operand/operator
- menggunakan menyela untuk mengontrol kerusakan operator

# PERSYARATAN STANDAR COMPUSEC PERTAMA DIKENAKAN PADA SISTEM KOMPUTER (LANJUTAN)

- memverifikasi hak baca, tulis, Edit, dan Hapus
- pelabelan materi diklasifikasikan
- kliring memori residu, menimpa memori sebelum digunakan kembali
- Logging upaya untuk mengakali tindakan keamanan sistem
- mengimplementasikan pengamanan keamanan selama pematiian, restart, dan start-up sistem yang terjadwal dan tidak terjadwal
- mempertahankan jejak audit transaksi terkait keamanan, seperti log on/log off upaya dan waktu, informasi tentang sumber daya yang diakses, dibuat, berubah, dihapus, output yang dihasilkan, dll.
- mempekerjakan pengguna dan terminal id sebagai bagian dari kontrol akses dan sistem otentikasi

# RINGKASAN THE ORANGE BOOK TERPERCAYA SISTEM KOMPUTER KRITERIA EVALUASI (TCSEC) DIVISI

Devisi evaluasi	Kelas evaluasi	Tingkat kepercayaan
A. Perlindungan terverifikasi	A1-desain terverifikasi	tertinggi
B. Perlindungan wajib	B3-domain keamanan	
	B2-perlindungan terstruktur	
	B1 Perlindungan keamanan berlabel	
C. kewenangan perlindungan	C2-perlindungan akses dikendalikan	
	C1-perlindungan keamanan discretionary	
D. minimal perlindungan	D1-minimal perlindungan terendah	

# TIGA SASARAN COMPUSEC

- Kontrol akses,  
fitur desain yang melindungi sistem IA-kritis dan IA-terkait, applications, dan data dengan mencegah akses yang tidak sah dan tidak beralasan ke sumber daya ini.
- otentikasi,  
menetapkan, memverifikasi, atau membuktikan validitas identitas pengguna, proses, atau sistem yang diklaim.
- jejak audit  
sekumpulan catatan yang secara kolektif menyediakan bukti dokumenter dari sumber daya sistem yang diakses oleh pengguna atau proses untuk membantu dalam melacak dari transaksi asli maju dan mundur dari catatan dan laporan untuk transaksi sumber komponen mereka.

# KEAMANAN INFORMASI (INFOSEC)

- Paradigma baru menggabungkan COMSEC dan COMPUSEC
- INFOSEC didefinisikan sebagai:  
perlindungan informasi terhadap pengungkapan, pengalihan, atau penghancuran yang tidak sah, baik disengaja atau disengaja.
- INFOSEC dapat diaplikasikan untuk semua jenis aplikasi perangkat lunak, arsitektur sistem, atau kebutuhan keamanan.
- Jaminan keamanan memberikan alasan untuk keyakinan bahwa produk atau sistem TI memenuhi tujuan keamanannya.

# TEKNIK EVALUASI JAMINAN KEAMANAN INFORMASI

- Analisis dan pemeriksaan proses dan prosedur
- Memeriksa bahwa proses dan prosedur sedang diterapkan
- Analisis korespondensi antara representasi desain TOE
- Analisis dari desain TOE representasi terhadap persyaratan
- Verifikasi bukti
- Analisis dokumen panduan
- Analisis tes fungsional dikembangkan dan hasil yang diberikan pengujian fungsional independen
- Analisis untuk kerentanan (termasuk hipotesis Cacat)
- Pengujian penetrasi

# VALIDITAS DOKUMENTASI DAN HASIL PRODUK IT ATAU SISTEM IT DIUKUR OLEH AHLI EVALUATOR DENGAN MENINGKATKAN PENEKANAN

- Lingkup : bagian dari produk IT atau sistem termasuk dalam evaluasi
- Kedalaman : tingkat desain dan detail pelaksanaan dievaluasi
- Kekakuan/rigor : penerapan upaya dalam terstruktur, cara formal

# LIMA TINGKAT KEMAMPUAN REKAYASA KEAMANAN KPA (KEY PROCESS AREAS)

- 0 — tidak dilakukan
- 1 — dilakukan secara informal
- 2 — direncanakan dan dilacak
- 3 — didefinisikan dengan baik
- 4 — dikontrol secara kuantitatif
- 5 — terus meningkatkan

# SSE-CMM MENGINDEKASI 11 BIDANG PROSES KUNCI REKAYASA KEAMANAN

- PA01 — mengelola kontrol keamanan
- PA02 — menilai dampak
- PA03 — menilai risiko keamanan
- PA04 — menilai ancaman
- PA05 — menilai kerentanan
- PA06 — membangun argumen jaminan
- PA07 — koordinat keamanan
- PA08 — memantau postur keamanan
- PA09 — memberikan masukan keamanan
- PA10 — menentukan kebutuhan keamanan
- PA11 — memverifikasi dan memvalidasi keamanan

# KEAMANAN OPERASI (OPSEC)

- keamanan Operasi atau OPSEC didefinisikan sebagai:  
pelaksanaan prosedur operasional standar yang menentukan sifat dan frekuensi interaksi antara pengguna, sistem, dan sumber daya sistem, yang tujuannya adalah untuk:
  - (1) mempertahankan sistem dalam keadaan aman yang dikenal setiap saat, dan
  - (2) mencegah pencurian, penghancuran, perubahan, atau sabotase terhadap sumber daya sistem yang tidak disengaja atau tidak.

- OPSEC menangani masalah keamanan yang terkait dengan pengoperasian suatu sistem.
- OPSEC lebih terlibat dengan masalah personil, tanggung jawab staf, dan tugas daripada tindakan keamanan lainnya.
- OPSEC menganggap kedua ancaman Insider dan luar.
- Untuk mengilustrasikan, satu persyaratan historis OPSEC dikenal sebagai "Man-In-The-loop." Persyaratan operasional ini menyatakan bahwa pesan elektronik (dan beberapa kali cetakan hardcopy) harus ditinjau oleh seseorang, untuk memverifikasi bahwa tanda keamanan sudah benar, sebelum mereka dapat dilepaskan atau diteruskan.
- Information dianggap terlalu sensitif untuk mengandalkan pemrosesan otomatis saja.

# ITEM UNTUK ALAMAT DALAM PROSEDUR OPSEC

A. personil operasi (pengguna, administrator sistem, trainee, pemeliharaan staf, pengunjung, dll)

1. keamanan Clearance, pemeriksaan latar belakang, lencana
2. bukti kompetensi staf
3. mencari koper, dompet, ransel, dll saat memasuki/meninggalkan bangunan
4. pelatihan staf tentang fitur keamanan dan tanggung jawab
5. mendefinisikan kebijakan bekerja sendiri, setelah jam kerja, dari rumah, atau saat bepergian (akses jarak jauh)
6. mendefinisikan kebijakan untuk mengambil komputer, laporan, file elektronik dari kantor

B. software/data operasi (teks, Gambar, audio, video)

1. jadwal untuk melakukan pemeriksaan integritas sistem dan data, pencadangan, pembuatan Arsip
2. jadwal dan prosedur untuk menghapus dan membuang materi sensitif, elektronik dan hardcopy
3. prosedur penyimpanan di luar lokasi
4. pelabelan data yang diklasifikasikan atau sensitif saat disimpan, diproses, ditampilkan, ditransmisikan, atau dicetak
5. mendefinisikan kebijakan untuk menyimpan disket dan media lainnya
6. mengontrol akses ke arsip
7. mendefinisikan Arsip Trail audit dan menimpa prosedur dan jadwal
8. menetapkan kebijakan untuk menggunakan kembali media penyimpanan elektronik
9. prosedur dan jadwal untuk mengeksekusi perangkat lunak virus scan pada server dan workstation pengguna
10. prosedur dan jadwal untuk memperbarui perangkat lunak virus scan
11. situs dan aplikasi khusus perangkat lunak dan data operasi

### C. administrasi operasi

1. mendefinisikan sistem jam dapat diakses, dan jenis transaksi yang dapat dilakukan selama jam tersebut
2. penjadwalan pemeliharaan preventif
3. mendefinisikan kondisi yang harus memicu shutdown darurat, otomatis atau operator dibantu, dari node komunikasi, sumber daya sistem, atau seluruh system
4. mendefinisikan kebijakan apakah atau tidak PC harus dimatikan sementara seseorang yang jauh dari meja mereka, saat makan siang, semalam, dan penggunaan screen saver dan layar privasi
5. menentukan seberapa sering kata sandi dan data autentikasi lainnya harus diubah dan diverifikasi
6. menentukan seberapa sering hak akses kontrol dan privilese harus ditinjau dan diperbarui
7. mendefinisikan prosedur untuk mengakhiri account pengguna biasanya dan secara darurat
8. jadwal dan prosedur untuk melakukan inspeksi keamanan, penilaian keamanan, dan pemeriksaan yang aman
9. jadwal dan prosedur untuk mengubah kombinasi
10. prosedur Pass property
11. jadwal dan prosedur untuk mengelola distribusi, pembuatan, pembaruan, Penyimpanan, penggantian, dan pencabutan materi kriptografi dan token keamanan lainnya

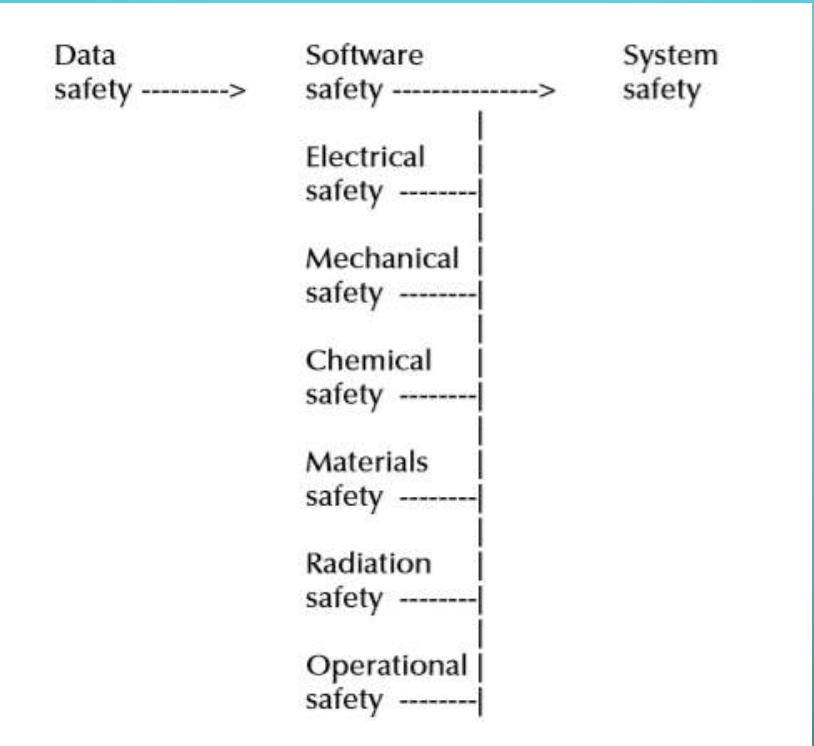
- OPSEC relatif mudah pada zaman mainframe dan pusat komputer; telah menjadi jauh lebih kompleks hari ini diberikan Mobile computing, telecommuting, klien/server aplikasi, dan aplikasi internet.

# KEAMANAN SISTEM

- Keamanan sistem didefinisikan sebagai:  
*penerapan prinsip rekayasa dan manajemen, kriteria, dan teknik untuk mencapai risiko kecelakaan yang dapat diterima, dalam constraints efektivitas operasional, waktu, dan biaya, di seluruh fase siklus hidup sistem.*

# KATEGORI KESELAMATAN PERANGKAT LUNAK:

- **Keselamatan-perangkat lunak kritis:** perangkat lunak yang melakukan atau mengontrol fungsi yang, jika dieksekusi keliru atau jika mereka gagal untuk mengeksekusi dengan benar, bisa langsung menimbulkan cedera serius kepada orang, properti, dan/atau lingkungan atau menyebabkan hilangnya nyawa.
- **Perangkat lunak yang berhubungan dengan keselamatan:** perangkat lunak yang melakukan atau mengontrol fungsi yang diaktifkan untuk mencegah atau meminimalkan efek kegagalan sistem kritis keselamatan.
- **Perangkat lunak terkait nonsafety:** perangkat lunak yang melakukan atau mengontrol func-tions yang tidak terkait dengan keselamatan.



# TUGAS DAN AKTIVITAS KEAMANAN SISTEM YANG DIBUTUHKAN OLEH MIL-STD-882D

- **program keselamatan**
  1. 102 Rencana program keamanan sistem
  2. 104 ulasan keamanan dan audit
  3. 105 kelompok kerja keselamatan
  4. 106 bahaya pelacakan

- **Analisa risiko**
  1. 201 awal daftar bahaya
  2. 202 awal Hazard analisis, fungsional FMECA
  3. 204 subsistem analisis bahaya, desain FMECA
  4. 205 sistem analisis bahaya, antarmuka FMECA
  5. 206 studi HAZOP



# KEANDALAN SISTEM

- Keandalan sistem adalah gabungan dari predictions atau perkiraan keandalan perangkat keras dan perangkat lunak untuk lingkungan operasional tertentu. Keandalan perangkat keras didefinisikan sebagai:
- kemampuan item dengan benar melakukan fungsi yang diperlukan di bawah kondisi tertentu dalam lingkungan operasional tertentu untuk jangka waktu yang ditetapkan.

# KEANDALAN PERANGKAT LUNAK DIDEFINISIKAN SEBAGAI

- *ukuran keyakinan bahwa perangkat lunak menghasilkan hasil yang akurat dan konsisten yang dapat diulang, di bawah beban rendah, normal, dan puncak, dalam lingkungan operasional yang dituju.*

# KETERBATASAN MODEL KEANDALAN PERANGKAT LUNAK DI AWALI OLEH

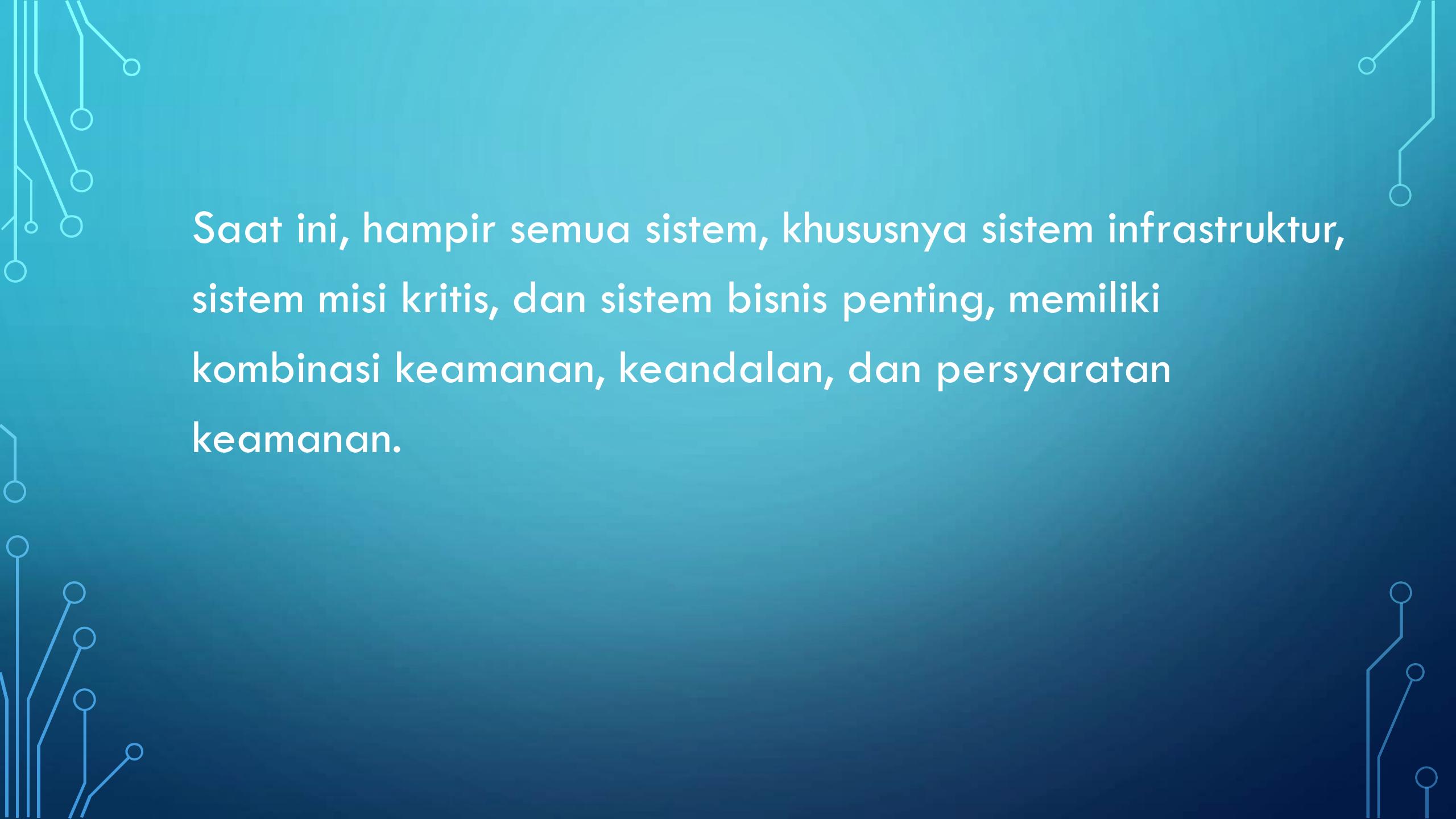
- mereka tidak membedakan antara jenis kesalahan ditemukan atau diprediksi akan tetap dalam perangkat lunak (fungsional, kinerja, keselamatan, reli-kemampuan, dll).
- mereka tidak membedakan antara tingkat keparahan konsekuensi dari kesalahan (tidak signifikan, marjinal, kritis, bencana) ditemukan atau diprediksi akan tersisa dalam perangkat lunak.
- mereka tidak memperhitungkan kesalahan account ditemukan oleh teknik selain pengujian (misalnya, analisis statis) atau sebelum tahap pengujian.

# TUJUAN DARI REKAYASA KEANDALAN

- adalah untuk memastikan bahwa sistem dan semua komponennya memamerkan Perfor-Mance yang akurat, konsisten, berulang, dan dapat diprediksi dalam kondisi tertentu. Berbagai analisis, Desain, dan teknik verifikasi, seperti yang dibahas dalam Lampiran B, digunakan sepanjang siklus hidup untuk mencapai tujuan ini. Dokumentasi pengguna saat ini dan menyeluruh adalah bagian penting dari proses ini karena akan menjelaskan operasi yang benar dari sistem, aplikasi yang sistem harus dan tidak boleh digunakan, dan prosedur untuk pencegahan, adaptif, dan perbaikan pemeliharaan.

# RINGKASAN

- Telah kita kaji tujuh pendekatan historis untuk keamanan informasi/IA: keamanan fisik, keamanan komunikasi (COMSEC), keamanan komputer (COM-PUSEC), keamanan informasi (INFOSEC), keamanan operasi (OPSEC), keselamatan sistem, dan keandalan sistem.
- Berbagai teknik digunakan oleh pendekatan historis ini untuk mencapai dan menjaga kerahasiaan informasi, data dan integritas sistem dan ketersediaan.
- Semua pendekatan harus berkembang dan perlu terus berkembang sesuai dengan perubahan dalam teknologi dan lingkungan operasional, Profile, dan misi.

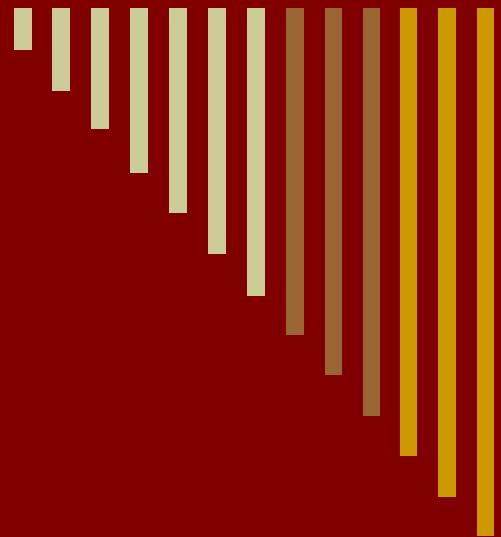


Saat ini, hampir semua sistem, khususnya sistem infrastruktur, sistem misi kritis, dan sistem bisnis penting, memiliki kombinasi keamanan, keandalan, dan persyaratan keamanan.

## Ringkasan dari berbagai peran yang dimainkan oleh pendekatan historis informasi keamanan/IA

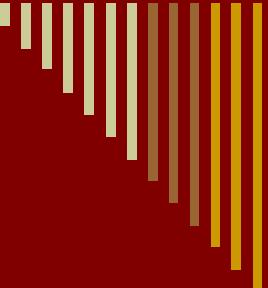
Tipe Aktifitas IA	Peran dan Tujuan
Keamanan fisik	melindungi sumber daya sistem dari kerusakan fisik yang operasi dan layanan yang mengganggu. Lindungi sistem fisik sumber daya dari pencurian.
Keamanan Komunikasi (COMSEC)	melindungi kerahasiaan, integritas, dan ketersediaan data keamanan saat ditransmisikan antara sistem dan Jaringan.
Keamanan Komputer(COMPUSEC)	mencegah, mendeteksi, dan meminimalkan konsekuensi dari tindakan yang tidak sah oleh pengguna (berwenang dan tidak sah) sistem komputer.
Keamanan Informasi (INFOSEC)	Melindungi informasi dari pengungkapan yang tidak sah, transfer, atau penghancuran, apakah disengaja atau disengaja.
Keamanan operasi (OPSEC)	Operasi keamanan menerapkan standar prosedur operasional yang menentukan sifat dan frekuensi interaksi antara pengguna, dan sumber daya sistem; yang tujuannya adalah untuk: <ol style="list-style-type: none"> <li>(1) memelihara sistem dalam keadaan aman yang diketahui setiap saat, dan</li> <li>(2) mencegah pencurian yang tidak disengaja atau disengaja, perubahan, atau sabotase sumber daya sistem.</li> </ol>
Keamanan sistem	mencapai risiko kecelakaan yang dapat diterima, dalam efektivitas operasional, waktu, dan biaya di seluruh fase siklus hidup sistem.
Keandalan sistem	mencapai kinerja fungsional yang benar di bawah beberapa dalam lingkungan operasional tertentu untuk suatu kondisi jangka waktu tertentu





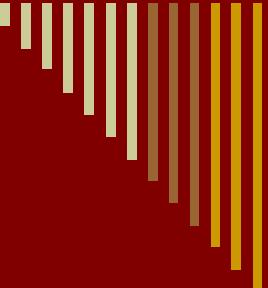
# Batasan Sistem

Priyo Sidik Sasongko



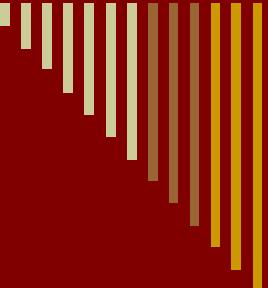
# Kemampuan akhir tiap tahapan pembelajaran

- Mahasiswa mampu mendeskripsikan isu keamanan yang muncul pada batas-batas di antara banyak komponen.



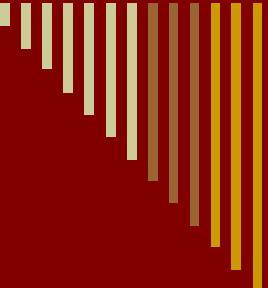
# Keamanan dan Jaminan Informasi Efektif

- harus sesuai dengan realitas teknologi saat ini
  - Pengolahan terdistribusi
  - Aplikasi Klien/server
  - Mobile
  - Terintegrasi (teks, image, audio,video)
  - Sistem tertanam
  - Komunikasi nirkabel - Internet



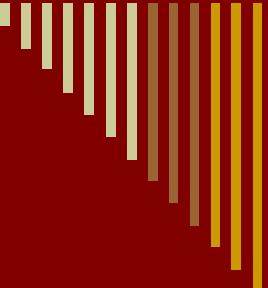
# Keamanan dan Jaminan Informasi Efektif

- **Lingkup komprehensif :**
  - ✓ Keselamatan
  - ✓ Keandalan
  - ✓ Rekayasa keamanan
- **Tantangannya interaksi dinamis dari :**
  - ✓ Perangkat lunak
  - ✓ Perangkat keras
  - ✓ Telekomunikasi
  - ✓ orang



## Komponen-komponen Program keamanan/jaminan Informasi :

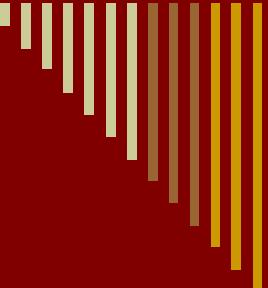
1. Menentukan apa yang harus dilindungi
2. Mengidentifikasi sistem
3. Karakteristik sistem operasi
4. Memastikan apa yang dilakukan seseorang dan tidak memiliki control lebih



# Definisi Melindungi (kamus Webster)

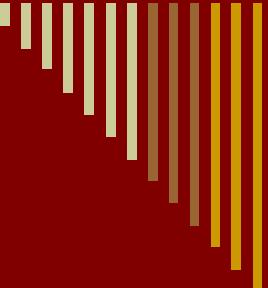
- untuk menutupi atau melindungi dari paparan, cedera, atau kehancuran, penjaga;
- untuk mempertahankan status atau integritas.

Tujuan dari informasi keamanan/IA adalah untuk melindungi sistem dan data penting.



# Menentukan apa yang harus dilindungi

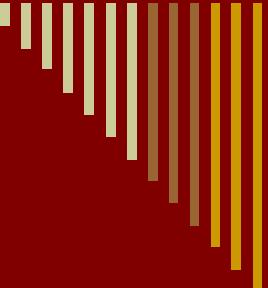
- Sistem yang memproses atau menghasilkan data?
- Sistem yang menampilkan data?
- Cadangan, pengarsipan, atau sistem penyimpanan online?
- Sistem kontrol yang bertindak berdasarkan data real-time?
- Sistem komunikasi?
- Suara, video, Gambar, atau data tekstual?
- Hardcopy output?
- Perangkat input?



# Contoh Tujuan Keamanan IA

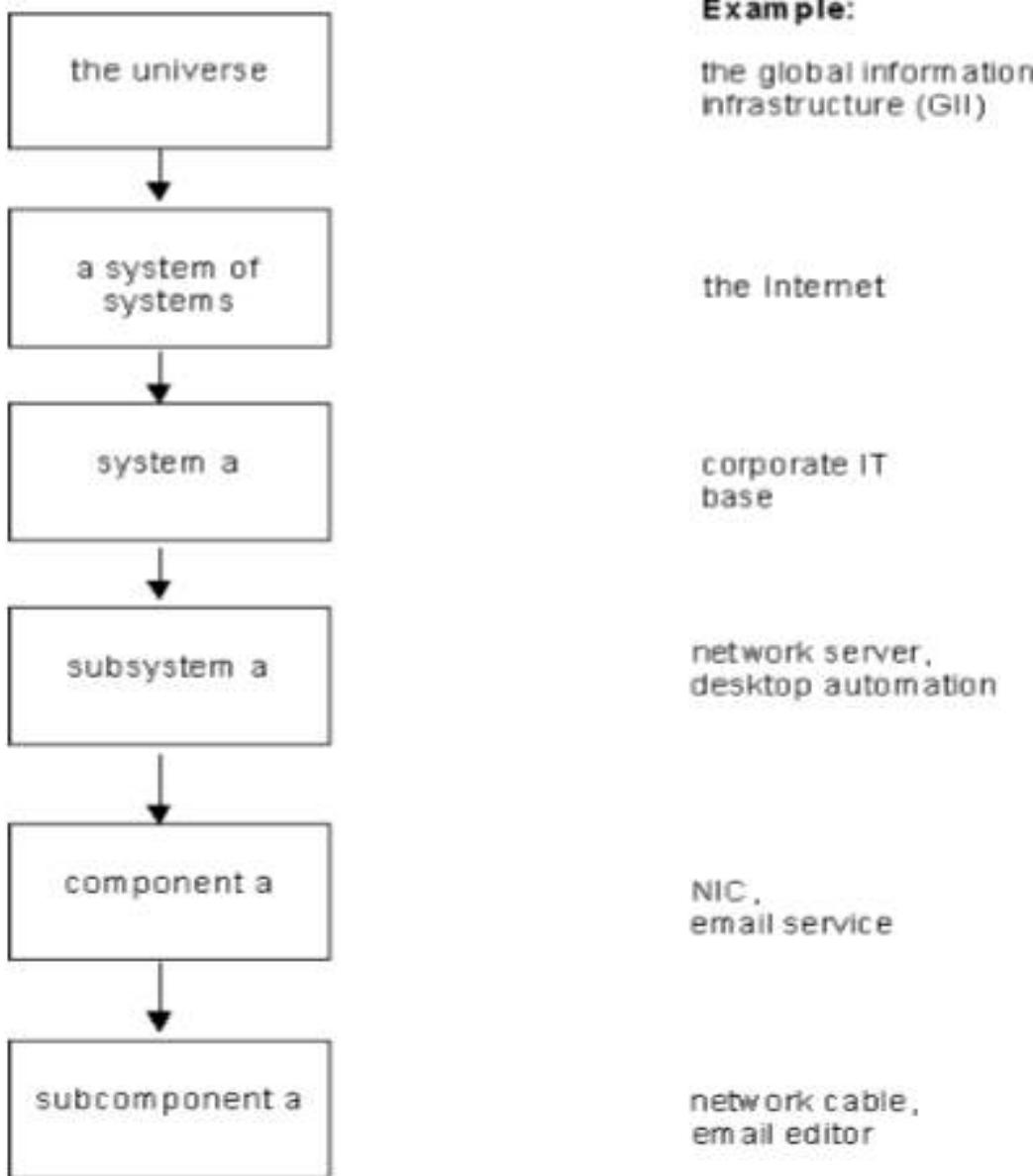
melindungi privasi dan integritas catatan pelanggan dari pengungkapan sengaja atau berbahaya disengaja, manipulasi, perubahan, penyalahgunaan, korupsi, dan pencurian.

- melindungi informasi identitas pribadi: nama, alamat, nomor telepon, alamat e-mail, nomor rekening, dan nomor faks.
- melindungi informasi pembayaran pelanggan dan sejarah.
- melindungi riwayat dan preferensi pembelian pelanggan.
- melindungi pelanggan secara online, suara, Faks, dan hardcopy transaksi.

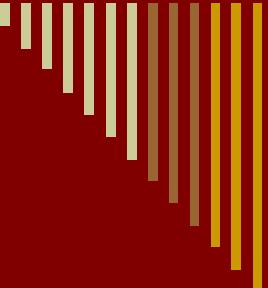


# Mengidentifikasi Sistem

- Definisi sistem: Sekumpulan komponen2 yang diorganisasi untuk mencapai fungsi tertentu



**Exhibit 2 Standard Hierarchy Used in System Definition**



# Contoh Statemen bertujuan Jaminan Informasi :

Melindungi privasi dan integritas catatan pelanggan dari pengungkapan sengaja atau berbahaya disengaja, manipulasi, perubahan, penyalahgunaan, korupsi, dan pencurian.

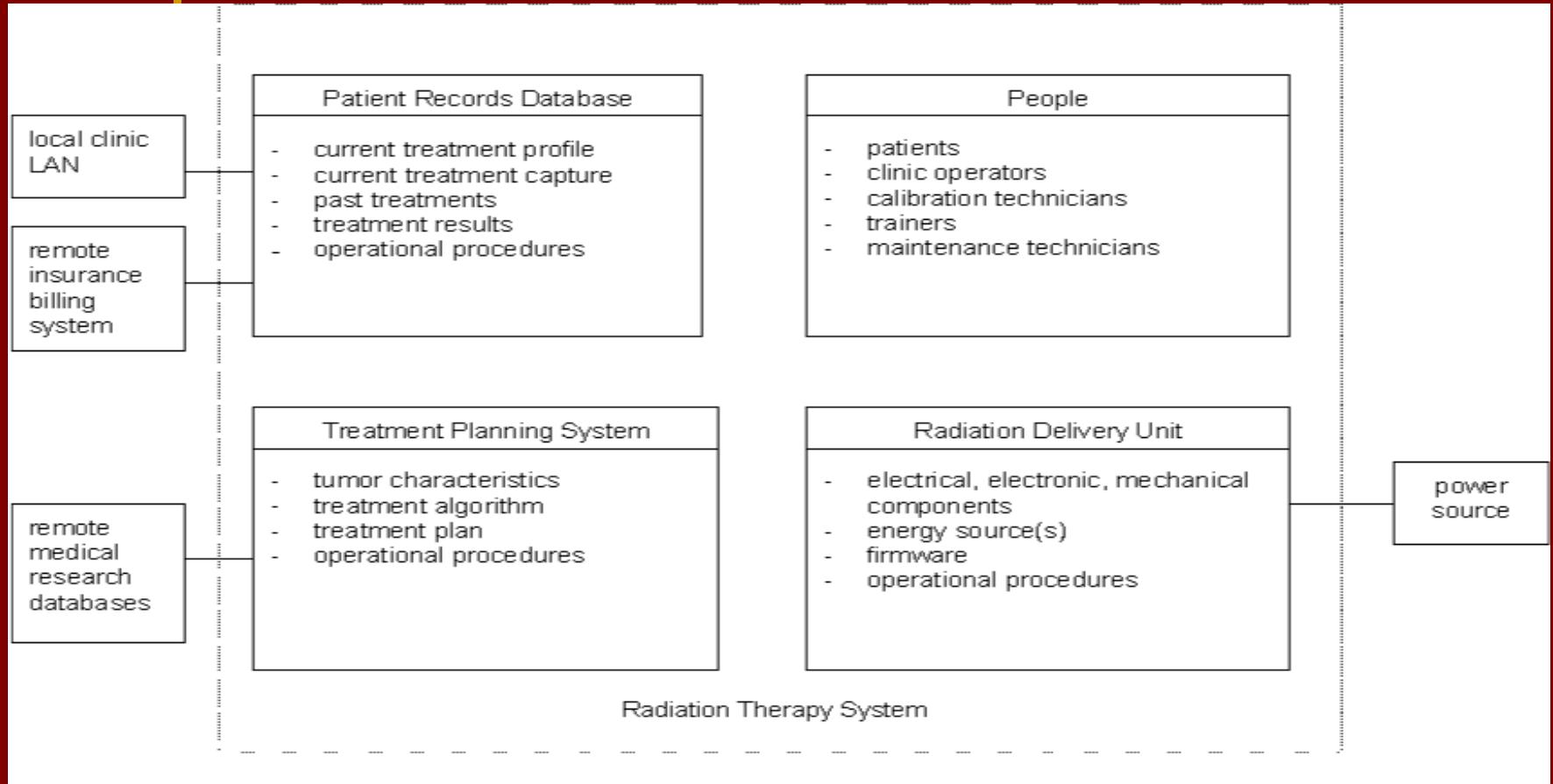
- melindungi informasi identitas pribadi: nama, alamat, nomor telepon, alamat e-mail, nomor rekening, dan nomor faks.
- melindungi informasi pembayaran pelanggan dan sejarah.
- melindungi riwayat dan preferensi pembelian pelanggan.
- melindungi pelanggan secara online, suara, Faks, dan hardcopy transaksi.

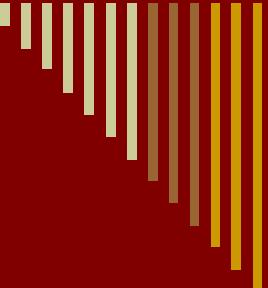


# Entitas Sistem

1. Logical : software
  2. Phisik : komputer, hard drive, floppy drive, dll
  3. Animate(Hidup): pengguna, administrator sistem, pelatih, dan staf pemeliharaan
1. Inanimate(Mati): Arsip system.
  2. Primary : mereka yang berkontribusi secara langsung untuk pencapaian fungsi sistem; misalnya CPU, sistem operasi, perangkat lunak aplikasi, dan pengguna akhir.
  1. Support : jaringan listrik dan backbone telekomunikasi
  2. Dinamis : konfigurasi sistem dan prosedur operasional
  3. Statis : jadwal pemeliharaan dan komponen elektromekanis.

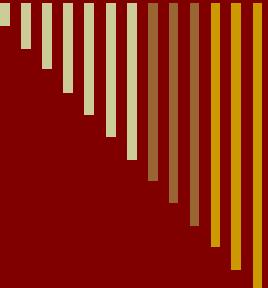
# Entitas Internal dan Eksternal dari sistem : suatu contoh





# Identifikasi batasan sistem

- Tentukan titik awal sbg entitas utama
- Utk bekerja ke atas utk mengidentifikasi batas luar sistem
- Utk bekerja ke bawah utk mengidentifikasi subsistem konstituen, komponen, dan subkomponen.



# Definisi sistem

- harus didokumentasikan.
- Digambarkan sistem secara grafis

Sistem :

- sistem terbatas
- sistem tak terbatas :
  - ✓ aplikasi internet atau
  - ✓ interaksi antar misi atau
  - ✓ sistem kritis atau
  - ✓ sistem infrastruktur

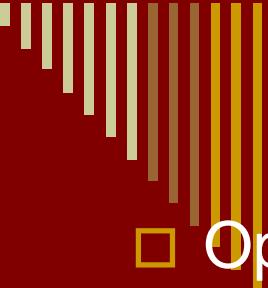
## **Exhibit 4 Sample High-Level System Definition**

**System: Radiation Therapy System as of: 20 March 2000**

<i>Subsystem</i>	<i>Component</i>	<i>Subcomponent</i>	<i>L/P</i>	<i>A/I</i>	<i>P/S</i>	<i>D/S</i>
1. People	1.1 Patients	—	P	A	P	D
	1.2 Clinical operators	—	P	A	P	D
	1.3 Calibration staff	—	P	A	S	D
	1.4 Maintenance staff	—	P	A	S	D
	1.5 Training staff	—	P	A	S	D
2. Patient records DBMS	2.1 Treatment profile	2.x.1 Data records	L	I	S	D
	2.2 Current treatment capture	2.x.2 Record management capability	L	I	S	D
	2.3 Past treatments	2.x.3 Report generation capability	L	I	S	S
	2.4 Treatment results	2.x.4 Query/response capability	L	I	S	D
	2.5 Operational procedures	2.x.5 Backup/archive capability	L	I	S	D
	**2.6 Local clinic LAN	—	P	I	S	D/S
	**2.7 Remote insurance/billing system	—	L	I	S	D/S

3. Treatment planning system	3.1 Tumor characteristics	—	L	I	P	D/S
	3.2 Radiation therapy algorithm	3.2.1 Optional components or variations of algorithm	L	I	P	S
	3.3 Operational procedures	—	L	I	S	D/S
	3.4 Treatment plan x	3.4.1 Dosage 3.4.2 Targeting information 3.4.3 Number of sessions	L	I	P	D/S
	**3.5 Remote medical research databases	—	L	I	S	D/S
	4.1 Electrical, electronic, and mechanical components	4.1.x Subassemblies	P	I	P	S
4. Radiation delivery system	**4.2 Energy source(s)	4.2.1 Energy delivery system	P	I	P	S
	4.3 Operational procedures	4.2.2 Power supply 4.3.1 Maintenance schedule and procedures 4.3.2 Calibration schedule and procedures 4.3.3 Patient use procedures	L	I	S	D/S
			L	I	S	D/S
			L	I	P	D/S
			L	I	P	D/S
			L	I	P	D/S

Note: L/P, logical or physical entity; A/I, animate or inanimate entity; P/S, primary or support entity; D/S, dynamic or static; and \*\*, external entity.



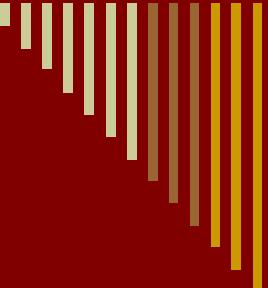
# Mode Operasional

## □ Operasi Normal

- start-up
- Shutdown
- Reconfiguration
- restart/reset
- backup
- standby
- Maintenance
- decommission
- perform normal system-specific functions

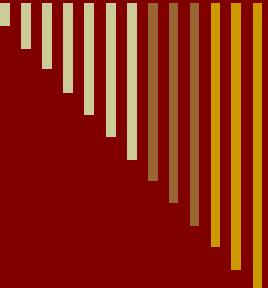
## □ Operasi Tidak Normal

- failure of system hardware
- failure of system or application software
- operator error
- degraded mode operations
- shutdown under abnormal conditions (e.g., an attack)



Mode Operasional dan keadaan dicirikan oleh kendala kinerja dan keandalan :

- **Waktu respon**
- **Beban prosesor**
- **Persyaratan bandwidth**
- **Pengurutan transisi state dll**



# Operasional Profil/skenario

- Mewakili serangkaian operasi yang sistem dapat eksekusi
- Menggambarkan bagaimana manusia berinteraksi dengan sistem utk menyelesaikan tugas, melalui analisis skenario operasional, tampilan pengguna, dan peristiwa system
- Pengguna akhir, untuk staf utama, pelatih, administrator sistem, pengguna super, penguji, dan penyusup potensial

## **Exhibit 5 Sample High-Level System Operation Characterization**

---

**System: Radiation Therapy System as of: 30 March 2000**

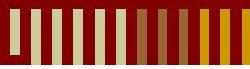
### **I. Operational Modes and States**

<i>Mode/State</i>	<i>Occurs Before</i>	<i>Occurs After</i>	<i>Occurs During</i>	<i>Constraints</i>	<i>Initiated by</i>
<b><i>Normal Operations</i></b>					
Start-up	All other modes	—	—	Power availability, absence of system fault	System administrator, maintenance staff
Shutdown	—	All other modes	—	System has been safed, records saved	System administrator, maintenance staff
Reconfiguration	Shutdown	Start-up	—	No end users active	System administrator, maintenance staff
Restart/reset	Shutdown	Start-up	—	No end users active	System administrator, maintenance staff
Backup	Shutdown	Start-up	—	No end users active	System administrator, maintenance staff
Standby	Shutdown	Start-up	—	No end users active	System administrator, maintenance staff
Maintenance	Shutdown	Start-up	—	No end users active	System administrator, maintenance staff



## Exhibit 5 Sample High-Level System Operation Characterization (continued)

<i>Mode/State</i>	<i>Occurs Before</i>	<i>Occurs After</i>	<i>Occurs During</i>	<i>Constraints</i>	<i>Initiated by</i>
Decommission	Shutdown	Start-up	—	System has been safed, no end users active	System administrator, maintenance staff
Perform normal system-specific functions	Shutdown	Start-up	Varies	System resources are available	All except intruders
<b><i>Abnormal Operations</i></b>					
Failure of patient records database	Shutdown	Start-up	—	Failure must not cause safety and/or security violation	Operator error, system HW/SW fault
Failure of treatment planning system	Shutdown	Start-up	—	Failure must not cause safety and/or security violation	Operator error, system HW/SW fault

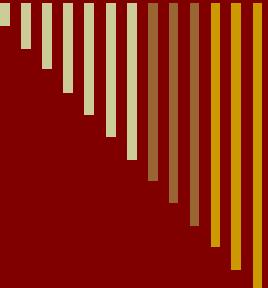


## Exhibit 5 Sample High-Level System Operation Characterization (continued)

<i>Mode/State</i>	<i>Occurs Before</i>	<i>Occurs After</i>	<i>Occurs During</i>	<i>Constraints</i>	<i>Initiated by</i>
Failure of radiation treatment unit	Shutdown	Start-up	—	Failure must not cause safety violation	Operator error, system HW/SW fault
Degraded mode operations	Shutdown	Start-up, system failure	—	Criteria for transferring to degraded mode operations must be defined and met	System software and/or system administrator

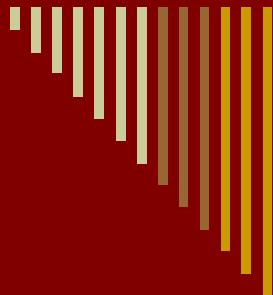
## II. Operational Profiles

<i>Operator</i>	<i>Primary Activities</i>	<i>Time Distribution</i>	<i>Sequencing, Timing, or Other Restrictions</i>
End user a	Logon Access, enter, store, forward patient records Logoff	5% 90% 5%	Patient records must be initialized before any other transactions can take place



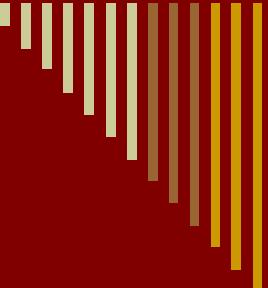
## **Kegiatan akhir dalam mendefinisikan batas-batas sistem**

- adalah untuk memastikan bahwa entitas sistem melakukan dan tidak melakukan atas kontrol yang dimiliki sistem.
- Informasi ini merupakan masukan penting bagi analisis kerentanan dan ancaman.
- Tingkat kontrol pemilik sistem ditentukan untuk semua entitas internal dan eksternal yang diidentifikasi.



# Status Kontrol

- mencatat tingkat kontrol atau tanggung jawab pemilik sistem memiliki fungsi yang akurat dari suatu entitas.
- dapat berupa Total, Parsial, atau tidak ada.



# Status Kontrol :

- **Kontrol Total** : pemilik sistem memiliki kontrol penuh atas dan tanggung jawab untuk entitas, kebenaran dan kinerja tindakannya.
- **Kontrol Parsial**: pemilik sistem berbagi kontrol atas dan bertanggung jawab atas suatu entitas, ketepatan dan kinerja tindakannya dengan satu atau lebih pihak kedua, biasanya melalui mekanisme hukum seperti kontrak.
- **Tidak ada** : pemilik sistem tidak memiliki kontrol atas atau tanggung jawab untuk entitas, tetapi tergantung pada layanan yang disediakan. Satu atau lebih pihak ketiga memiliki tanggung jawab dan kontrol ini. Sistem infrastruktur adalah contoh yang baik.

## Exhibit 6 Sample High-Level System Entity Control Analysis

<i>Subsystem</i>	<i>Component</i>	<i>Subcomponent</i>	<i>Control Status</i>	<i>Explanation</i>
1. People	1.1 Patients	—	None	Patients are not employees or otherwise under contract to the clinic.
	1.2 Clinical operators	—	Total	All legitimate operators are clinic employees.
	1.3 Calibration staff	—	Partial	Calibration staff are under contract to the clinic.
	1.4 Maintenance staff	—	Partial	Maintenance staff are under contract to the clinic.
	1.5 Training staff	—	Partial	Trainers are under contract to the clinic.

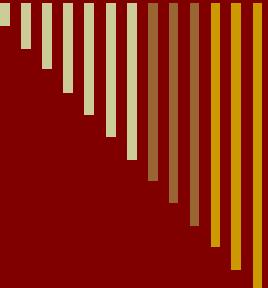
<i>Subsystem</i>	<i>Component</i>	<i>Subcomponent</i>	<i>Control Status</i>	<i>Explanation</i>
				Clinic.
2. Patient records DBMS	2.1 Treatment profile 2.2 Current treatment capture	2.x.1 Data records 2.x.2 Record management capability	Total None	Clinic owns patient records. DBMS application software is provided and maintained by vendor.
	2.3 Past treatments	2.x.3 Report generation capability		
	2.4 Treatment results	2.x.4 Query/response capability		
	2.5 Operational procedures	2.x.5 Backup/archive capability	Partial	Clinic owns backup/archive records. Vendor owns software that generates backups.
**2.6 Local clinic LAN	—		Partial	Clinic contracts for LAN services.
**2.7 Remote insurance/billing system	—		None	Third party maintains insurance/billing databases.

## Exhibit 6 Sample High-Level System Entity Control Analysis (continued)

<i>Subsystem</i>	<i>Component</i>	<i>Subcomponent</i>	<i>Control Status</i>	<i>Explanation</i>
3. Treatment planning system	3.1 Tumor characteristics	—	Total	Clinic owns patient records.
	3.2 Radiation therapy algorithm	3.2.1 Optional components or variations of algorithm	Partial	Clinic implements specific instance of algorithm. Vendor owns application software.
	3.3 Operational procedures	—	Partial	Clinic is responsible for enforcing operational procedures. Vendor is responsible for developing operational procedures.
	3.4 Treatment plan x	3.4.1 Dosage 3.4.2 Targeting information 3.4.3 Number of sessions	Total	Clinic employee develops specific treatment plan.
	**3.5 Remote medical research databases	—	None	Clinic neither creates or maintains research databases; a third party does.

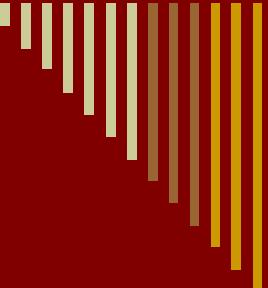
<i>Subsystem</i>	<i>Component</i>	<i>Subcomponent</i>	<i>Control Status</i>	<i>Explanation</i>
4. Radiation delivery system	4.1 Electrical, electronic, and mechanical components	4.1.x Subassemblies	None	Vendor has total responsibility.
	**4.2 Energy sources	4.2.1 Energy delivery system	None	Power company and vendor have responsibility.
	4.3 Operational procedures	4.2.2 Power supply 4.3.1 Maintenance schedule and procedures 4.3.2 Calibration schedule and procedures 4.3.3 Patient use procedures	Partial	Clinic is responsible for enforcing procedures. Vendor is responsible for developing accurate procedures.

Note: \*\*, external entity.



# Kesimpulan

- Komponen pertama dari program Security/IA informasi yang efektif adalah untuk menentukan batasan dari sebuah sistem.
- Ada empat kegiatan yang terlibat dalam mendefinisikan batasan-batasan suatu sistem, seperti :
  - Menentukan apa yang dilindungi dan mengapa
  - Mengidentifikasi sistem
  - Karakterisasi operasi sistem
  - Memastikan apa yang dilakukan seseorang dan tidak memiliki kendali atas sistem



# Tanya Jawab !





# ANALISIS KERENTANAN DAN ANCAMAN

# KEMAMPUAN AKHIR TAHAPAN PEMBELAJARAN

- Mahasiswa mampu mendeskripsikan pertimbangan keamanan yang dievaluasi pada tiap tahap siklus hidup produk.

## DILAKUKAN KEGIATAN BERIKUT :

- Memilih dan menggunakan teknik analisis IA
- Mengidentifikasi kerentanan, jenis, sumber, dan tingkat keparahan
- Mengidentifikasi ancaman, jenis, sumber, dan kemungkinan
- Mengevaluasi jalur transaksi, zona ancaman kritis, dan eksposur risiko

# DEFINISI KERENTANAN

- Kerentanan adalah kelemahan dalam sistem yang dapat dimanfaatkan untuk melakukan pelanggaran perilaku terhadap keselamatan, keamanan, keandalan, ketersediaan, integritas, dan sebagainya.
- kerentanan adalah kelemahan yang dapat dimanfaatkan untuk melanggar keselamatan, keandalan, dan/atau keamanan sistem
- Kerentanan melekat pada desain, operasi, atau lingkungan operasional sistem. Mereka bertambah akibat kesalahan kelalaian, kesalahan komisi, dan kesalahan operasional yang terjadi selama masa hidup suatu sistem.

## DEFINISI ANCAMAN :

- potensi bahaya bahwa kerentanan dapat dimanfaatkan secara niat, dipicu secara tidak sengaja atau sengaja dilakukan.
- ancaman merupakan potensi untuk mengeksplorasi kerentanan itu.

## DEFINISI BAHAYA:

- potensi bahaya atau situasi yang berpotensi membahayakan.
- Bahaya merupakan potensi cedera atau kematian bagi manusia, atau kerusakan atau perusakan terhadap properti atau lingkungan

# DEFINISI RESIKO

1. kombinasi kemungkinan bahaya yang terjadi dan tingkat keparahan konsekuensi seharusnya terjadi;
  2. ekspresi kemungkinan dan dampak peristiwa yang tidak direncanakan atau serangkaian peristiwa yang mengakibatkan kematian, cedera, penyakit okupasi, kerusakan atau hilangnya peralatan atau properti, atau kerusakan lingkungan dalam hal potensi keparahan dan probabilitas terjadinya.
- bahaya adalah peristiwa yang tidak diinginkan dengan konsekuensi negatif, sementara risiko merupakan kemungkinan bahwa bahaya akan terjadi dan tingkat keparahan konsekuensi daripadanya.

# KEPARAHAN

- Keparahan mencirikan konsekuensi dari potensi bahaya, tingkat bahaya atau cedera yang dapat ditimbulkan. Mengikuti praktik manajemen risiko standar, yaitu mengevaluasi skenario terburuk.

# TINGKAT KEPARAHAN

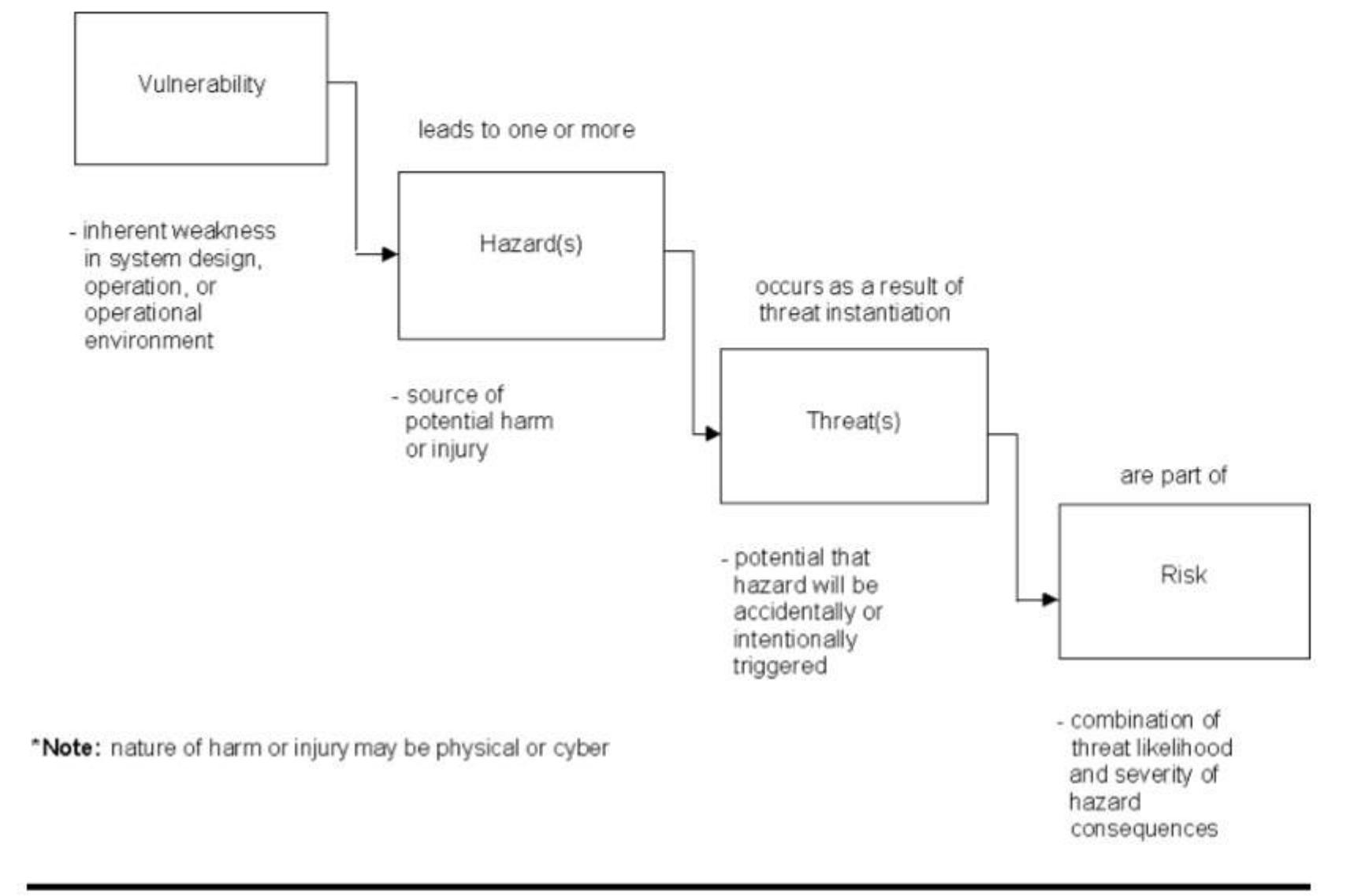
- **Bencana:** kematian atau beberapa luka parah; kehilangan satu atau lebih sistem utama
- **Kritis:** kematian atau cedera parah tunggal; hilangnya sistem utama
- **Marginal:** luka ringan; kerusakan system parah
- **Tidak signifikan:** kemungkinan cedera ringan tunggal; kerusakan system

# CIDERA

- cedera mengacu pada potensi bahaya yang mungkin atau tidak mungkin secara fisik di alam
- tingkat keparahan dapat diterapkan untuk berbagai keselamatan, keandalan, dan masalah keamanan.

# KEMUNGKINAN

- Kemungkinan mencirikan probabilitas ancaman instansi, yaitu, bahaya yang dilakukan.
- Skenario yang paling mungkin dievaluasi.



Gambar : Interaksi antara kerentanan, bahaya, ancaman, dan risiko

## LEVEL KEMUNGKINAN :

1. Frequent: cenderung sering terjadi; bahaya akan dialami terus-menerus ( $10^{-2}$ )
2. kemungkinan: akan terjadi beberapa kali; bahaya dapat diharapkan terjadi sering ( $10^{-3}$ )
3. sesekali: mungkin terjadi beberapa kali selama masa hidup sistem ( $10^{-4}$ )
4. remote: mungkin terjadi pada suatu waktu selama masa hidup sistem ( $10^{-5}$ )
5. mustahil: tidak mungkin tetapi mungkin terjadi selama kehidupan sistem ( $10^{-6}$ )
6. Incredible: sangat tidak mungkin terjadi selama kehidupan sistem ( $10^{-7}$ )

## JENIS PENILAIAN KEMUNGKINAN

- **Penilaian kuantitatif** : kegagalan hardware sangat mudah.
- **penilaian kualitatif** : kegagalan perangkat lunak yang sistematis, kesalahan operasional, dan tindakan yang disengaja dan membahayakan diri sendiri

# PEMILIHAN/PENGGUNAAN TEKNIK ANALISA IA

- Berbagai teknik analisis yang digunakan untuk menemukan kerentanan dalam spesifikasi, Desain, pelaksanaan, operasi, dan lingkungan operasional sistem, potensi bahaya yang terkait dengan kerentanan ini, dan ancaman bahwa bahaya ini akan dipicu secara tidak sengaja atau dengan niat jahat.
- Beberapa kerentanan dapat diidentifikasi melalui sesi brainstorming informal.
- Namun, eksplorasi komprehensif kerentanan, bahaya, dan ancaman memerlukan penggunaan teknik yang lebih formal.

## Exhibit 2 Information Assurance Analysis Techniques

I. IA Analysis Techniques	C/R	Type	Life-Cycle Phase in which Technique is Used		
			Concept	Development	Operations
Bayesian Belief networks (BBNs) <sup>b</sup>	C1	All	x	x	x
Cause consequence analysis <sup>a,b</sup>	R1/C1	SA, SE	x	x	x
Change impact analysis	C1	All		x	x
Common cause failure analysis <sup>a</sup>	C1	All	x	x	x
Develop operational profiles, formal scenario analysis	C1	All	x	x	x
Develop IA integrity case	C1	All	x	x	x
Event tree analysis <sup>a,b</sup>	R1/C1	All	x	x	x
Functional analysis	C1	SA, SE	x	x	x
Hazard analysis	C1	SA, SE	x	x	x
HAZOP studies <sup>a,b</sup>	C1	SA, SE	x	x	x
Highlighting requirements likely to change	C1	All	x		
Petri nets <sup>a,b</sup>	C1	SA, SE		x	x
Reliability block diagrams	C1	RE	x	x	x
Reliability prediction modeling	C1	RE	x	x	
Response time, memory, constraint analysis	C1	All		x	x
Software, system FMECA <sup>a,b</sup>	C1	All	x	x	x
Software, system FTA <sup>a,b</sup>	R1/C1	SA, SE	x	x	x
Sneak circuit analysis <sup>a,b</sup>	C1	SA, SE		x	x
Usability analysis	C1	SA, SE	x	x	x

# TEKNIK ANALISIS JAMINAN INFORMASI

Teknik Analisis	C/R	Type	Phase siklus hidup dimana teknik digunakan		
			Konsep	Pengembangan	Operasi
Jaringan kepercayaan Bayesian (BBN)	C1	All	X	X	X
Analisis Penyebab konsekuensi	R1/C1	SA,SEE	X	X	X
Analisis Dampak Perubahan	C1	All		X	X
Analisis Penyebab Kegagalan Umum	C1	All	X	X	X
Analisis Skenario Formal, Pengembangan Operasional Profil	C1	All	X	X	X
Mengembangkan kasus integritas IA	C1	All	X	X	X
Analisis Pohon Peristiwa	R1/C1	All	X	X	X
Analisis Fungsional	C1	SA/SE	X	X	X
Analisis Bahaya	C1	SA/SE	X	X	X
Studi HAZOP	C1	SA/SE	X	X	X
Menyoroti persyaratan kemungkinan akan berubah	C1	All	X	X	X
Petri netsa	C1	SA/SE	X	X	X
Keandalan blok diagram	C1	RE	X	X	X
Keandalan prediksi model	C1	RE	X	X	X
Waktu respon, memori, analisa kendala	C1	All	X	X	X
Software, sistem FMECA	C1	All	X	X	X
Software, sistem FTA	R1/C1	SA,SE	X	X	X

# MAKNA KOLOM KODE

kolom	Code	arti
Type	SA	Teknik terutama mendukung rekayasa keselamatan
	SE	Teknik terutama mendukung rekayasa keamanan
	RE	Teknik terutama mendukung rekayasa keandalan
	ALL	Teknik mendukung kombinasi keselamatan, keamanan, dan keandalan
C/R	Cx	kelompok teknik pelengkap
	Rx	kelompok teknik redundan; hanya salah satu yang berlebihan teknik harus digunakan

# MASUKAN DARI DEFINISI BATAS SISTEM

1. Tujuan IA
2. Definisi entitas system
3. Karakterisasi operasi sistem
4. Analisis kontrol entitas sistem

# PERAN ANALISIS IA DARI MASING-MASING TEKNIK

## Exhibit 3 Analysis Role of IA Techniques

<i>Analysis Technique</i>	<i>IA Analysis Role</i>
Bayesian belief networks (BBNs)	Provide a methodology for reasoning about uncertainty as part of risk analysis and assessment.
Cause consequence analysis	Enhance IA integrity by identifying possible sequences of events that can lead to a system compromise or failure.
Change impact analysis	Analyze <i>a priori</i> the potential local and global effects of changing requirements, design, implementation, data structures, or interfaces on system performance, safety, reliability, and security; prevent errors from being introduced during enhancements or maintenance.
Common cause failure (CCF) analysis	Enhance IA integrity by identifying scenarios in which two or more failures or compromises occur as the result of a common design defect.
Develop operational profiles, formal scenario analysis	Identify operational profiles, capture domain knowledge about MWFs and MNWFs; understand human factors safety, reliability, and security concerns.
Develop IA integrity case	Collect, organize, analyze, and report information to prove that IA integrity requirements have been (or will be) achieved and maintained.
Event tree analysis	Enhance IA integrity by preventing defects through analysis of sequences of system events and operator actions that could lead to failures, compromises, or unstable states.

### Exhibit 3 Analysis Role of IA Techniques (Lanjutan....)

<i>Analysis Technique</i>	<i>IA Analysis Role</i>
Functional analysis	Identify safety and security hazards associated with normal operations, degraded mode operations, incorrect usage, inadvertent operation, absence of function(s), and accidental and intentional human error.
Hazard analysis	Enhance IA integrity by identifying potential hazards associated with using a system so that appropriate mitigation features can be incorporated into the design and operational procedures.
HAZOP studies	Prevent potential hazards (accidental and intentional, physical and cyber) by capturing domain knowledge about operational environment, parameters, modes/ states, etc. so that this information can be incorporated in the requirements, design, and operational procedures.
Highlighting requirements likely to change	Enhance the maintainability of threat control measures and IA integrity.
Petri nets	Identify potential deadlock, race, and nondeterministic conditions that could lead to a system compromise or failure.
Reliability block diagrams	Enhance IA integrity by identifying diagrammatically the set of events that must take place and the conditions that must be fulfilled for a system or task to execute correctly <sup>69,131</sup> ; support initial reliability allocation, reliability estimates, and design optimization.

## Analisis Peran Teknik Analisis IA

Teknik Analisis	Peran Analisis IA
Jaringan kepercayaan Bayesian (BBN)	menyediakan metodologi untuk penalaran tentang ketidakpastian sebagai bagian dari analisis risiko dan penilaian.
Analisis Penyebab konsekuensi	meningkatkan integritas IA dengan mengidentifikasi urutan yang mungkin peristiwa yang dapat menyebabkan sistem disusupi atau kegagalan.
Analisis Dampak Perubahan	menganalisis apriori potensi efek lokal dan global perubahan persyaratan, Desain, implementasi, struktur data, atau antarmuka pada kinerja sistem, keselamatan, keandalan, dan keamanan; mencegah kesalahan dari diperkenalkan selama perangkat tambahan atau pemeliharaan.
Analisis Penyebab Kegagalan Umum	meningkatkan integritas IA dengan mengidentifikasi skenario di mana dua atau lebih kegagalan atau kompromi terjadi akibat Cacat desain umum.
Analisis Skenario Formal, Pengembangan Operasional Profil	identifikasi profil operasional, tangkap domain skenario formal analisis pengetahuan tentang MWFs dan MNWFs; Memahami faktor manusia keamanan, keandalan, dan masalah keamanan.
Mengembangkan kasus integritas IA	mengumpulkan, mengatur, menganalisa, dan melaporkan informasi membuktikan bahwa persyaratan integritas IA akan) tercapai dan dipertahankan.

## Analisis Peran Teknik Analisis IA (lanjutan )

<b>Analisis Pohon Peristiwa</b>	meningkatkan integritas IA dengan mencegah cacat melalui Analisis urutan peristiwa sistem dan operator tindakan yang dapat menyebabkan kegagalan, kompromi, atau negara yang tidak stabil.
<b>Analisis Fungsional</b>	mengidentifikasi bahaya keselamatan dan keamanan yang terkait dengan operasi normal, operasi mode terdegradasi, penggunaan yang salah, pengoperasian yang tidak disengaja, fungsi (s), dan disengaja dan disengaja kesalahan manusia.
<b>Analisis Bahaya</b>	meningkatkan integritas IA dengan mengidentifikasi potensi bahaya  terkait dengan penggunaan sistem sehingga sesuai Fitur mitigasi dapat dimasukkan ke dalam Desain dan prosedur operasional.
<b>Studi HAZOP</b>	mencegah potensi bahaya (kebetulan dan disengaja, fisik dan Cyber) dengan menangkap pengetahuan domain tentang lingkungan operasional, parameter, mode/ negara, dll sehingga informasi ini dapat yang tercakup dalam persyaratan, Desain, dan prosedur operasional.
<b>Menyoroti persyaratan kemungkinan akan berubah</b>	meningkatkan kemampuan pemeliharaan tindakan pengendalian ancaman akan berubah
<b>Petri netsa</b>	mengidentifikasi potensi kemacetan, ras, dan kondisi yang tidak

## Analisis Peran Teknik Analisis IA (lanjutan )

<b>Software, sistem FMECA</b>	memeriksa efek disengaja dan disengaja, kegagalan acak dan sistematis pada perilaku sistem dalam integritas Umum dan IA khususnya.
<b>Software, sistem FTA</b>	mengidentifikasi penyebab potensi akar sistem yang tidak diinginkan peristiwa (kebetulan dan disengaja) sehingga mengurangi Fitur dapat dimasukkan ke dalam desain dan prosedur operasional.
<b>Analisis Sirkuit Menyelinap</b>	mengidentifikasi tersembunyi yang tidak disengaja atau perangkat keras yang tak terduga atau jalur logika perangkat lunak atau urutan kontrol yang menghambat fungsi sistem yang dikehendaki, memulai peristiwa sistem, atau menyebabkan kesalahan waktu dan sequencing, yang mengarah ke sistem kompromi atau kegagalan
<b>Analisis kegunaan</b>	meningkatkan integritas operasional dengan memastikan lunak mudah digunakan sehingga upaya oleh pengguna manusia untuk mendapatkan layanan yang diperlukan adalah minimal; Mencegah kesalahan yang disebabkan atau diundang yang dapat mengakibatkan kegagalan/kompromi.

### Exhibit 3 Analysis Role of IA Techniques (continued)

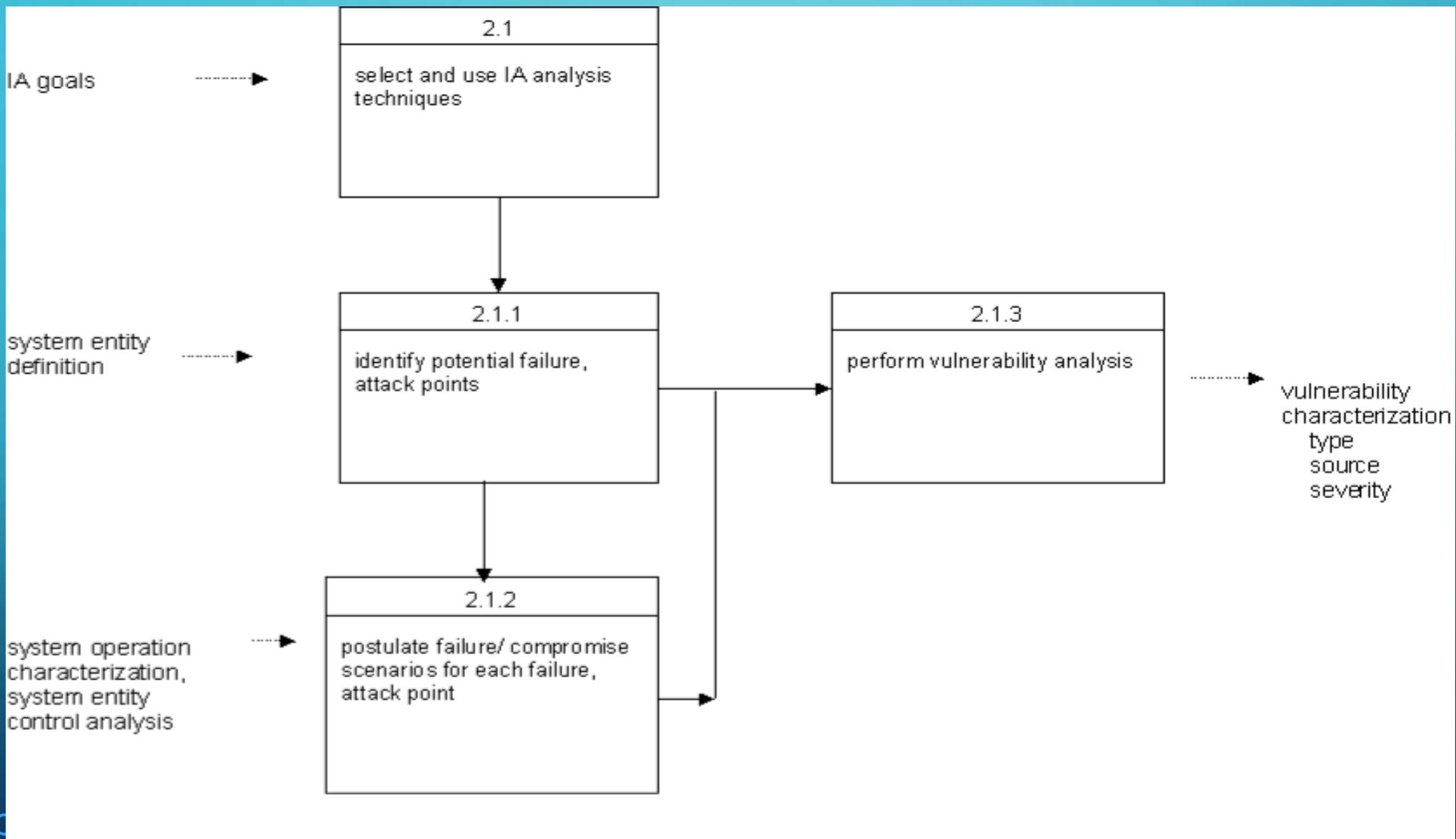
<i>Analysis Technique</i>	<i>IA Analysis Role</i>
Reliability prediction modeling	Predict future reliability of a software system.
Response time, memory, constraint analysis	Ensure that the operational system will meet all stated response time, memory, and other specified constraints under low, normal, and peak loading conditions. <sup>333</sup>
Software, system FMECA	Examine the effect of accidental and intentional, random and systematic failures on system behavior in general and IA integrity in particular.
Software, system FTA	Identify potential root causes of undesired system events (accidental and intentional) so that mitigating features can be incorporated into the design and operational procedures.
Sneak circuit analysis	Identify hidden unintended or unexpected hardware or software logic paths or control sequences that could inhibit desired system functions, initiate undesired system events, or cause incorrect timing and sequencing, leading to a system compromise or failure.
Usability analysis	Enhance operational IA integrity by ensuring that software is easy to use so that effort by human users to obtain the required service is minimal <sup>18</sup> ; prevent induced or invited errors that could lead to a system failure/compromise.

# TITIK KEGAGALAN

- definisi entitas sistem digunakan untuk mengidentifikasi titik kegagalan potensial tingkat tinggi.
- Pikirkan pada kedua entitas : entitas internal dan eksternal dianggap.
- Titik kegagalan merupakan titik serangan potensial.

# TITIK KEGAGALAN POTENTIAL, MELIPUTI

- Kegagalan server web
- Kegagalan LAN, workstation, atau printer lokal
- Kegagalan link ke sistem keuangan lainnya
- Kegagalan link ke lembaga keuangan lainnya
- Telekomunikasi backbone atau kegagalan ISP
- Sumber daya atau kontrol lingkungan yang salah
- Tindakan pengguna (pelanggan, karyawan Bank, staf pemeliharaan atau vendor, penyusup potensial)



# MENGIDENTIFIKASI KERENTANAN, JENIS, SUMBER, DAN TINGKAT KEPARAHAAN

**Kerentanan IA diklasifikasikan tiga cara**

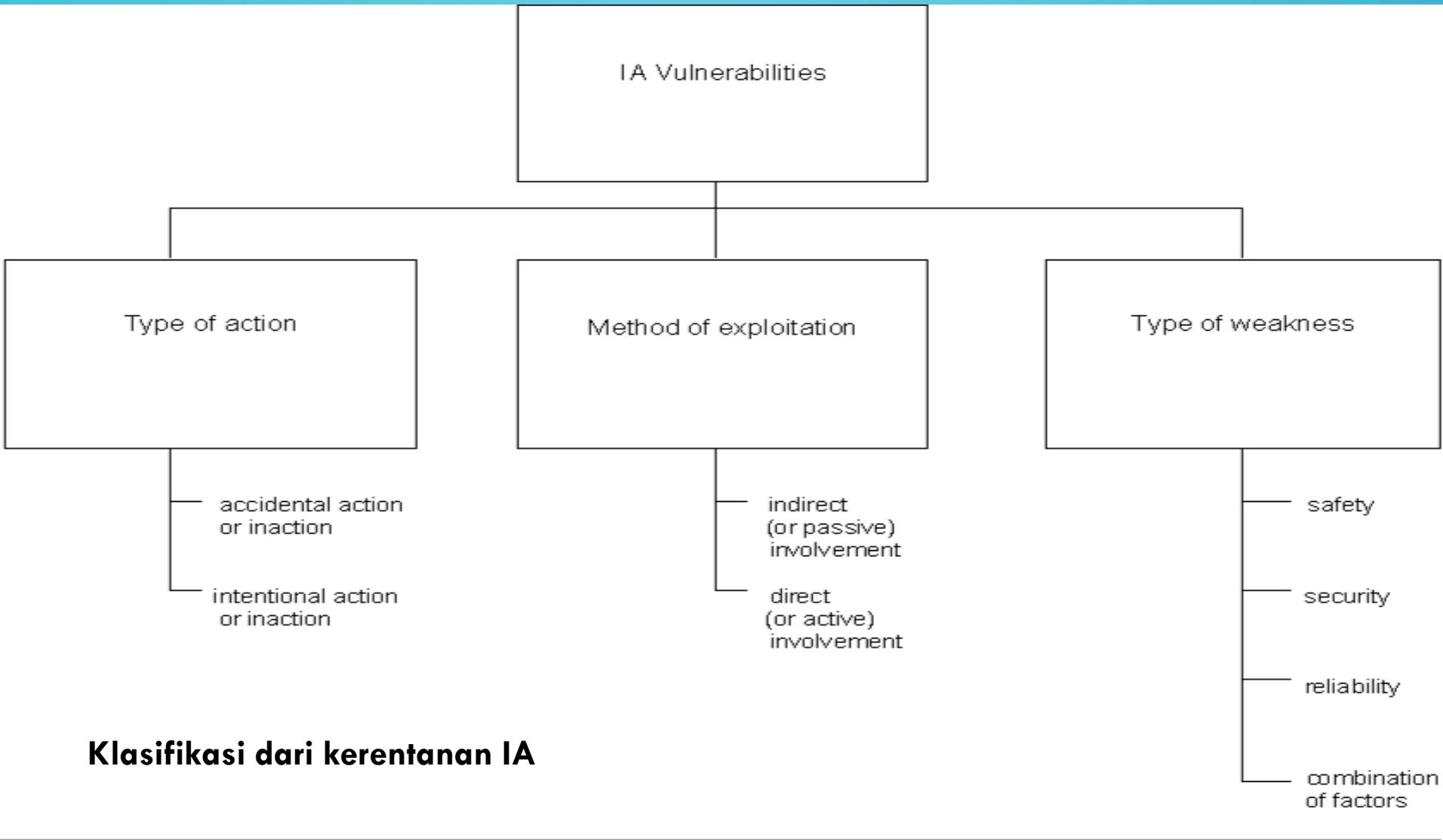
- **Jenis tindakan (type action)** yang menyebabkan kerentanan untuk memanifestasikan dirinya: tindakan disengaja (atau tidak bertindak) atau tindakan jahat disengaja atau tidak bertindak.
- **Metode Eksplorasi kerentanan** : keterlibatan pelaku baik langsung atau tidak langsung pada bagian tertentu.
- **Sifat dari kerentanan atau kelemahan (type kerentanan)**: keselamatan, keandalan, keamanan, atau beberapa kombinasi daripadanya

**Exhibit 5 Correlation of Failure Points, Failure Scenarios, and Vulnerabilities****System: online banking**

<i>Failure Point</i>	<i>Failure Scenario</i>	<i>Vulnerability</i>
Web server	Application software not protected	Little or no error detection/correction or fault tolerance
Web server	Operating system saturated	If number of simultaneous users exceeds x, system becomes unstable and exhibits unpredictable behavior
Web server	DBMS data files corrupted	Data files can be accessed directly without going through DBMS applications software
Web server	Sporadic system shut down or unpredictable behavior	Server hardware subjected to extreme environmental conditions
User action	User authorizations not checked in order to speed up system response times; security compromised	End users and system administrator lack sufficient training, limited understanding of system security features and procedures
User action	Backups and archives generated sporadically or not at all; backups and archives not verified and are unreliable	Unsecure backups, archives
User action	Hardcopy printouts thrown in open trash bins; security compromised	Careless disposal of hardcopy printouts

## System: online banking

<i>Failure Point</i>	<i>Failure Scenario</i>	<i>Vulnerability</i>
User action	Portable equipment and storage media taken out of facility, occasionally lost or stolen; files from unknown/untrusted sources loaded onto system	No control over portable equipment or storage media
Web server	Conflicts between COTS applications cause unpredictable behavior; unauthorized user can access COTS applications	COTS components installed with default values, guest accounts, possible trap doors



## Exhibit 7 Identification of Vulnerability Types

System: online banking

Vulnerability	Type of Action	Vulnerability Type	
		Method of Exploitation	Type of Weakness
Little or no error detection/correction or fault tolerance	Accidental inaction	Indirect	Security, reliability
If number of simultaneous users exceeds x, system becomes unstable and exhibits unpredictable behavior	Accidental inaction	Indirect	Security, reliability
Data files can be accessed directly without going through DBMS applications front-end	Accidental inaction	Direct	Security
Suboptimal operational environment, sporadic system shutdown or unpredictable behavior	Accidental inaction and intentional action	Indirect	Security, reliability
End users and system administrator lack sufficient training, understanding of system security features and procedures	Accidental inaction	Indirect	Security
Unsecure backups, archives	Accidental inaction	Indirect	Security, reliability
Careless disposal of hardcopy printouts	Accidental inaction	Indirect	Security
No control over portable equipment or storage media	Accidental inaction	Direct	Security, reliability
COTS components installed with default values, guest accounts, possible trap doors	Accidental inaction and intentional action	Direct	Security, reliability

## Exhibit 8 Identification of Vulnerability Sources

### System: online banking

Vulnerability	Source of Vulnerability
Little or no error detection/correction or fault tolerance	Failure to specify and implement requirements so that system remains in known safe and secure state at all times IA goals not defined
If number of simultaneous users exceeds $x$ , system becomes unstable and exhibits unpredictable behavior	Failure to perform response time, memory, constraint analysis
Data files can be accessed directly without going through DBMS applications front-end	Limited/weak access control and authentication mechanisms
Suboptimal operational environment, sporadic system shutdown or unpredictable behavior	Failure to perform HAZOP studies Vendor recommendations for operational environment ignored or incorrect
End users and system administrator lack sufficient training, limited understanding of system security features and procedures	Failure to develop operational profiles and scenarios Inadequate operational procedures Poor planning and training prior to system deployment
Unsecure backups, archives	Inadequate operational procedures Physical security issues not considered
Careless disposal of hardcopy printouts	Inadequate operational procedures Physical security issues not considered
No control over portable equipment or storage media	Inadequate operational procedures Physical and operational security issues not considered
COTS components installed with default values, guest accounts, possible trap doors	Inadequate analysis of COTS vulnerabilities prior to installation Failure to confine COTS products

## Exhibit 9 Identification of Vulnerability Severity

System: online banking

Vulnerability	Hazard Consequences	Severity
Little or no error detection/correction or fault tolerance	Transactions posted to wrong accounts; interest payable, interest due calculated incorrectly; automatic deposits and payments lost; etc.	Critical - catastrophic
If number of simultaneous users exceeds x, system becomes unstable and exhibits unpredictable behavior	Screens are displayed very slowly; wrong screens are displayed; screens are displayed in wrong sequence; customer A sees customer B's transaction; etc.	Marginal - critical
Data files can be accessed directly without going through DBMS applications front-end	Critical/sensitive data can be maliciously altered, deleted, copied, and/or stolen with ease.	Critical - catastrophic
Suboptimal operational environment, sporadic system shutdown or unpredictable behavior	Customers cannot access the system; system crashes in the middle of a transaction; partial posting of transactions.	Marginal
End users and system administrator lack sufficient training, limited understanding of system security features and procedures	System security features are routinely disabled and/or bypassed.	Critical - catastrophic
Unsecure backups, archives	Critical/sensitive data can be maliciously altered, deleted, copied, and/or stolen with ease.	Critical - catastrophic

## Exhibit 9 Identification of Vulnerability Severity (Lanjutan)

System: online banking

Vulnerability	Hazard Consequences	Severity
Careless disposal of hardcopy printouts	Critical/sensitive data can be stolen, copied, and/or distributed.	Critical - catastrophic
No control over portable equipment or storage media	Critical/sensitive data and applications can be stolen, copied, altered, or given to a third party.	Critical
COTS components installed with default values, guest accounts, possible trap doors	COTS components perform incorrectly, however, error is not overtly obvious; system security authorizations can be bypassed for malicious purposes.	Critical

# ANALISIS KERENTANAN

- Analisis kerentanan mengevaluasi entitas internal dan eksternal.
- Seperti kebanyakan sistem, aplikasi berbasis Internet bergantung pada entitas eksternal untuk mencapai misi mereka.
- Setiap entitas eksternal adalah sumber potensial dari kemampuan vulner tambahan

# MENGIDENTIFIKASI BEBERAPA POTENSI KERENTANAN YANG TERKAIT DENGAN ROUTER,

## Exhibit 10 Potential COTS Vulnerabilities

1. Component design:
  - Inadvertently flawed component design
  - Intentionally flawed component design
  - Excessive component functionality
  - Open or widely spread component design
  - Insufficient or incorrect documentation
2. Component procurement:
  - Insufficient component validation
  - Delivery through insecure channel
3. Component integration:
  - Mismatch between product security levels
  - Insufficient understanding of integration requirements
4. System Internet connection:
  - Increased external exposure
  - Intrusion information and tools easily available
  - Executable content
  - Outward channel for stolen information
5. System use:
  - Unintended use
  - Insufficient understanding of functionality
6. System maintenance:
  - Insecure updating
  - Unexpected side effects
  - Maintenance of trap doors

Source: Summarized from U. Lindquist and E. Jonsson, *Computer*, 31(6), 60–66, 1998. With permission.

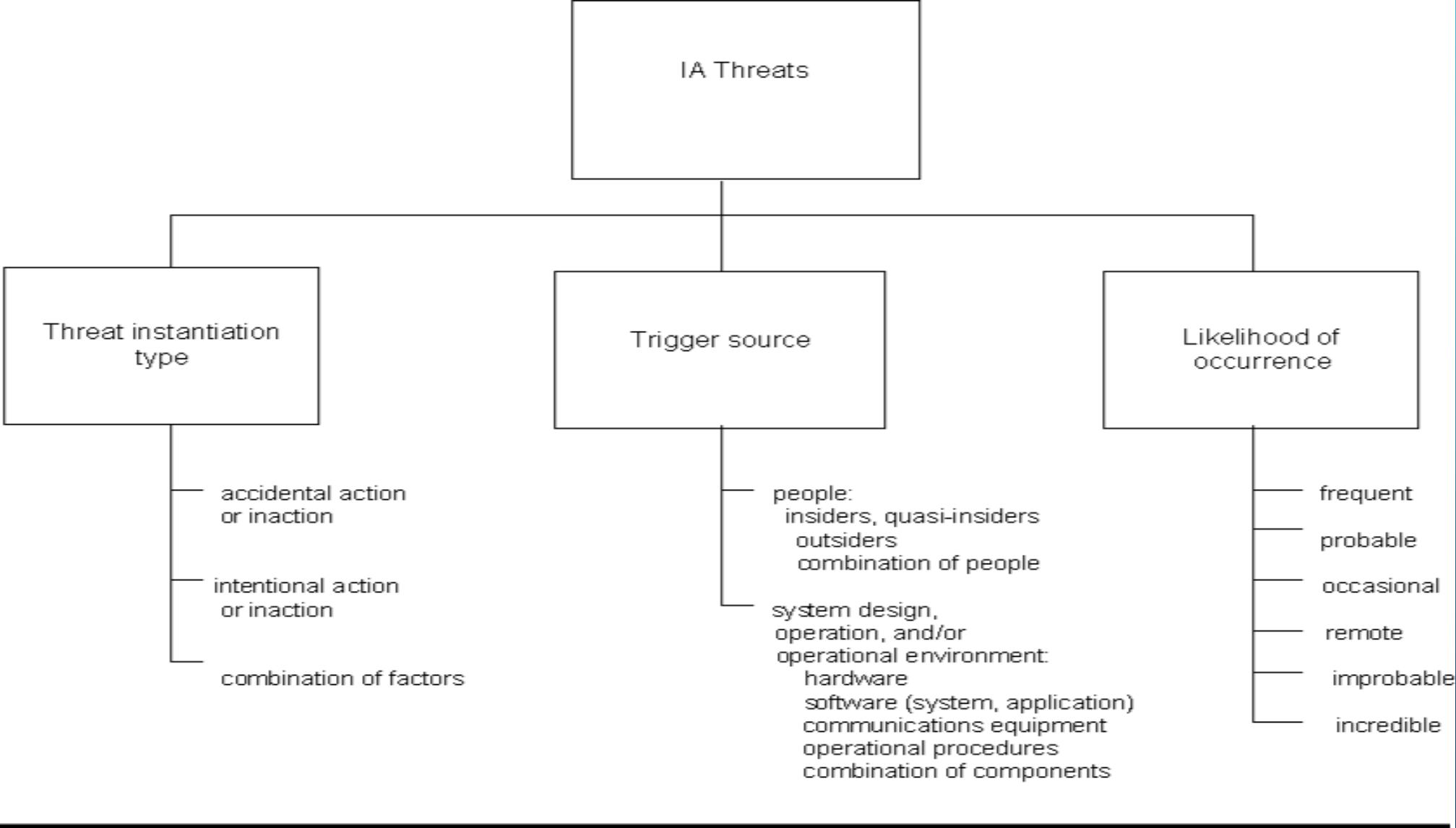
## KERENTANAN :

- Kerentanan dapat ada di sistem perangkat keras, perangkat lunak, peralatan komunikasi, prosedur operasional, dan lingkungan operasional.
- Kerentanan dapat berhubungan dengan keselamatan, keandalan, dan keamanan sistem
- Kerentanan dapat hasil dari tindakan disengaja atau tidak disengaja atau tidak disengaja.
- Secara historis, komunitas keamanan dan keandalan berfokus pada kerentanan yang tidak disengaja, sementara komunitas keamanan berfokus pada kerentanan yang disengaja berbahaya.
- Informasi keamanan/IA bersama-sama membawa perspektif yang berbeda.

# MENGIDENTIFIKASI ANCAMAN, JENISNYA, SUMBER, DAN KEMUNGKINAN

Ancaman keamanan informasi/IA dicirikan dalam tiga cara,

- Jenis tindakan yang dapat instantiate ancaman
- Sumber tindakan yang dapat memicu ancaman
- Kemungkinan terjadinya ancaman



# karakterisasi ancaman IA

# PERBEDAAN ANTARA KERENTANAN DENGAN ANCAMAN

- kerentanan (kelemahan dalam desain sistem, operasi, atau lingkungan operasional yang dapat dimanfaatkan)
- ancaman (potensi bahwa kelemahan akan dimanfaatkan).
- Sebuah ancaman dapat dipakai oleh tindakan yang tidak disengaja atau disengaja atau tidak bertindak, atau kombinasi faktor.
- Hal ini berbeda dari tindakan disengaja atau tidak bertindak dan tindakan disengaja atau tidak bertindak yang merupakan penyebab kerentanan.

# MENGIDENTIFIKASI ANCAMAN UNTUK SEMBILAN KERENTANAN YANG TERKAIT DENGAN SISTEM PERBANKAN ONLINE

**Exhibit 13 Threat Identification: Online Banking System**

as of date: _____			
Vulnerability	Instantiation Type	Trigger Source	Likelihood of Occurrence
1. Little or no error detection/ correction or fault tolerance	Accidental inaction	System design: system will corrupt itself	Frequent
2. If number of simultaneous users exceeds x, system becomes unstable and exhibits unpredictable behavior	Accidental or intentional action	System design: system will corrupt itself (accidental) People: insiders or outsiders who become aware of this design flaw may purposely exploit it (intentional)	Probable Occasional
3. Data files can be accessed directly without going through DBMS applications front-end	Intentional action	People: insiders or outsiders who become aware of this design flaw may purposely exploit it	Occasional
4. Suboptimal operational environment, sporadic system shutdown or unpredictable behavior	Accidental inaction	System design: system will corrupt itself	Occasional

<i>Vulnerability</i>	<i>Instantiation</i>		<i>Likelihood of Occurrence</i>
	<i>Type</i>	<i>Trigger Source</i>	
5. End users and system administrator lack sufficient training, limited understanding of system security features and procedures	Accidental or intentional action	People: insiders, by not understanding or following security procedures, create opportunities for outsiders to trigger more serious threats	Probable
6. Unsecure backups, archives	Intentional action	People: insiders or outsiders who become aware of this operational weakness may purposely exploit it	Occasional
7. Careless disposal of hardcopy printouts	Intentional action	People: insiders or outsiders who become aware of this operational weakness may purposely exploit it	Occasional
8. No control over portable equipment or storage media	Intentional action	People: insiders, or insiders colluding with outsiders, could purposely exploit this operational weakness	Occasional
9. COTS components installed with default values, guest accounts, possible trap doors	Intentional action	People: system components create the vulnerability, but it takes deliberate action on the part of insiders or outsiders to exploit it	Occasional

# karakterisasi ancaman sistem perbankan online

Mayoritas ancaman  
sengaja dipakai (56  
persen) dan dipicu oleh  
orang (67 persen).

Exhibit 14 Threat Characterization Summary: Online Banking System

as of date: \_\_\_\_\_

## I. Threat Instantiation Type Summary

Threats	Accidental		Intentional		Combination	
	#	%	#	%	#	%
Safety	—	—	—	—	—	—
Reliability	—	—	—	—	—	—
Security	—	—	2	22%	1	11%
Combination	2	22%	3	33%	1	11%
Total	2	22%	5	56%	2	22%

## II. Threat Trigger Source Summary

Threats	People		Systems		Combination	
	#	%	#	%	#	%
Safety	—	—	—	—	—	—
Reliability	—	—	—	—	—	—
Security	3	33%	—	—	—	—
Combination	3	33%	2	22%	1	11%
Total	6	67%	2	22%	1	11%

## III. Threat Likelihood Summary

Threats	Frequent		Probable		Occasional		Remote		Improbable		Incredible	
	#	%	#	%	#	%	#	%	#	%	#	%
Safety	—	—	—	—	—	—	—	—	—	—	—	—
Reliability	—	—	—	—	—	—	—	—	—	—	—	—
Security	—	—	1	11%	2	22%	—	—	—	—	—	—
Combination	1	11%	1	11%	4	45%	—	—	—	—	—	—
Total	1	11%	2	22%	6	67%	—	—	—	—	—	—

# KORELASI AWAL KEPARAHAN KERENTANAN DAN KEMUNGKINAN ANCAMAN UNTUK CONTOH PERBANKAN ONLINE.

- Dengan menggunakan informasi ini, prioritas dapat dibentuk untuk tindakan pengendalian ancaman. Satu kemungkinan pengelompokan akan:
- Prioritas tinggi: kerentanan 1, 3, 5, 6, 7
- Prioritas medium: kerentanan 2, 8, 9
- Prioritas rendah: kerentanan 4
- Prioritas diputuskan berdasarkan kasus per kasus, dengan mempertimbangkan berbagai parameter seperti: hukum dan peraturan, kewajiban dan masalah hukum lainnya,

# MENGEVALUASI JALUR TRANSAKSI, ZONA ANCAMAN, DAN EKSPOSUR RISIKO

- jalur transaksi potensial dikembangkan.
- kemudian zona ancaman dievaluasi
- dan paparan risiko awal ditentukan.

# JALUR TRANSAKSI POTENSIAL DIKEMBANGKAN.

- Jalur transaksi menangkap urutan peristiwa diskrit yang dapat menyebabkan peristiwa berlangsung-dalam hal ini,
- sistem yang akan diserang/dikompromikan.
- Jalur transaksi menggambarkan semua logis mungkin cara di mana suatu peristiwa mungkin terjadi.
- Jalur transaksi yang berkaitan dengan apa yang secara logis mungkin-bagaimana sesuatu dapat dicapai, bukan apakah itu layak, ekonomis, mungkin, dll.

# JALUR TRANSAKSI POTENSIAL DIKEMBANGKAN - LANJUTAN

- Semua jalur yang mungkin ditampilkan dalam satu diagram.
- Setiap peristiwa diskrit diberi nomor hieronis.
- Jalur individual mewakili rute unik dari acara teratas hingga peristiwa bawah. Simbol logika menentukan hubungan antara peristiwa alternatif.
- Jalur dikembangkan ke tingkat yang bermakna untuk membawa analisis.
- jalur transaksi juga dapat dikembangkan sebagai posteriori untuk merekonstruksi bagaimana kecelakaan/insiden terjadi.

# ZONA ANCAMAN DIEVALUASI

- Korelasi keparahan kerentanan dan kemungkinan ancaman
- Menganalisis jalur transaksi dari perspektif ancaman yang berbeda
- Mengisolasi zona ancaman kritis

- Apakah mengevaluasi keparahan kerentanan, kemungkinan ancaman, jalur transaksi, atau zona ancaman-bahwa kerugian dapat terjadi sebagai akibat dari tindakan disengaja atau disengaja atau tidak bertindak.
- Pada saat yang sama, Semua entitas dan faktor yang mempengaruhi desain, operasi, dan lingkungan operasional sistem harus dianalisis.
- Keamanan, keandalan, dan masalah keamanan harus dinilai secara tandem. Singkatnya, efektivitas pelaksanaan ancaman

# PAPARAN RISIKO AWAL DITENTUKAN

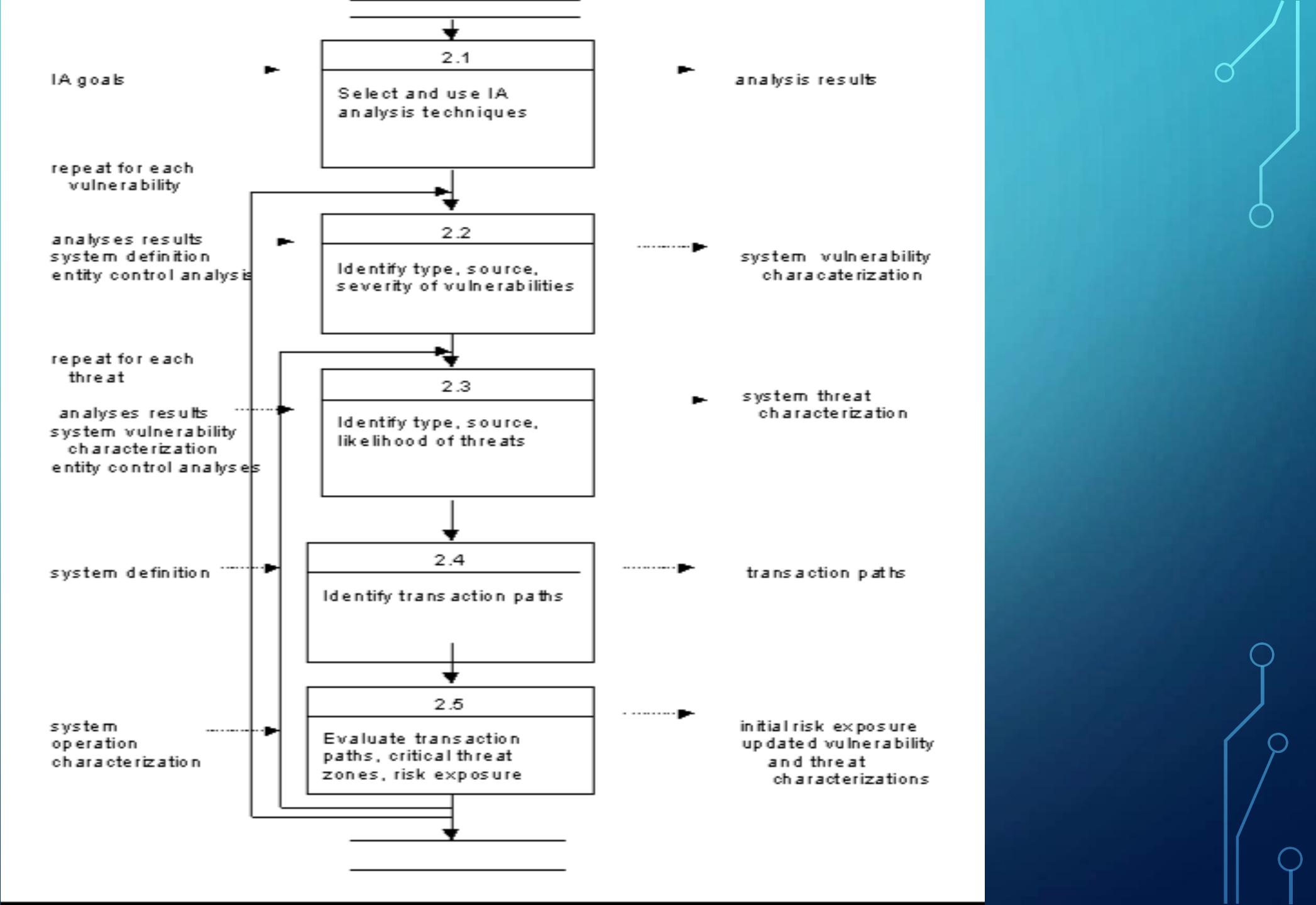
- tindakan pengendalian tergantung pada ketelitian analisis eksposur risiko yang mendahuluinya.
- Eksposur risiko ditentukan dan ditinjau secara bertahap:
  1. paparan risiko awal dipastikan untuk memprioritaskan tindakan pengendalian ancaman (Bab 5).
  2. tindakan pengendalian ancaman dilaksanakan sesuai dengan prioritas ini (Bab 6).
  3. efektivitas tindakan pengendalian ancaman (sisa risiko eksposur) diverifikasi (Bab 7).

# TINGKAT ANALISIS MEMPERKUAT DAN MEMPERBAIKI SATU SAMA LAIN (KERENTANAN DAN ANCAMAN) MEMBANTU UNTUK:

- Mengungkap kerentanan baru dan metode eksloitasi
- Memperbaiki definisi sumber ancaman dan perkiraan kemungkinan
- Meneliti perspektif ancaman yang berbeda
- Mengevaluasi bagaimana berbagai mode operasional dan keadaan dan elemen waktu berkontribusi terhadap eksposur risiko
- Optimalkan penerapan sumber daya kontrol ancaman dengan mengidentifikasi peristiwa tingkat rendah umum dalam jalur transaksi

# RINGKASAN

- Komponen kedua dari program Security/IA informasi yang efektif adalah analisis kerentanan dan ancaman
- Empat kegiatan yang dilakukan selama analisis kerentanan dan ancaman, seperti yang ditunjukkan pada gambar di bawah



- Kerentanan dan ancaman diidentifikasi dan dicirikan sehingga sumber daya dapat diterapkan untuk kebutuhan yang paling penting untuk mencegah kerugian.
- Identifikasi dan analisis kerentanan dan ancaman menganggap tindakan dan ketidaksengajaan yang tidak disengaja dan disengaja.
- Peristiwa individu serta kombinasi tidak direncanakan biasa dan urutan peristiwa yang dapat menyebabkan kegagalan/kompromi dianalisis.

# RINGKASAN KEGIATAN YANG TERLIBAT DALAM MELAKUKAN ANALISIS KERENTANAN DAN ANCAMAN

- Jalur transaksi yang dikembangkan untuk mengidentifikasi semua logis mungkin kombinasi kegiatan diskrit yang dapat menyebabkan sistem yang akan dikompromikan atau diberikan tidak dapat dioperasikan.
- Jalur transaksi dapat dikembangkan apriori untuk menentukan perlunya tindakan pengendalian ancaman, atau posteriori sebagai bagian dari kecelakaan/investigasi insiden.
- Jalur transaksi dianalisis dari perspektif beberapa pemangku kepentingan untuk memperbaiki kerentanan/ancaman penilaian dan mengungkap zona ancaman kritis.
- Eksposur risiko berasal dari berkorelasi kerentanan keparahan dan kemungkinan instasi ancaman, analisis transaksi jalan, dan mengisolasi zona ancaman kritis.

SEKIAN  
TERIMA KASIH

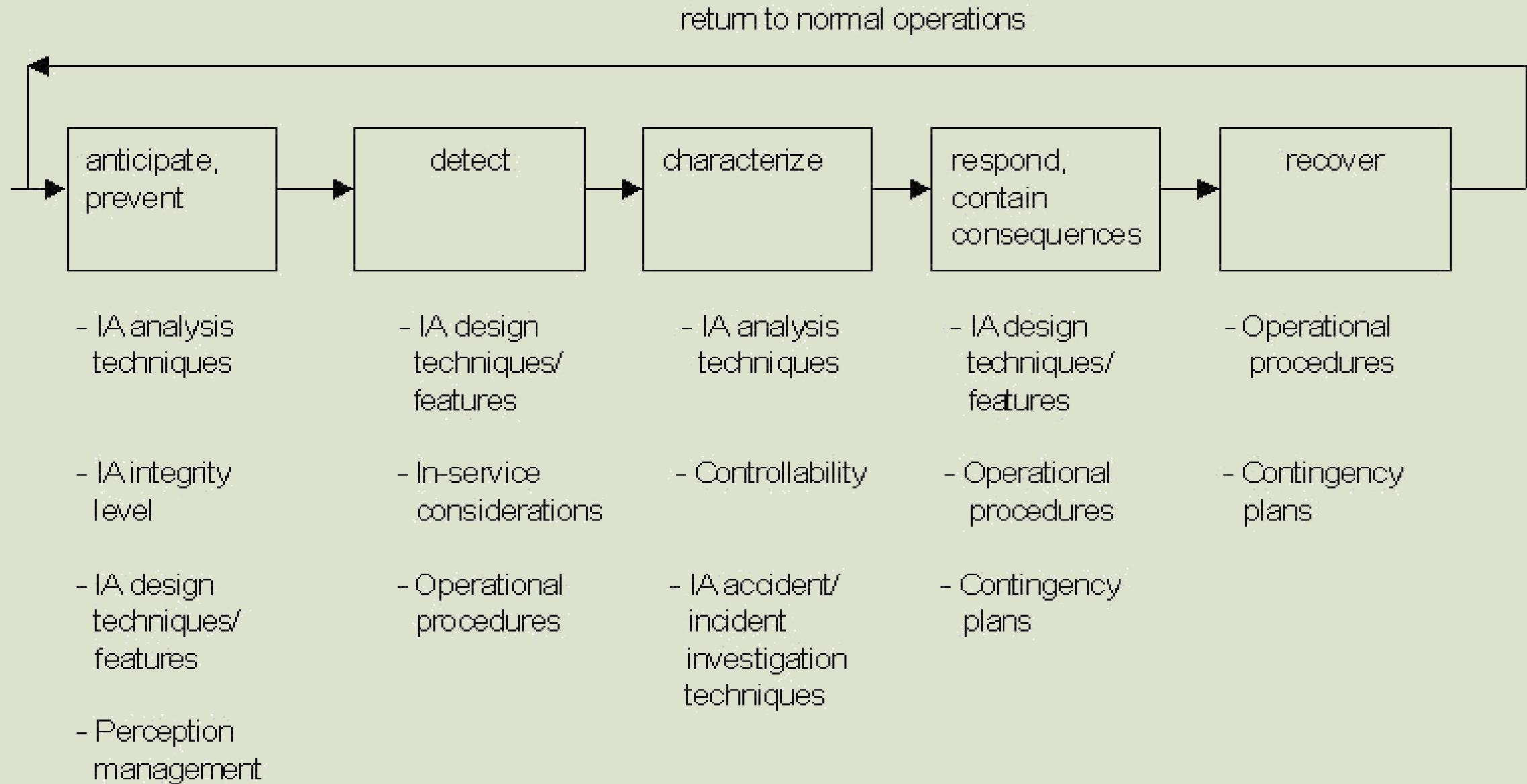
# Menerapkan pengukuran Kendali atas Ancaman

Mahasiswa mampu mendeskripsikan langkah-langkah dalam penerapan pengukuran Kendali atas Ancaman.

# Kegiatan yang dilakukan selama pelaksanaan tindakan pengendalian ancaman:

- Tingkat perlindungan yang diperlukan ditentukan.
- Pengendalian, prosedur operasional, dan pertimbangan dalam Layanan dievaluasi.
- Rencana dibuat untuk kontingensi dan pemulihan bencana.
- Penggunaan manajemen persepsi dipikirkan.
- Teknik dan Fitur desain IA dipilih dan diimplementasikan.

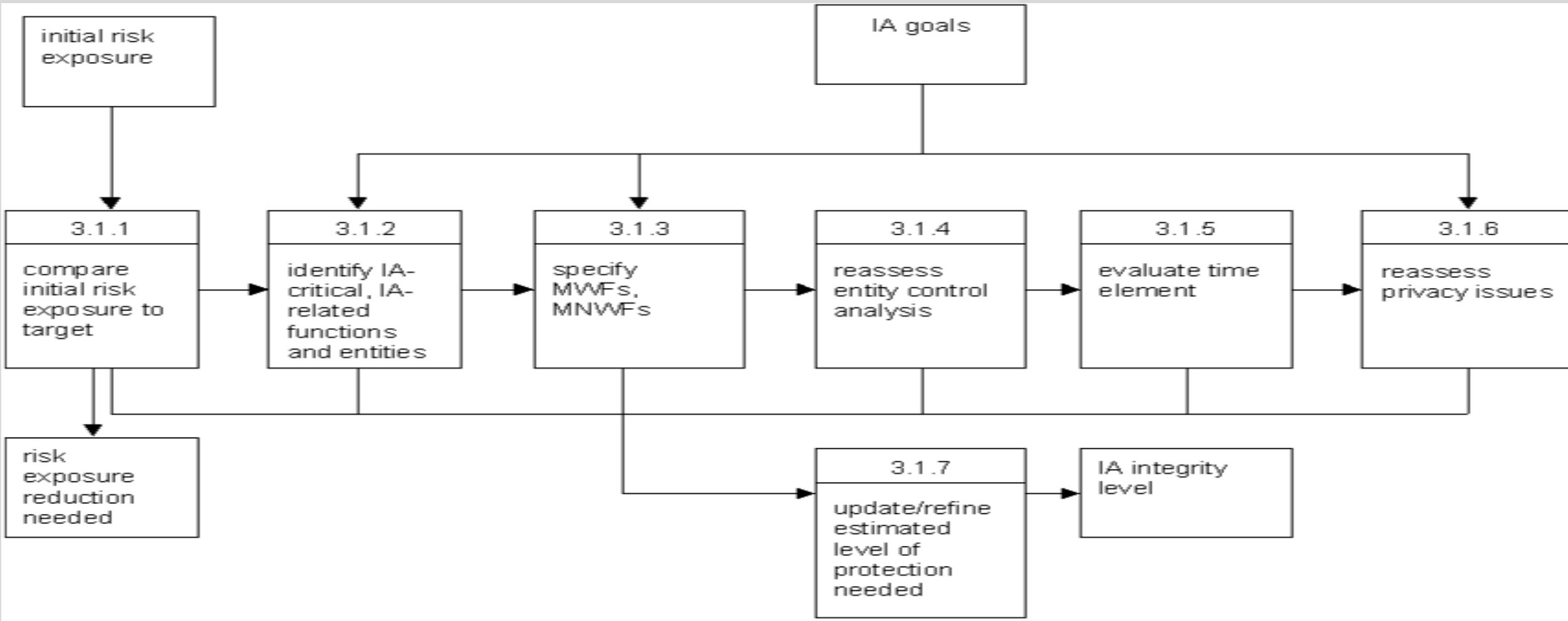
# Kronologi Pengukuran Kendali Ancaman



# Menentukan Berapa Banyak Perlindungan Yang Diperlukan

- perbandingan paparan risiko awal terhadap paparan risiko target
- analisis sistem entitas dan fungsi yang IA kritis atau IA terkait
- spesifikasi fungsi harus bekerja(MWF) dan fungsi tidak boleh bekerja (MNWF)
- analisis kontrol entitas sistem
- evaluasi dari elemen waktu relatif terhadap tindakan pengendalian ancaman yang diusulkan
- pemeriksaan ulang masalah privasi

# Kegiatan yang terlibat dalam penentuan tingkat perlindungan yang dibutuhkan



#### **Exhibit 4 High-Level Identification of Entity Criticality**

<i>Example</i>	<i>IA-Critical Entity/Function</i>	<i>IA-Related Entity/Function</i>	<i>Not IA-Critical or IA-Related</i>
Radiation therapy system	Functions that control the release of radiation Functions that verify that the type of radiation, dosage, etc. are within known safe parameters and consistent with the treatment plan	Functions that abort or inhibit the release of energy when an anomaly is detected	Remote billing system
Online banking system	Access control, authentication functions	Intrusion detection and response functions	Ancillary functions not related to account transactions
ATC system	Aircraft transmitter that sends location signal Radar signal transmitter/receiver ATC signal receiver ATC terminal displays	Voice communication system	Ancillary functions on ATC terminals not related to air traffic control mission

## Identifikasi Tingkat Tinggi Dari MWF Dan MNWF

Contoh	MWF	MNWF
System terapi Radiasi	<p>Fungsi bertanggung jawab untuk mengendalikan keakuratan pelepasan energi</p> <p>Fungsi yang memverifikasi parameter untuk pengobatan dalam sesi yang diketahui batas aman dan konsisten dengan rencana perawatan</p>	<p>Fungsi yang akan memungkinkan pelepasan radiasi yang keliru</p> <p>Fungsi yang akan memungkinkan rencana perawatan yang sedang berlangsung atau catatan perlakuan sejarah untuk diubah atau dihapus tanpa otorisasi</p>
Sistem Perbankan Online	<p>Fungsi yang bertanggung jawab menjaga kerahasiaan dan integritas transaksi dan data</p>	<p>Fungsi yang akan memungkinkan akses ke informasi akun tanpa otorisasi</p> <p>Fungsi yang akan memungkinkan akses kontrol/fitur otentikasi yang akan dilewati</p>
sistem ATC	<p>Fungsi yang bertanggung jawab untuk menjaga integritas dan ketersediaan informasi lokasi sinyal r/t</p>	<p>Fungsi yang memungkinkan r/t lokasi informasi sinyal yang akan diubah, dihapus, atau tertunda</p> <p>Fungsi yang akan memungkinkan dua pengendali untuk mengarahkan beberapa pesawat ke landasan pacu yang sama atau jalur penerbangan pada saat yang sama</p>

# Taksonomi keprihatinan privasi yang berkaitan dengan e-commerce, meliputi:

- Tidak benar akses ke komputer pribadi konsumen
- Tidak benar pengumpulan informasi pribadi konsumen
- Tidak semestinya memantau terhadap aktivitas Internet konsumen tanpa pemberitahuan atau otorisasi
- Tidak benar menganalisis informasi pribadi konsumen
- Tidak benar mengalihkan informasi pribadi konsumen kepada pihak ketiga
- Mengirimkan permohonan yang tidak diinginkan
- Tidak tepat menyimpan informasi pribadi konsumen

## Tingkat integritas IA digunakan :

1. Memprioritaskan distribusi sumber daya IA sehingga sumber daya yang diterapkan secara efektif dan kebutuhan yang paling kritis
2. Memilih tindakan pengendalian ancaman yang sesuai berdasarkan jenis, tingkat, dan tingkat perlindungan yang diperlukan.

# Identifikasi masalah privasi yang terkait dengan catatan medis, yaitu:

## Insider ancaman

Pengungkapan yang tidak disengaja

Keingintahuan Insider

Orang dalam-subordo

## Ancaman pengguna sekunder (kuasi-Insider)

Akses/penggunaan yang tidak terkendali

Ancaman luar

Akses/penggunaan yang tidak sah

# Kontrol Ancaman

Tindakan kontrol ancaman melampaui fitur desain dan teknik.

Tindakan pengendalian ancaman mencakup aspek apa pun yang dapat meningkatkan operasi sistem yang selamat, aman, dan andal.

Semua entitas, termasuk orang, diperiksa untuk peluang untuk mengurangi eksposur risiko dan meningkatkan integritas sistem.

## Kategori pengendalian :

1. **Tak terkendali**: tindakan manusia tidak berpengaruh
2. **Sulit dikendalikan**: potensi tindakan manusia
3. **Melemahkan**: respon manusia yang masuk akal
4. **Mengganggu**: keterbatasan operasional, respon manusia normal
5. **Gangguan**: keselamatan (atau keamanan) bukan masalah

## hubungan antara pengendalian dan tingkat integritas:

Kategori pengendalian untuk setiap bahaya mendefinisikan tingkat integritas yang diperlukan untuk desain sistem baru yang pada gilirannya mendefinisikan persyaratan untuk proses pembangunan.

# Pengendalian

- mencerminkan potensi efek mengurangi tindakan manusia sub-sequent untuk kerentanan eksploitasi dan instansi ancaman.
- tindakan manusia dapat diambil untuk mengurangi, mengandung, atau mendahului konsekuensi yang terungkap dari bahaya, fisik atau Cyber

## Prosedur operasional :

- adalah komponen utama dari tindakan pengendalian ancaman, meskipun mereka sering diabaikan seperti itu. Prosedur operasional yang totalitas dari keprihatinan IA relatif terhadap aman, aman, dan dapat diandalkan operasi dari sistem dalam lingkungan operasional.
- ditinjau untuk memastikan bahwa mereka dengan quately menangani semua masalah yang berkaitan dengan operasi personil, operasi perangkat lunak/data, dan operasi administras

# Pertanyaan berikut harus dijawab:

1. Apakah prosedur sesuai dengan tujuan IA, tingkat integritas IA, dan rencana kontinjensi? Apakah semua fitur keselamatan dan keamanan dan prosedur dijelaskan?
2. Lakukan prosedur sesuai dengan saat ini sebagai sistem yang dibangun, atau update yang diperlukan? Apakah prosedur menentukan lingkungan operasional yang benar dan setiap keterbatasan atau kendala yang dikenakan oleh itu?
3. Apakah prosedurnya lengkap? Apakah mereka mengatasi semua operasional mode/negara, misi, dan profil? Apakah mereka mengatasi dekomisioning sistem sensitif dan pembuangan informasi sensitif, termasuk password kadaluarsa dan kunci? Apakah cukup detail yang disediakan? Apakah informasi jelas, ringkas, tidak ambigu, dan dapat diakses dalam jumlah waktu yang wajar?
4. Mintalah anggota staf terlatih dalam cara mengikuti prosedur?
5. Apakah prosedur yang diikuti?

# Evaluasi pertimbangan dalam layanan

## 1. Kemampuan perawatan sistem,

Tindakan pemeliharaan, upgrade perangkat keras, peningkatan perangkat lunak, Versi baru produk COTS, dll dapat semua berpotensi berdampak pada tingkat integritas IA sistem

mendesain sebuah sistem sesuai fungsionalitasnya, terutama fungsi yang berhubungan dengan IA-kritis dan IA, dapat dipertahankan; dan (2) merancang sebuah sistem sehingga dapat diperoleh tanpa mengganggu tindakan pengendalian ancaman.

# Evaluasi pertimbangan dalam layanan

## 2. profil penggunaan sistem.

- Sebuah profil harus dikembangkan yang mendefinisikan diantisipasi rendah, normal, puncak, dan kelebihan atau kondisi jenuh.
- Pemuatan sistem dapat bervariasi menurut mode/status operasional, jumlah pengguna, waktu, waktu dalam seminggu, waktu tahun (hari libur), dsb.
- Karakteristik untuk setiap kategori pemuatan sistem harus didefinisikan dan dibandingkan dengan kendala/kapasitas sistem yang diketahui.
- Integritas IA-kritis func-tions, IA-fungsi terkait, dan tindakan pengendalian ancaman harus diverifikasi di bawah rendah, normal, dan puncak loading skenario.

# Perencanaan Kontingensi Dan Pemulihan Bencana

Bagian integral dari manajemen risiko secara umum dan menerapkan tindakan pengendalian ancaman pada khususnya

# Kontingensi

- a. suatu peristiwa, seperti keadaan darurat, yang mungkin tetapi kejadian yang tidak pasti,
- b. sesuatu yang bertanggung jawab terjadi sebagai tambahan untuk sesuatu yang lain,
- c. sesuatu yang terjadi secara kebetulan atau disebabkan oleh keadaan yang tidak sepenuhnya diramalkan.

Kontinjensi menyiratkan gagasan ketidakpastian, peristiwa tak terduga, dan yang tidak diketahui.

# Rencana kontingensi

- Mengidentifikasi strategi alternatif untuk diikuti atau tindakan yang harus diambil untuk memastikan keberhasilan misi yang sedang berlangsung harus **tidak diketahui, tidak pasti, atau tidak terduga** peristiwa terjadi.
- Rencana kontinjensi memberikan **respons terukur** direncanakan untuk peristiwa ini, berbeda dengan solusi yang **tidak direncanakan, respons yang salah, atau tidak ada respon sama sekali**, untuk mengembalikan sistem ke keadaan yang dikenal aman.

# Proses perencanaan kontingensi.

1. mengidentifikasi semua internal dan eksternal sistem entitas dan tingkat kontrol atas sistem
2. mengidentifikasi apa yang bisa salah dengan sistem dan entitas: kegagalan titik/mode dan kehilangan/kompromi skenario
3. respon yang tepat untuk masing-masing didefinisikan, konsisten dengan tujuan IA dan tingkat integritas IA.
4. menetapkan tanggung jawab untuk menggelar kursus alternatif tindakan dan sumber daya.

Pertanyaan ini ditangani dari dua sudut pandang :

- Sebab dan akibat: apa yang bisa terjadi dan apa yang akan menimpa (analisa penyebab konsekuensi)
- Efek dan penyebab: apa hasil yang harus dihindari atau didorong dan bagaimana masing-masing mungkin terjadi

**Perencanaan kontinjensi mengasumsikan scenario kasus terburuk sistem ATC , Pada tingkat tinggi, rencana kontingensi harus dibuat untuk skenario berikut:**

- Hilangnya sistem radar (tidak ada transmisi atau penerimaan)
- Hilangnya komunikasi suara antara pilot dan pengendali lalu lintas udara
- Hilangnya ATC DBMS
- Hilangnya terminal ATC
- Hilangnya sinyal lokasi dari pesawat terbang (tidak ada transmisi atau penerimaan) tidak ada pengendali lalu lintas udara di menara kontrol

# Manajemen Persepsi

alat yang berguna dalam banyak usaha, termasuk IA.

- Vendor memiliki kepentingan dalam mengelola harapan pelanggan.
- Pembicara memiliki kepentingan dalam mengelola ekspektasi khalayak.
- pemilik sistem memiliki kepentingan dalam mengelola realitas pengguna memandang relatif terhadap keselamatan, keamanan, dan dapat diandalkan operasi sistem.

# Manajemen persepsi melayani beberapa tujuan

- Pengguna akhir, Apakah pelanggan bisnis online atau karyawan organisasi, mendapatkan penipu dalam sistem dan hasil yang dihasilkan jika sistem tampaknya kuat dan memberikan informasi yang akurat dengan cepat sekaligus melindungi privasi.
- Sebagai penghalang untuk menjadi penyerang, baik di dalam maupun di luar organisasi; sistem ini dianggap sangat sulit untuk diserang
- Sistem seharusnya tidak tampak terlalu mudah untuk diserang.

# Tindakan pengendalian ancaman terutama diimplementasikan melalui

- teknik desain dan fitur,
- prosedur operasional,
- rencana kontinjensi,
- praktek keamanan fisik menjadi faktor utama lainnya.

Teknik desain dan fitur harus dipilih dengan cermat karena peran penting yang mereka mainkan dalam mencapai dan mempertahankan integritas IA.

# Memilih .....

- Tindakan pengendalian ancaman dipilih berdasarkan eksposur risiko target dan tingkat perlindungan dan tingkat integritas IA diperlukan
- Teknik desain keamanan dan fitur dipilih berdasarkan studi trade-off yang dievaluasi analisis risiko, tingkat risiko yang dapat ditoleransi, dan biaya.
- Tindakan kontrol ancaman tertentu dipilih sebagai respons terhadap kerentanan, bahaya, dan ancaman tertentu. Tindakan kontrol ancaman merupakan solusi untuk masalah tertentu yang ditentukan, maksudnya adalah untuk mengurangi paparan risiko awal pada atau di bawah target.
- Tindakan pengendalian ancaman harus dilaksanakan yang efisien, tidak menurunkan kinerja sistem, dan sesuai untuk tingkat eksposur risiko.

# Desain teknik dan fitur

- kumpulan metode yang sistem (atau komponen) dirancang dan kemampuan ditambahkan ke sistem untuk meningkatkan integritas IA.
- Untuk perangkat lunak/sistem kustom, mereka mewakili teknik dan fitur untuk mempekerjakan ketika merancang dan mengembangkan sistem.
- Untuk perangkat lunak/sistem COTS, mereka mewakili teknik dan fitur untuk menentukan dan evaluasi selama proses pemilihan/pengadaan produk.

# model ISO OSI.

Standar ini membahas berbagai topik, berlaku untuk lapisan yang berbeda dalam model, seperti:

- kontrol akses,
- jejak audit,
- otentikasi,
- tanda tangan digital,
- blok sandi,
- fungsi hashing,
- manajemen kunci, dan
- alarm keamanan.

# Ringkasan

- Komponen ketiga dari program keamanan/IA informasi yang efektif adalah pelaksanaan tindakan pengendalian ancaman. Lima kegiatan yang dilakukan selama pelaksanaan tindakan pengendalian ancaman
- Jenis, tingkat, dan tingkat perlindungan yang diperlukan ditentukan. Controllability, prosedur operasional, dan pertimbangan dalam Layanan dievaluasi.

TERIMA KASIH



# VERIFIKASI KEMANGKUSAN PENGUKURAN

MAHASISWA MAMPU MELAKUKAN VERIFIKASI KEMANGKUSAN  
PENGUKURAN PENGENDALIAN ANCAMA TERHADAP JAMINAN  
INFORMASI

## MEMVERIFIKASI EFEKTIVITAS TINDAKAN PENGENDALIAN ANCAMAN:

- Teknik verifikasi IA dipilih dan digunakan.
- Eksposur risiko sisa ditentukan dan penerimaan yang dievaluasi.
- Kerentanan, ancaman, dan survivability yang sedang berlangsung dipantau.

# EFEKTIVITAS TINDAKAN PENGENDALIAN ANCAMAN DIVERIFIKASI MELALUI PROSES 3 LANGKAH:

- Pastikan bahwa teknik/fitur desain IA yang sesuai dipilih.
- verifikasi bahwa teknik/fitur desain IA yang dilaksanakan dengan benar.
- verifikasi ketangguhan dan ketahanan dari tindakan pengendalian ancaman.

# TEKNIK VERIFIKASI IA

Teknik verifikasi IA	C/R	Type	Life-Cycle Phase		
			di mana teknik ini digunakan		
			Konsep	Pengembangan	Operasi
Analisis nilai batas	C3	All		X	x
Cleanroom	C3	All		X	
Analisis Aliran Kontrol	C3	All		X	x
Analisis aliran data atau informasi	C3	All		X	x
Partisi kelas ekuivalen	C3	All		X	x
Kebenaran Bukti Formal	C3	SA,SE	x	X	x
Pengujian Antarmuka	C3	All		X	x
Pengujian Kinerja	C3	All		X	x
Pengujian Statistik dan Probabilitas	C3	All		X	x
Pengujian Regresi	C3	All		X	x
Pemodelan Estimasi Keandalan	C3	RE		X	x
Kemampuan telusur Persyaratan (IA)	C3	All	x	X	x
Kasus Integritas Review IA	C3	All	x	X	x
Analisis Akar Penyebab	C3	All		X	x
Inspeksi, Ulasan, dan Audit Kenyamanan dan keamanan	C3	SA/SE		x	x
Pengujian Stres	C3	All		x	x
Analisis Testabilitas, Injeksi kesalahan, penyertaan kegagalan	C3	All		X	x
Pengujian Kegunaan	C3	All		X	x

# KETERANGAN

Kolom	Kode	Arti
Type	SA	teknik terutama mendukung rekayasa keselamatan
	SE	teknik terutama mendukung rekayasa keamanan
	RE	teknik terutama mendukung rekayasa kehandalan
	All	teknik terutama mendukung rekayasa keselamatan, keamanan, dan kehandalan
C/R	Cx	kelompok teknik pelengkap
	Rx	kelompok teknik redundan; hanya salah satu teknik berlebihan harus digunakan

# VERIFIKASI PERAN TEKNIK IA

Teknik	Peran Verifikasi IA
I. Teknik Verifikasi	
<b>Analisis nilai batas</b>	Mengidentifikasi kesalahan perangkat lunak yang terjadi pada fungsi dan entitas IA-kritis dan IA terkait saat memproses pada atau di luar batas parameter yang ditentukan, baik input atau output.
<b>Cleanroom</b>	Mencegah cacat dari diperkenalkan atau tersisa tidak terdeteksi pada fungsi dan entitas IA-kritis dan IA-terkait melalui evaluasi kelengkapan, konsistensi, ketepatan, dan jelas persyaratan, desain, dan implementasi.
<b>Analisis Aliran Kontrol</b>	Menemukan struktur logika program yang buruk dan tidak benar yang dapat membahayakan integritas IA.
<b>Analisis Aliran Data/Informasi</b>	Mengungkap transformasi dan operasi data yang tidak benar dan tidak sah yang dapat membahayakan integritas IA.
<b>Partisi Kelas Equivalensi</b>	Mengidentifikasi serangkaian kasus uji minimum dan data pengujian yang akan menguji setiap domain input secara memadai.
<b>Kebenaran Bukti Formal</b>	Membuktikan bahwa persyaratan, desain, dan implementasi fungsi dan entitas IA-Critical dan IA-terkait benar, lengkap, tidak ambigu, dan konsisten.

# VERIFIKASI PERAN TEKNIK IA

Teknik Verifikasi	Peran Verifikasi IA
Pengujian Antarmuka	Memverifikasi bahwa antarmuka persyaratan sudah benar dan bahwa antarmuka telah diterapkan dengan benar
Pengujian Kinerja	Memverifikasi apakah sistem akan memenuhi persyaratan kinerja yang dinyatakan dan persyaratan ini sudah benar.
Pengujian Statistik dan Probabilitas	memberikan penilaian kuantitatif dari integritas IA operasional; memverifikasi integritas desain terhadap profil operasional.
Pengujian Regresi	Memverifikasi bahwa perubahan atau penyempurnaan telah diterapkan dengan benar dan bahwa mereka tidak memperkenalkan kesalahan baru atau mempengaruhi integritas IA.
Pemodelan Estimasi Keandalan	Memperkirakan keandalan perangkat lunak untuk saat ini atau beberapa waktu mendatang
Kemampuan telusur Persyaratan (IA)	Memverifikasi bahwa (1) semua keamanan, keandalan, dan persyaratan keamanan yang berasal dari tujuan IA adalah benar; (2) semua persyaratan keselamatan, keandalan, dan keamanan telah diterapkan dengan benar pada produk akhir; dan (3) tidak ada tambahan kemampuan yang tidak ditentukan atau tidak diinginkan telah diperkenalkan.

# VERIFIKASI PERAN TEKNIK IA

Teknik Verifikasi	Peran Verifikasi IA
<b>Kasus Integritas Review IA</b>	Menentukan apakah klaim yang dibuat mengenai integritas IA dibenarkan oleh argumen dan bukti pendukung.
<b>Analisis Akar Penyebab</b>	Mengidentifikasi penyebab, peristiwa, kondisi, atau tindakan yang secara individu atau dalam kombinasi menyebabkan kecelakaan/insiden Menentukan mengapa Cacat tidak terdeteksi sebelumnya.
<b>Inspeksi, Ulasan, dan Audit Kenyamanan dan keamanan</b>	Mengungkap kesalahan dan kesalahan sepanjang hidup sistem yang dapat mempengaruhi integritas IA.
<b>Pengujian Ketahanan</b>	Menentukan (1) maksimum kondisi pemuatan puncak di mana sistem akan terus melakukan seperti yang ditentukan dan integritas IA akan dipertahankan, dan (2) sistem overload/saturasi kondisi yang dapat menyebabkan sistem kompromi atau kegagalan.
<b>Analisis Testabilitas, Injeksi kesalahan, penyertaan kegagalan</b>	Memverifikasi integritas IA dengan menentukan apakah desain sistem dapat diverifikasi dan dipelihara, dan bahwa ia mendeteksi dan merespon dengan benar untuk data yang keliru, kondisi, dan keadaan.
<b>Pengujian Kegunaan</b>	Tentukan apakah sistem bekerja di lingkungan operasional dengan cara yang dapat diterima dan dimengerti oleh administrator dan pengguna akhir; memverifikasi bahwa desain tidak berkontribusi untuk diinduksi atau mengundang kesalahan yang dapat menyebabkan sistem kompromi atau kegagalan.

# VERIFIKASI PERAN TEKNIK IA

I. Teknik Analisis	Peran Verifikasi IA
<b>Analisis Konsekuensi Penyebab</b>	Mengidentifikasi tindakan pengendalian ancaman yang tidak pantas, tidak efektif, dan hilang; memverifikasi bahwa semua mode kegagalan yang disengaja dan disengaja memiliki ukuran kontrol ancaman yang sesuai.
<b>Analisis Kegagalan Penyebab Umum</b>	Memverifikasi bahwa komponen desain toleransi kesalahan yang kebal terhadap CCFs.
<b>Analisis Pohon Peristiwa</b>	Mengidentifikasi tindakan pengendalian ancaman yang tidak pantas, tidak efektif, dan hilang.
<b>Studi HAZOP</b>	memverifikasi bahwa semua kecelakaan dan disengaja, fisik dan Cyber, bahaya yang terkait dengan operasi dari sistem telah dihilangkan atau dikurangi

# VERIFIKASI PERAN TEKNIK IA

I. Teknik Analisis	Peran Verifikasi IA
<b>Petri Nets</b>	Petri verifikasi bahwa kondisi kemacetan, ras, dan nondeterministik yang dapat menyebabkan sistem kompromi atau kegagalan tidak ada.
<b>Software, System FMECA</b>	Memeriksa efek kegagalan disengaja dan tidak disengaja, acak dan sistematis pada perilaku sistem secara umum dan IA integritas pada khususnya
<b>Software, system FTA</b>	Mengidentifikasi potensi akar penyebab dari sistem yang tidak diinginkan kejadian (kebetulan dan disengaja) untuk memverifikasi efektivitas mengurangi fitur desain dan prosedur operasional.
<b>Analisis Sirkuit Menyelinap</b>	Memverifikasi bahwa semua tersembunyi, tidak disengaja, dan tidak sah perangkat keras dan perangkat lunak jalur Logis atau urutan kontrol yang dapat menghambat fungsi sistem yang diinginkan, memulai peristiwa sistem yang tidak diinginkan, atau menyebabkan kesalahan waktu dan pengurutan telah dihapus.

# VERIFIKASI PERAN TEKNIK IA

I. Teknik Investigasi Kecelakaan/insiden	Peran Verifikasi IA
<b>Analisis Penghalang</b>	pastikan lapisan defensif gagal atau hilang atau tidak memadai selama kecelakaan/insiden.
<b>Analisis Efek Modus Bahaya</b>	Postulat yang mekanisme ancaman tertentu menyebabkan kecelakaan/insiden dari analisis mode kerusakan.

# MENENTUKAN EKSPOSUR RISIKO RESIDUAL

- Apakah tindakan pengendalian ancaman mengurangi kemungkinan dan tingkat keparahan potensi bahaya seperti yang direncanakan?
- Apakah paparan risiko awal telah dikurangi menjadi ALARP?
- Apakah eksposur risiko Residual diterima dalam kendala operasional yang diketahui?
- Apakah tingkat integritas IA yang ditentukan telah ditunjukkan?
- Adakah peluang untuk memperbaiki atau mengoptimalkan teknik/fitur desain IA, prosedur operasional, rencana kontinjensi, atau praktik keamanan fisik?

## EKSPOSUR RISIKO RESIDUAL DIEVALUASI UNTUK SEMUA SKENARIO YANG BERLAKU:

- Mode/keadaan operasional yang berbeda, profil, lingkungan, dan misi
- kondisi dan kejadian normal dan abnormal
- bahaya secara independen, ketergantungan, dan simultan
- Kegagalan secara acak dan sistematis
- kegagalan disengaja dan kegagalan disengaja
- berbahaya fisik dan Cyber

# TUJUH FAKTOR UTAMA DISELIDIKI SEBAGAI BAGIAN DARI PENILAIAN EFEKTIFITAS TINDAKAN PENGENDALIAN ANCAMAN :

- kesesuaian dari sekumpulan teknik untuk menghilangkan atau mengurangi kerentanan ini/ancaman
- Efektivitas sekumpulan teknik ini terhadap semua operasional mode/keadaan dan profil di mana kerentanan/ancaman ini terjadi (sistem operasi karakterisasi ditinjau)
- Apakah sekumpulan teknik ini mencakup semua lapisan dalam model referensi TCP/IP atau ISO OSI di mana kerentanan/ancaman terjadi
- Apakah sekumpulan teknik ini mencakup semua tahapan dari kronologi kontrol ancaman
- Apakah EAL yang tepat dan analisis statis dan dinamis hasil positif
- Apakah tingkat integritas IA menunjukkan sesuai dengan tingkat integritas IA
- Apakah sekumpulan teknik ini memberikan pertahanan yang memadai secara mendalam

# KASUS INTEGRITAS IA

- cara yang sistematis untuk mengumpulkan, mengatur, menganalisa, dan melaporkan data yang dibutuhkan oleh otoritas internal, kontraktual, regulasi, dan sertifikasi untuk mengkonfirmasi bahwa sistem telah memenuhi tujuan dan tingkat integritas IA yang ditentukan dan cocok untuk digunakan dalam lingkungan operasional yang dituju.
- Menyajikan informasi secara logis, lengkap, dan ringkas

# BUKTI PENILAIAN EFEKTIVITAS PENGENDALIAN ANCAMAN

Sistem/entitas :

Tanggal :

## I. Identifikasi kerentanan/ancaman identifikasi

No	Deskripsi	Keparahan	Kemungkinan	Hadir pada layer	
				TCP/IP	ISO OSI
1					

## II. Pengukuran Kontrol Ancaman

Teknik/fitur Desain IA	Efektifitas dalam layer		Efektifitas Kronologi Kontrol Ancaman			EAL	Level Integritas IA
	TCP/IP	ISO OSI	A/P	D/C	R/R		
1a							
1b							
1c							

## III. Penilaian

- a. Apakah seperangkat teknik ini yang sesuai untuk menghilangkan atau mengurangi kerentanan /ancaman ini?
- b. Apakah seperangkat teknik ini yang efektif terhadap semua mode operasional/keadaan dan profil di mana kerentanan/ancaman ini terjadi?
- c. Apakah seperangkat teknik ini mencakup semua lapisan di mana kerentanan/ancaman terjadi?
- d. Apakah seperangkat teknik ini mencakup semua tahapan pada kronologi kendali ancaman?
- e. untuk setiap teknik/fitur: (a) adalah EAL sesuai? (b) adalah hasil analisis statis dan dinamis positif?
- f. Apakah tingkat integritas IA ditunjukkan dari seperangkat teknik yang konsisten dengan tingkat integritas IA yang diperlukan?
- g. Apakah seperangkat teknik ini memberikan pertahanan yang memadai secara mendalam?
- h. Apakah ada mismatches atau kesenjangan dalam mengendalikan kerentanan ini/ancaman?

# TABEL RINGKASAN EFEKTIVITAS CONTROL ANCAMAN

**Exhibit 8 Threat Control Effectiveness Summary**

Assessment Criteria	Vulnerability/Threat Severity							
	Catastrophic		Critical		Marginal		Insignificant	
	#	%	#	%	#	%	#	%
1. TCP or ISO OSI layers:								
a. Covered								
b. Not covered								
2. Operational modes/states, operational profiles:								
a. Covered								
b. Not covered								
3. Phases of threat control chronology:								
a. Covered								
b. Not covered								
4. EAL, static and dynamic analysis results:								
a. Appropriate								
b. Inappropriate								
5. Demonstrated IA integrity level:								
a. Appropriate								
b. Inappropriate								
6. Defense in depth:								
a. Adequate								
b. Inadequate								
7. Threat control gaps or mismatches:								
a. None remaining								
b. Some remaining								
Total vulnerabilities/threats		100%		100%		100%		100%

# KASUS INTEGRITAS IA HARUS DITINJAU/DIVALIDASI ULANG SETIAP KALI ADA CLAIM

- dokumen hidup
- ditinjau pada tonggak reguler untuk memverifikasi bahwa sistem berada di jalur yang tepat untuk mencapai atau mempertahankan tujuan dan tingkat integritas IA

# STRUKTUR KASUS INTEGRITAS IA

Sistem :-

Untuk : \_\_

Ulasan terakhir/persetujuan: \_\_

1. IA tujuan
  - a. IA tujuan untuk sistem ini
  - b. pemberian untuk tujuan IA
  - c. tingkat integritas IA diperlukan untuk sistem ini
2. Asumsi dan klaim
  - a. asumsi tentang lingkungan pengembangan, lingkungan operasional, profil operasional, misi operasional
  - b. klaim tentang pengalaman sebelumnya dengan sistem dan teknologi yang serupa
  - c. klaim tentang desain, pengembangan, dan teknik verifikasi dan proses yang digunakan
  - d. evaluasi produk COTS oleh laboratorium independen, seperti EAL
3. (Current) bukti
  - a. karakterisasi kerentanan sistem
  - b. karakterisasi ancaman sistem
  - c. zona ancaman kritis
  - d. IA desain teknik/fitur yang dilaksanakan
  - e. menunjukkan tingkat integritas IA
  - f. penilaian efektivitas pengendalian ancaman dan ringkasan
  - g. eksposur risiko Residual
4. Masalah luar biasa
5. Kesimpulan dan rekomendasi
  - a. pengembang sistem
  - b. pemilik sistem
  - c. otoritas regulator (jika ada)
  - d. otoritas sertifikasi
6. Persetujuan, sejarah sertifikasi

# **MEMANTAU EKSPOSUR RISIKO YANG SEDANG BERLANGSUNG, TANGGAPAN, DAN SURVIVABILITY**

- Efektivitas tindakan pengendalian ancaman selama fase dalam layanan dari suatu sistem sering dinilai sebagai fungsi dari survivability
- Survivability didefinisikan sebagai kemampuan sebuah sistem untuk memenuhi misinya, pada waktu yang tepat, dengan adanya serangan, kegagalan, atau kecelakaan.

# **SURVIVABILITY TERGANTUNG PADA TIGA KEMAMPUAN UTAMA**

- *Perlawan* : kemampuan sistem untuk mengusir serangan
- *Pengakuan* : kemampuan untuk mendeteksi serangan ketika mereka terjadi dan untuk mengevaluasi tingkat kerusakan dan kompromi.
- *Pemulihan* : mempertahankan layanan dan aset penting selama serangan, membatasi tingkat kerusakan, dan mengembalikan layanan penuh setelah serangan

# PENILAIAN SURVIVABILITY MENCAKUP KRONOLOGI KONTROL ANCAMAN PENUH:

- mengantisipasi/mencegah,
- mendekksi/mencirikan,
- merespon/pulih

# MAINTAINABILITY

- *adalah penilaian sistematis dari efektivitas strategi pemeliharaan dan dapat memiliki pengaruh yang cukup besar pada keselamatan dan keamanan sistem*

# RINGKASAN

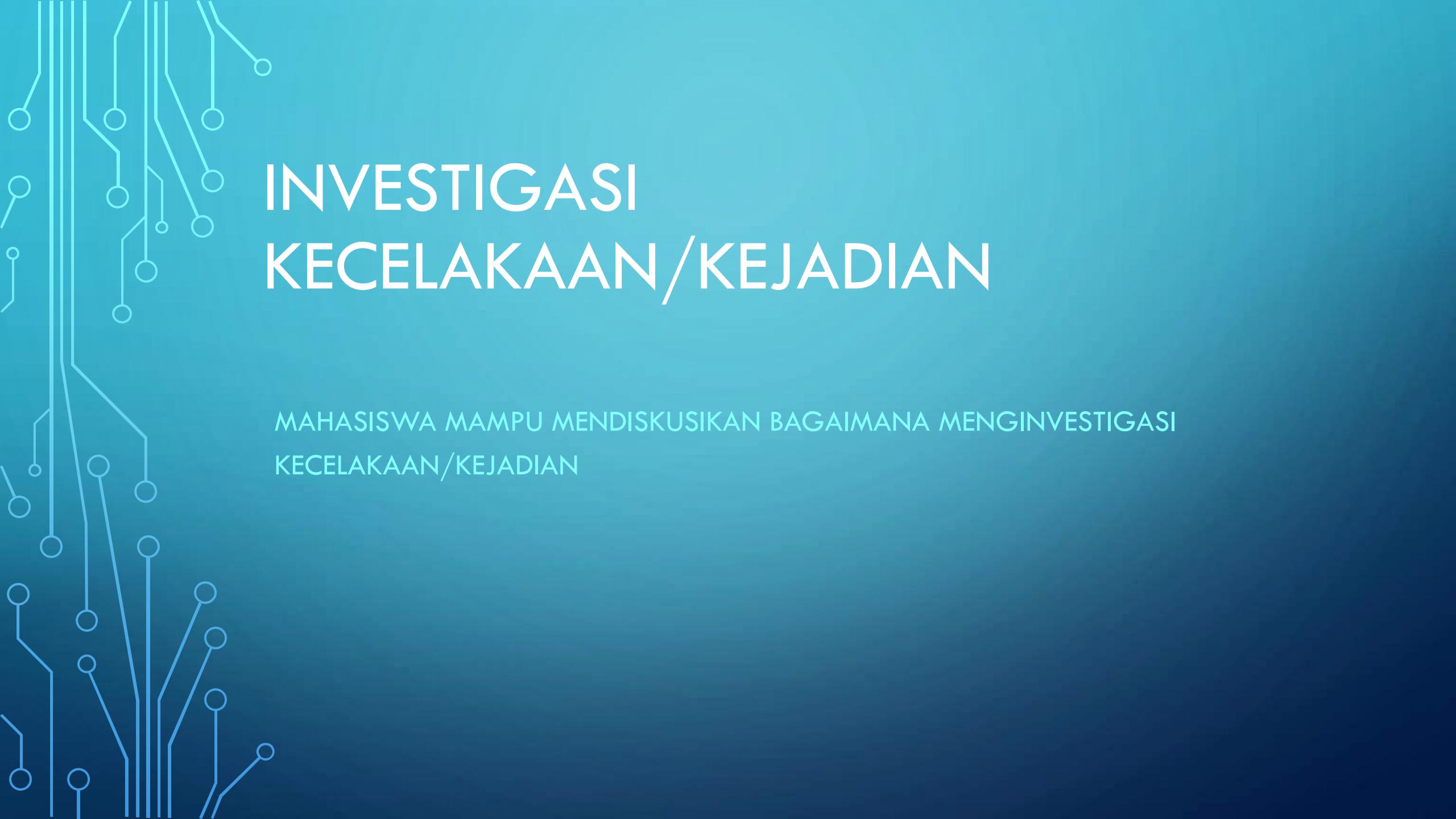
- Komponen keempat dari program keamanan/IA informasi yang efektif adalah memverifikasi efektivitas tindakan pengendalian ancaman.
- Tiga kegiatan dilakukan ketika memverifikasi efektivitas tindakan pengendalian ancaman :
  - Teknik verifikasi IA dipilih dan digunakan.
  - Eksposur risiko residual ditentukan dan penerimaan dievaluasi.
  - Kerentanan, ancaman, dan survivability yang sedang berlangsung dipantau.

Kombinasi Teknik Analisis Statis Dan Dinamis Digunakan Untuk Memverifikasi Efektivitas Tindakan Pengendalian Ancaman Sepanjang Hidup Suatu Sistem. Proses Tiga Langkah Diikuti:

- Pastikan bahwa teknik/fitur desain IA yang sesuai dipilih.
- verifikasi bahwa teknik/fitur desain IA yang dilaksanakan dengan benar.
- verifikasi ketangguhan dan ketahanan dari tindakan pengendalian ancaman.

Tanpa Verifikasi Aktual, Tidak Ada Dasar Faktual Untuk  
Mengklaim Bahwa Sistem Selamat, Aman, Atau Dapat  
Diandalkan.

TERIMA KASIH



# INVESTIGASI KECELAKAAN/KEJADIAN

MAHASISWA MAMPU MENDISKUSIKAN BAGAIMANA MENGINVESTIGASI  
KECELAKAAN/KEJADIAN

## KEGIATAN BERIKUT DILAKUKAN SAAT MELAKUKAN PENYELIDIKAN KECELAKAAN/KEJADIAN:

- Penyebab, luasnya, dan konsekuensi dari kegagalan/kompromi dianalisis.
- Mekanisme pemulihan dimulai.
- Kecelakaan/kejadian ini dilaporkan.
- Tindakan Remedial disebarluaskan.
- Masalah hukum dievaluasi.

# BEBERAPA ISTILAH YANG DIGUNAKAN

- **Kecelakaan(accident)**
  1. teknis — setiap peristiwa, urutan, atau kombinasi peristiwa yang tidak direncanakan atau tidak diinginkan yang mengakibatkan kematian, cedera, atau penyakit pada personel atau kerusakan atau hilangnya peralatan atau properti (termasuk data, kekayaan intelektual, dll.), atau kerusakan pada environment
  2. hukum — setiap kejadian yang tidak menyenangkan atau disayangkan yang menyebabkan cedera, kehilangan, penderitaan, atau kematian; sebuah peristiwa yang terjadi tanpa pandangan ke depan atau harapan

- **Kejadian (Incident)**

setiap kejadian yang tidak direncanakan atau tidak diinginkan, urutan, atau kombinasi dari peristiwa yang tidak mengakibatkan kematian, cedera, atau penyakit pada personil atau kerusakan atau kehilangan peralatan, properti (termasuk data, kekayaan intelektual, dll), atau kerusakan lingkungan, tetapi memiliki potensi untuk melakukannya.

- **Kegagalan/ Failure:**

gagal atau ketidakmampuan suatu sistem, entitas, atau komponen untuk melakukan fungsi yang diperlukan, sesuai dengan kriteria kinerja yang ditentukan, karena satu atau lebih kondisi kesalahan.

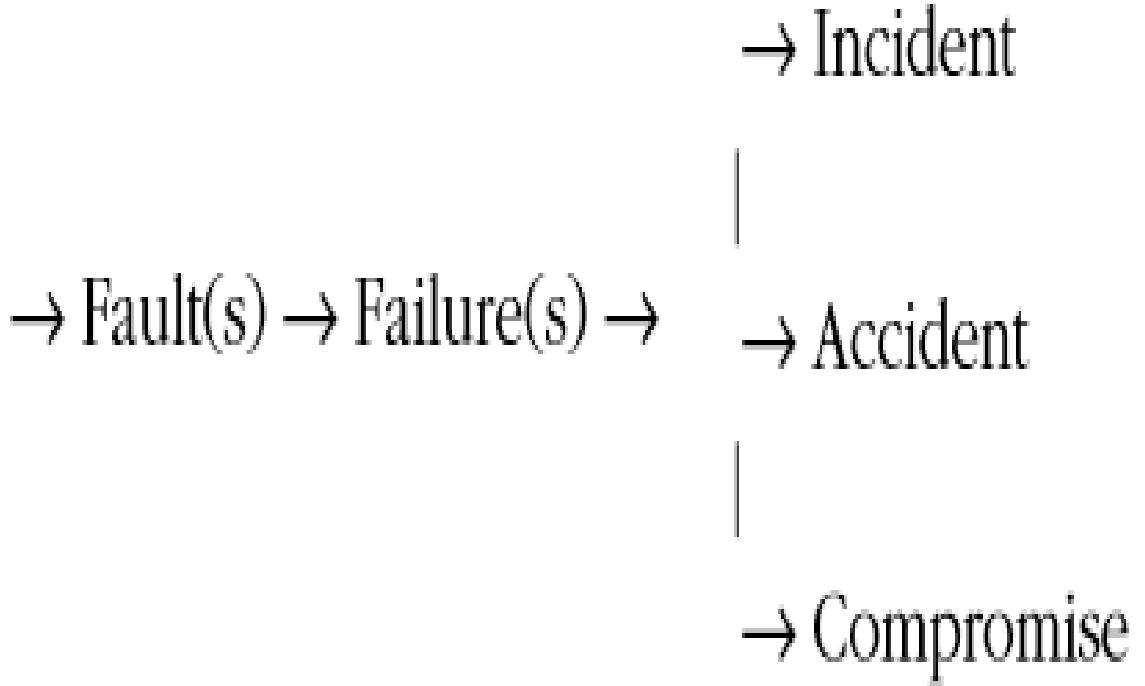
- **Kompromi/Compromise:**

yang tidak beralasan dan tidak diundang serangan ofensif, pelanggaran, atau gangguan dari suatu sistem, biasanya dengan siluman, yang mengalahkan keselamatan dan mekanisme keamanan untuk melanggar dan merebut sumber daya dan data dalam cara yang bermusuhan dan merugikan.

# TIGA KATEGORI KEGAGALAN

1. gagasan kegagalan adalah kegagalan yang akan terjadi;
2. kegagalan keras adalah kegagalan yang mengakibatkan shutdown sistem yang lengkap; dan
3. kegagalan lunak adalah kegagalan yang mengakibatkan transisi ke mode terdegradasi operasi atau gagal status operasional. kegagalan, khususnya fungsi/entitas dengan IA-kritis atau IA terkait, berdampak langsung pada integritas IA.

Accidental or intentional  
error or mistake



→ Incident

→ Accident

→ Compromise

- **Penyebab/ Cause:**

tindakan atau kondisi di mana peristiwa berbahaya (fisik atau Cyber) dimulai — peristiwa memulai. Penyebabnya mungkin timbul akibat kegagalan, kesalahan manusia yang disengaja atau tidak disengaja, ketidakcukupan Desain, diinduksi atau lingkungan operasional alami, konfigurasi sistem, atau mode/keadaan operasional.

# PENYEBAB, LUASNYA, DAN KONSEKUENSI DARI KEGAGALAN/KOMPROMI DIANALISIS

- Kecelakaan/kejadian selama fase pengembangan merupakan:
  - ✓ Kecelakaan/kejadian selama fase pengembangan merupakan :indikasi kekurangan desain yang mendasari,
  - ✓ kesalahpahaman tentang operasi atau misi sistem, dan komponen yang tidak kompatibel.
- Kecelakaan/kejadian selama fase operasional dapat timbul dari
  - salah satu penyebab di atas, serta
  - kekurangan dalam lingkungan operasional, prosedur operasional, praktik keamanan fisik, dan karakteristik sistem survivability

# BEBERAPA ALASAN KUAT UNTUK MENYELIDIKI KECELAKAAN/KEJADIAN

- menentukan sebenarnya apa yang dilakukan dan tidak terjadi, bagaimana hal itu terjadi, dan mengapa hal itu terjadi atau diizinkan terjadi
- memastikan sejauh mana konsekuensi dan kebutuhan yang sesuai untuk (segera) mekanisme pemulihan, dan (jangka panjang) perbaikan langkah
- mengumpulkan informasi yang diperlukan untuk mengajukan laporan yang akurat dari kecelakaan/kejadian
- mengevaluasi masalah hukum

# PERBANDINGAN HUKUM DAN REKAYASA PENYEBAB KATEGORI

Kategori Legal	Kategori Rekayasa	Definisi
<b>Penyebab bersamaan</b>	tidak ada rekayasa yang tepat setara. Penyebab bersamaan mungkin dianggap sebagai penyebab tergantung paralel akar.	Penyebab bertindak serentak dan bersama-sama, menyebabkan cedera yang tidak akan terjadi dengan tidak adanya baik. Dua penyebab berbeda yang beroperasi pada saat yang sama untuk menghasilkan hasil yang diberikan.
<b>Penyebab Berkontribusi</b>	tidak ada rekayasa yang sama persis. Penyebab Berkontribusi mungkin dianggap sebagai penyebab menengah.	Setiap faktor yang berkontribusi pada hasil, meskipun perhubungan kausal mungkin tidak segera
<b>Penyebab intervensi</b>	tidak ada rekayasa yang tepat setara. Penyebab intervensi yang positif dapat diakibatkan oleh tindakan pengendalian ancaman yang efektif, lapisan defensif, atau tanggap darurat. Sebab campur tangan yang negatif mungkin timbul dari tindakan manusia yang salah sebagai respon terhadap pendahulu kecelakaan.	Sebuah penyebab independen yang campur tangan antara peristiwa asli dan kecelakaan/kejadian, meniadakan program alami peristiwa, dan menghasilkan hasil yang berbeda, positif atau negatif.

Kategori Legal	Kategori Rekayasa	Definisi
<b>Penyebab Langsung, proximate, atau hukum</b>	Penyebab dasar, mendasari, atau akar penyebab	penyebab mendasar, peristiwa, kondisi, atau tindakan yang secara individu atau dalam kombinasi menyebabkan kecelakaan/insiden; peristiwa pendahulu utama yang memiliki (memiliki) potensi untuk dikoreksi.
<b>penyebab yang mungkin atau wajar</b>	tidak ada rekayasa setara.	Sebuah dasar yang wajar untuk kepercayaan dalam dugaan tertentu fakta. Satu set probabilitas didasarkan pada pertimbangan faktual dan praktis yang mengatur keputusan yang masuk akal dan bijaksana orang dan lebih dari sekadar kecurigaan tetapi kurang dari kuantum bukti yang diperlukan untuk keyakinan.
<b>Penyebab jarak jauh</b>	tidak ada rekayasa setara.	Suatu perkara yang tidak sesuai dengan pengalaman umat manusia menuntun pada peristiwa yang terjadi.
<b>tidak ada hukum yang setara</b>	Penyebab antara	Peristiwa antara penyebab yang mendasari dan kecelakaan/kejadian yang terjadi dalam rantai peristiwa langsung; epiphenomenon

## REKOMENDASI DALAM PERENCANAAN, KOORDINASI, DAN PELATIHAN UNTUK MENGATASI MASALAH :

- Kecepatan, akurasi, dan kelengkapan dari pengumpulan informasi
- saluran dan tanggung jawab pelaporan, dalam dan di luar team
- bentuk Laporan standar (draft dan terakhir)
- Daftar peserta yang ditunjuk, per skenario kecelakaan, untuk memastikan tim interdisipliner
- Daftar generik pertanyaan untuk bertanya, per scenario kecelakaan, untuk merangsang jalan investigasi
- Rantai tahanan tetap untuk bukti, mengingat sifat sekilas dari prosedur bukti digital untuk mendapatkan persetujuan dari saksi sebelum melakukan wawancara insiden kritis

# GAMBARAN TUGAS UTAMA DARI PENYELIDIKAN KECELAKAAN/KEJADIAN

- definisi umum formal pengaruh kausal
- Tepat spesifikasi sistem dan perilaku entitas
- Pengumpulan bukti dan analisis
- metode untuk melacak lebih banyak bukti dari bukti di tangan
- metode memvalidasi penalaran kausal

# TEKNIK INVESTIGASI/PENYELIDIKAN SELAMA KECELAKAAN/KEJADIAN

Teknik investigasi Kecelakaan/kejadian IA	C/R	Type	Life-Cycle Phase		
			di mana teknik ini digunakan		
			Konsep	Pengembangan	Operasi
<b>Analisis nilai batas</b>	C4	SA, SE		x	x
<b>Interview insiden kritis</b>	C4	SA, SE		x	
<b>Analisis efek mode bahaya peristiwa dan faktor kausal charting</b>	C4	SA, SE		x	x
<b>Analisis Skenario</b>	R4/C4	SA, SE		x	x
<b>berurutan berjangka waktu plot acara sistem investigasi</b>				x	x
<b>Analisis waktu/Rugi (TLA) untuk respon tanggap darurat</b>	C4	SA, SE			x
<b>Analisis saat peringatan</b>	C4	SA, SE			x

# PERAN INVESTIGASI KECELAKAAN/KEJADIAN TEKNIK IA

Teknik Innestigasi	Aturan Investigasi Kecelakaan/kejadian IA
<b>Analisis nilai batas</b>	Tentukan lapisan defensif yang gagal atau hilang atau tidak memadai selama kecelakaan/kejadian.
<b>Interview kejadian kritis</b>	mengumpulkan bukti tentang kecelakaan/kejadian dan sebelumnya terkait kesalahan, anomali, dan dekat-rindu dari personil operasional.
<b>Analisis efek mode bahaya</b>	Postulate yang mekanisme ancaman tertentu menyebabkan kecelakaan/kejadian dari analisis mode kerusakan.
<b>peristiwa dan faktor kausal charting</b>	secara grafis merekonstruksi peristiwa, segera, menengah, dan akar penyebab kecelakaan/kejadian.
<b>Analisis Skenario</b>	mengembangkan jalan untuk menyelidiki dari teori kausasi dan rantai peristiwa hipotetis
<b>berurutan berjangka waktu plot acara sistem investigasi</b>	Expound diagram terkait, secara berurutan berjangka waktu peristiwa dan hubungan kausal mereka yang menunjukkan bagaimana kecelakaan/kejadian terjadi.
<b>Analisis waktu/Rugi (TLA) untuk respon tanggap darurat</b>	mengevaluasi: (1) efek dari intervensi manusia setelah kecelakaan/kejadian, (2) pengendalian dari kecelakaan/kejadian, dan (3) efektivitas mitigasi tindakan pengendalian ancaman waktu.
<b>Analisis waktu peringatan</b>	menyelidiki Delta antara waktu respons yang tersedia dan aktual (manusia dan otomatis) hingga kecelakaan/insiden dan faktor yang berkontribusi, seperti penundaan yang keliru, tak terduga, atau tidak perlu.

## Peran Investigasi Kecelakaan/kejadian Teknik IA

Teknik Analisis	Aturan Investigasi Kecelakaan/kejadian IA
Jaringan kepercayaan Bayesian	Menyediakan metodologi untuk penalaran tentang ketidakpastian sebagai bagian dari kecelakaan/kejadian penyelidikan.
Analisis penyebab konsekuensi	Mengidentifikasi tindakan pengendalian ancaman yang tidak pantas, tidak efektif, dan hilang; memverifikasi bahwa semua mode kegagalan yang disengaja dan disengaja memiliki ukuran kontrol ancaman yang sesuai.
Analisis Pohon Peristiwa	identifikasi tindakan pengendalian ancaman yang tidak pantas, tidak efektif, dan hilang.
Studi HAZOP	memverifikasi bahwa semua kecelakaan dan disengaja, fisik dan Cyber, bahaya yang terkait dengan operasi dari sistem telah dihilangkan atau dikurangi

# PERAN INVESTIGASI KECELAKAAN/KEJADIAN TEKNIK IA

II. Teknik Analisis	Aturan Investigasi Kecelakaan/kejadian IA
<b>Petri Nets</b>	verifikasi bahwa kondisi kemacetan, ras, dan nondeterministik yang dapat menyebabkan sistem kompromi atau kegagalan tidak ada.
<b>Software, System FMECA</b>	Memeriksa efek kegagalan disengaja dan tidak disengaja, acak dan sistematis pada perilaku sistem secara umum dan IA integritas pada khususnya
<b>Software, system FTA</b>	Mengidentifikasi potensi akar penyebab dari sistem yang tidak diinginkan kejadian (kebetulan dan disengaja) untuk memverifikasi efektivitas mengurangi fitur desain dan prosedur operasional.
<b>Analisis Sirkuit Menyelinap</b>	verifikasi bahwa semua tersembunyi, tidak disengaja, dan perangkat keras dan lunak yang tidak sah jalur Logis atau urutan kontrol yang dapat menghambat fungsi sistem yang diinginkan, memulai peristiwa sistem yang tidak diinginkan, atau menyebabkan kesalahan waktu dan pengurutan telah dihapus.

# PERAN INVESTIGASI KECELAKAAN/KEJADIAN TEKNIK IA

Teknik Verifikasi	Aturan Investigasi Kecelakaan/kejadian IA
<b>Analisis Jalur Kendali</b>	mengungkap struktur logika program yang buruk dan tidak benar yang dapat membahayakan integritas IA.
<b>Analisis Jalur Data dan Informasi</b>	mengungkap transformasi dan operasi data yang tidak benar dan tidak sah yang dapat membahayakan integritas IA.
<b>Meninjau kasus integritas IA</b>	menentukan apakah klaim yang dibuat mengenai integritas IA dibenarkan oleh argumen dan bukti pendukung
<b>Analisa akar penyebab</b>	mengidentifikasi penyebab, peristiwa, kondisi, atau tindakan yang secara individu atau dalam kombinasi menyebabkan kecelakaan/insiden; menentukan mengapa Cacat tidak terdeteksi sebelumnya.

## Exhibit 6 Barrier Analysis Report

Barrier Analysis Report for: \_\_\_\_\_

as of date: \_\_\_\_\_

### I. Existing Defensive Layers

Threat Control Measure	Function	Location <sup>a</sup>	Type <sup>b</sup>	Accident/Incident Status			
				Effective	Partially Effective	Failed	Remarks

### II. New Defensive Layers Needed

Threat Control Measure	Function	Location <sup>a</sup>	Type <sup>b</sup>	Defensive Layer Being Replaced or Reinforced	Rationale

# **MEMULAI MEKANISME PEMULIHAN JANGKA PENDEK**

- setelah kecelakaan/kejadian terjadi, penyebab, tingkat, dan konsekuensi diselidiki. Laporan awal kecelakaan/kejadian memicu segera pemulihan jangka pendek mekanisme
- Laporan tindak lanjut kecelakaan/kejadian lengkap merangsang tindakan perbaikan jangka panjang.

# LANGKAH PEMULIHAN KECELAKAAN/KEJADIAN

- Tinjau hasil investigasi awal tentang penyebab, luasnya, dan konsekuensi dari kecelakaan/kejadian.
- Tentukan apa yang bisa dan tidak dapat dipulihkan dalam jangka pendek:  
( sistem , perangkat lunak sistem , peralatan komunikasi , perangkat lunak aplikasi, Layanan , perangkat keras, data)
- Memastikan ketika setiap sistem, entitas, dan komponen dapat dan harus dipulihkan:  
(pertimbangan teknis, prioritas operasional , prioritas keselamatan dan keamanan )
- Putuskan bagaimana setiap sistem, entitas, dan komponen dapat dan harus dipulihkan:  
(tingkat layanan yang akan dipulihkan ; tindakan, perintah yang diperlukan untuk efek pemulihan; memverifikasi efektivitas upaya pemulihan )
- Beritahu pelanggan, pengguna akhir, administrator sistem, staf pemeliharaan, dll  
(masalah mengalami, tindakan pencegahan darurat, perkiraan waktu pemulihan)

# TINDAKAN DAN PERINTAH PEMULIHAN DAPAT MELIBATKAN HAL BERIKUT:

- Mengaktifkan dingin cadangan atau panas siaga berlebihan perangkat keras
- konfigurasi ulang sistem atau jaringan
- restart, reload, reinitializing sistem atau data dari lokal atau offsite Arsip
- switching operasi ke lokasi terpencil
- beralih ke penyedia layanan alternatif
- memulihkan dan restart aturan kontrol akses, parameter otentikasi dan pengolahan, jejak audit keamanan/alarm, dan tindakan pengendalian ancaman lainnya

# LAPORAN KECELAKAAN/KEJADIAN

pelaporan kecelakaan/kejadian adalah bagian penting dari menyelidiki, menanggapi, dan pulih dari itu.

# ALASAN UNTUK MELAPORKAN KECELAKAAN/KEJADIAN, DI DALAM DAN DI LUAR ORGANISASI, DAN MANFAAT YANG AKAN DIPEROLEH DARI MELAKUKANNYA.

1. kecelakaan/kejadian harus dilaporkan sebelum situasi dapat dikoreksi. Jika kecelakaan/kejadian dilaporkan pada waktu yang tepat, kerusakan/kehilangan yang dialami oleh sistem ini dan lainnya dapat diminimalkan.
2. melaporkan hasil penyelidikan kecelakaan/kejadian dan apa yang dipelajari dari itu mengurangi kemungkinan kekambuhan, dalam dan di antara organisasi.
3. pelanggan dan karyawan akan memiliki lebih percaya diri dalam sebuah organisasi yang melaporkan kecelakaan/kejadian; mereka mendapatkan kesan bahwa organisasi sedang terbuka dan berada di atas situasi. Ini adalah contoh lain dari manajemen persepsi.
4. sebuah organisasi mungkin memiliki tanggung jawab hukum untuk melaporkan kecelakaan/kejadian kepada pemegang saham, pelanggan, publik, atau badan pengatur, tergantung pada sifat organisasi dan yurisdiksi hukum di mana ia tinggal.
5. sebuah kecelakaan/kejadian pasti telah dilaporkan jika tindakan hukum berikutnya harus diambil.

# MENYEBARKAN TINDAKAN REMEDIAL JANGKA PANJANG

- sebuah kecelakaan/kejadian penyelidikan dilakukan untuk menemukan apa yang sebenarnya terjadi, bagaimana hal itu terjadi, dan mengapa hal itu terjadi atau diizinkan terjadi.
- Laporan investigasi kecelakaan/kejadian dianalisis untuk belajar dari apa, bagaimana, dan mengapa kecelakaan/kejadian.
- Alasan yang paling adalah untuk menentukan apa tindakan perbaikan yang diperlukan untuk mencegah kecelakaan yang sama atau serupa dari berulang.

# LAPORAN KECELAKAAN/KEJADIAN: BAGIAN I-DESKRIPSI

No	Kolom Laporan	Laporan Awal	Laporan Tidaklanjut
1	laporan referensi nomor	x	x
2	Klasifikasi anomaly (Lihat Bab 6, pameran 12)	x	x
3	Deskripsi kegagalan/kompromi	x	x
4	Keparahan: a. bencana c. kritis b. marginal d. tidak signifikan	x	x
5	Tanggal/waktu pertama terdeteksi atau berpengalaman	x	x
6	Frekuensi berpengalaman	x	x
7	Durasi	x	x
8	Signifikansi misi:  a. kegagalan fungsi dan entitas IA-kritis (mengutip) b. kegagalan fungsi/entitas yang terkait dengan IA (kutip) c. kegagalan MWFs (mengutip) d. kegagalan MNWFs (Cite) e. Tidak ada pilihan tetapi untuk gagal aman/aman f. Tidak ada pilihan tetapi gagal operasional g. Total hilangnya sistem h. hilangnya data kritis/sensitive i. Jumlah personil yang terkena	x	x

# LAPORAN KECELAKAAN/KEJADIAN: BAGIAN I-DESKRIPSI

No	Kolom Laporan	Laporan Awal	Laporan Tidaklanjut
9	Sistem/entitas utama yang terpengaruh: a. entitas/sistem ID dan asal b. jenis sistem/entitas c. jumlah sistem/entitas yang terpengaruh	x	x
10	waktu operasi sebelum kecelakaan/kejadian	x	x
11	Sistem lain/entitas di dalam dan di luar organisasi yang mungkin berdampak	x	x
12	Konfigurasi sistem, nomor versi, dll	x	x
13	Konfigurasi jaringan, nomor versi, dll	x	x
14	Asumsi	x	x

# LAPORAN KECELAKAAN/KEJADIAN : BAGIAN II-PENILAIAN

- Penilaian Kecelakaan /kejadian

No	Kolom Laporan	Laporan Awal	Laporan Tidaklanjut
1	kondisi yang menghasilkan kecelakaan/kejadian	?	x
2	Urutan peristiwa kritis		x
3	near-misse yang terkait		x
4	Konsekuensi		
	a. kemungkinan	x	
	b. aktual		x
5	Tindakan korektif diambil		
	a. sistem otomatis	x	x
	b. manusia yang diinisiasi	x	x
6	Investigasi teknik yang digunakan.		x
	a. Analisis Barrier		
	b. Wawancara insiden kritis		
	c. Analisis efek modus kerusakan		
	d. charting peristiwa dan faktor kausal		
	e. analisis skenario		
	f. STEP Investigasi system		
	g. TLA untuk tanggap darurat		
	h. Analisis waktu peringatan		
	i. Lain		

No	Kolom Laporan	Laporan Awal	Laporan Tidaklanjut
7	Hasil investigasi: termasuk laporan, diagram, grafik, dll		x
8	Intermediate dan akar penyebab <ul style="list-style-type: none"> <li>a. Desain galat</li> <li>b. implementasi galat</li> <li>c. operasional prosedur galat</li> <li>d. rencana kontinjenensi galat</li> <li>e. praktik keamanan fisik galat</li> <li>f. tindakan manusia yang tidak disengaja</li> <li>g. tindakan manusia yang disengaja</li> <li>h. tidak sengaja operasi</li> <li>i. kegagalan atau tidak tersedianya sistem infrastruktur kunci</li> <li>j. Lain</li> </ul>		x
9	Sisa masa manfaat sistem		x
10	Perkiraan kerugian/kerusakan		x
11	Rekomendasi untuk pemulihan jangka pendek	?	x
12	Pengamatan/pelajaran yang dipelajari untuk tindakan perbaikan jangka panjang		x

# PELAJARAN DARI ANALISIS LAPORAN KECELAKAAN/KEJADIAN, YANG KEMUDIAN DAPAT DIKERAHKAN SEBAGAI LANGKAH PERBAIKAN:

- Penemuan strategi pencegahan baru, alat, dan teknik
- identifikasi kerentanan baru dan ancaman
- menunjukkan efektivitas tindakan pengendalian ancaman
- menunjukkan efektivitas kegiatan verifikasi
- meningkatkan prosedur operasional, rencana kontinjensi, dan praktik keamanan fisik
- kebutuhan untuk perubahan desain

# EVALUASI MASALAH HUKUM

Beberapa definisi hukum yang terlibat dalam informasi keamanan/IA :

- **Cacat:** defisiensi; ketidaksempurnaan insufisiensi ketiadaan sesuatu yang diperlukan untuk kelengkapan atau kesempurnaan; kekurangan dalam sesuatu yang penting untuk penggunaan yang tepat untuk tujuan yang suatu hal yang akan digunakan; Cacat manufaktur, Cacat Desain, atau peringatan yang tidak memadai. Sebuah cacat desain ada setiap kali desain itu sendiri menimbulkan bahaya yang tidak masuk akal untuk konsumen.
- **Kerusakan:** kehilangan, cedera, atau kemerosotan, disebabkan oleh kelalaian, Desain, atau kecelakaan dari satu orang ke yang lain, sehubungan dengan orang atau properti terakhir; membahayakan, merugikan, atau kehilangan yang diderita karena cedera.
- **Cedera:** setiap kesalahan atau kerusakan yang dilakukan pada orang lain, baik pribadi, hak, reputasi, atau properti; untuk menyerang kepentingan yang dilindungi secara hukum dari pihak lain.

- **Kelalaian:** kegagalan untuk menggunakan perawatan seperti itu sebagai orang yang cukup bijaksana dan berhati-hati akan menggunakan dalam keadaan yang sama; melakukan beberapa tindakan yang seseorang dari kehati-hatian biasa tidak akan dilakukan di bawah keadaan yang sama atau kegagalan untuk melakukan apa yang orang biasa kehati-hatian akan dilakukan di bawah keadaan yang sama; yang berada di bawah norma perlindungan orang lain terhadap risiko bahaya yang tidak masuk akal. Hal ini ditandai dengan tidak sengaja, ketidakberdayaan, kurangnya perhatian, sembronoan,...
- **Kewajiban:** kondisi menjadi atau berpotensi tunduk pada suatu kewajiban; kondisi bertanggung jawab atas kemungkinan kerugian atau aktual, penalti, kejahatan, beban, atau beban; kondisi yang menciptakan suatu kewajiban untuk melakukan suatu tindakan segera atau di masa depan; termasuk hampir setiap karakter bahaya atau tanggung jawab, mutlak, kontingen, atau mungkin.
- **Asumsi risiko:** seorang penggugat mungkin tidak pulih untuk cedera yang ia assents, yaitu, bahwa seseorang mungkin tidak pulih untuk cedera yang diterima ketika ia secara sukarela mengekspos dirinya untuk yang dikenal dan dihargai bahaya. Persyaratan untuk pertahanan... adalah bahwa:
  1. penggugat memiliki pengetahuan tentang fakta yang merupakan kondisi yang berbahaya,
  2. ia tahu bahwa kondisi ini berbahaya,
  3. ia menghargai sifat atau tingkat bahaya, dan
  4. dia secara sukarela mengekspos dirinya untuk bahaya.



# PEMANGKU KEPENTINGAN HARUS MENYADARI DAN HIDUP SAMPAI TANGGUNG JAWAB HUKUM INI

- **Designer:** sistem perancang/pengembang bertanggung jawab untuk memastikan bahwa sistem akan gagal aman/aman atau gagal operasional, yang sesuai, dalam semua situasi sehingga tidak ada kerusakan atau kerugian yang ditimbulkan.
- **Para ahli Teknis:** ahli teknis, Apakah karyawan atau konsultan, bertanggung jawab untuk menjaga lengkap, mendalam, dan saat ini kompetensi dalam bidang mereka, sehingga kompetensi ini di atas rata, tetapi belum tentu pada tingkat jenius.
- **Pemasok komponen:** pemasok komponen, seperti vendor COTS, bertanggung jawab untuk mewakili kemampuan komponen, keterbatasan, klaim, pelabelan, dan petunjuk penggunaan
- **Lab pengujian dan sertifikasi:** Lab pengujian dan sertifikasi bertanggung jawab untuk menjelaskan secara akurat apa yang telah dan tidak diuji atau dievaluasi, memberikan hasil pengujian yang akurat, deskripsi yang akurat tentang cakupan pengujian, dan klaim keandalan, keselamatan, dan keamanan yang dapat dipertahankan. Laboratorium Uji dan sertifikasi bertanggung jawab untuk mempekerjakan orang yang kompeten dalam melakukan tes/evaluasi dan memverifikasi bahwa fakta, pendapat, dan asumsi dipisahkan.

# RINGKASAN

- komponen kelima dari informasi yang efektif keamanan/IA program melakukan kecelakaan/kejadian penyelidikan. Lima kegiatan dilakukan saat melakukan penyelidikan kecelakaan/kejadian :
  - Penyebab, luasnya, dan konsekuensi dari kegagalan/kompromi dianalisis.
  - Mekanisme pemulihan dimulai.
  - Kecelakaan/kejadian ini dilaporkan.
  - Tindakan Remedial disebarluaskan.
  - Masalah hukum dievaluasi.

TERIMA KASIH