- **Pengukuran Teknologi Informasi dengan Octave Allegro**

- Program Magister – Teknologi Informasi

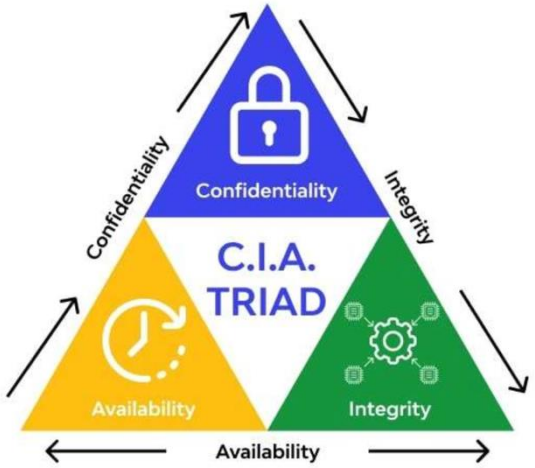
Dosen: Prof.Dr. Muhammad Said Hasibuan

Mata Kuliah: IT Risk Management

CIA

- **Kerahasiaan (Confidentiality):**

Tujuannya adalah untuk mencegah akses tidak sah ke informasi sensitif.



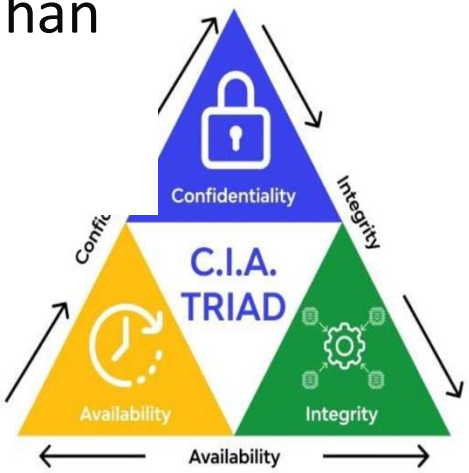
Mekanisme Perlindungan:

- **Enkripsi:** Mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang tepat.
- **Kontrol akses:** Membatasi akses ke sistem dan data berdasarkan peran dan kebutuhan pengguna.
- **Otentikasi:** Memastikan identitas pengguna sebelum memberikan akses.
- **Autentikasi:** Memastikan bahwa data yang diterima adalah asli dan belum diubah.

CIA

Integritas (Integrity):

- Menjaga keakuratan, kelengkapan, dan konsistensi data.
- Memastikan data tidak dimodifikasi atau dihapus secara tidak sengaja atau tidak sah.
- Contohnya termasuk menggunakan checksum untuk mendeteksi perubahan data dan backup rutin untuk pemulihan.



Integritas (Integrity):

- **Hash function:** Menghasilkan nilai hash unik yang mewakili suatu data. Jika data diubah, nilai hash-nya juga akan berubah.
- ***Digital signature:*** Menggunakan kriptografi untuk memverifikasi keaslian dan integritas suatu pesan.
- **Kontrol versi:** Melacak perubahan pada data dan memungkinkan pemulihan ke versi sebelumnya jika terjadi kesalahan.

CIA

- **Ketersediaan (Availability):**
  - Memastikan pengguna yang berwenang dapat mengakses data dan sistem saat dibutuhkan.
  - Contoh ancaman terhadap ketersediaan adalah serangan Denial of Service (DoS) atau Distributed Denial of Service (DDoS) yang membuat sistem tidak dapat diakses.
  - Strategi untuk memastikan ketersediaan meliputi disaster recovery dan backup.

OCTAVE

Mahasiswa mampu:

- Memahami konsep dasar *IT risk assessment* dan *measurement framework*.
- Mengenali prinsip dan langkah kerja **OCTAVE Allegro**.
- Melakukan identifikasi aset informasi dan ancaman.
- Menggunakan *template* pengukuran risiko TI berbasis OCTAVE Allegro.
- Menginterpretasikan hasil untuk mendukung keputusan tata kelola TI.

Konsep Dasar Pengukuran IT

•Pengukuran IT adalah proses menilai **kapabilitas, risiko, dan kinerja sistem TI** berdasarkan indikator terukur.

Tujuan utama:

•Mendukung *IT governance decision-making*

•Mengontrol biaya dan risiko

•Menjamin kesesuaian dengan standar seperti COBIT, ISO 27005

•Dimensi utama pengukuran:

•**Efektivitas**

•**Efisiensi**

•**Kepatuhan**

•**Keamanan Informasi**

Pengenalan OCTAVE Framework

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
  dikembangkan oleh **SEI – Carnegie Mellon University**
  Versi:
- OCTAVE Classic
- OCTAVE-S
- **OCTAVE Allegro (versi ringan & terstruktur)**
- Fokus utama Allegro:
- *Identifikasi dan mitigasi risiko informasi berdasarkan konteks organisasi, bukan teknologi semata.*

Pengenalan OCTAVE Framework

- **Asset Identification**
→ Menentukan aset informasi kritis.
- **Threat Profiling**
→ Menilai potensi ancaman terhadap aset.
- **Impact Evaluation**
→ Menganalisis dampak dari risiko.
- **Risk Mitigation Strategy**
→ Menentukan prioritas tindakan mitigasi

Octave alegro

- Membangun konteks risiko organisasi
- Mengidentifikasi aset informasi
- Menentukan konteks aset
- Mengidentifikasi ancaman aset
- Menilai dampak ancaman
- Menganalisis risiko
- Menentukan strategi mitigasi
- Menyusun profil risiko organisasi
- 💡 *Catatan:* Setiap langkah dapat didokumentasikan dalam *Octave Allegro Worksheet*.

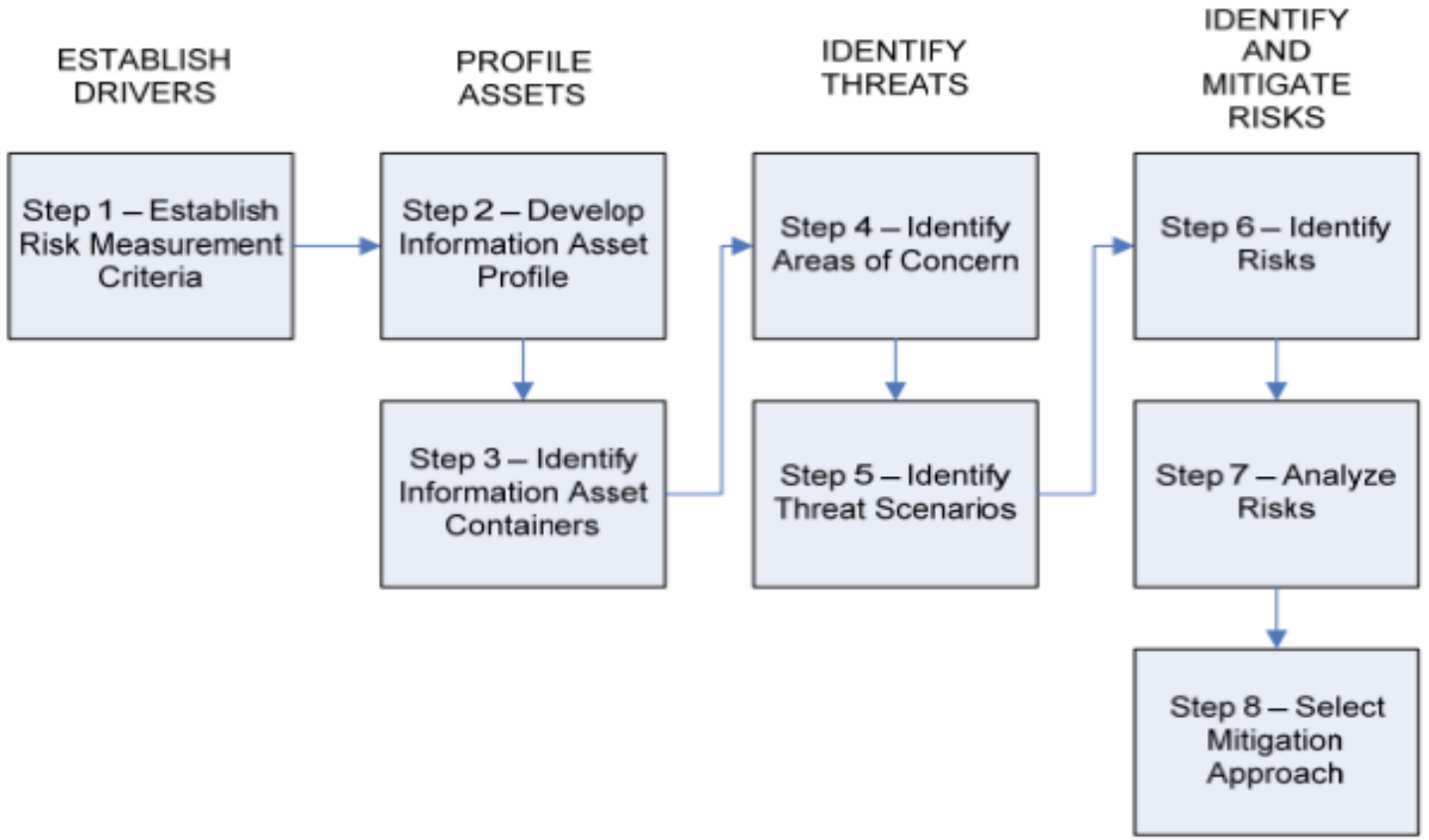
Contoh Pengukuran

Tahap	Kegiatan	Output
1	Identifikasi aset informasi	Daftar aset & nilai kritikal
2	Identifikasi ancaman	Daftar ancaman per aset
3	Analisis dampak	Matriks dampak-risiko
4	Mitigasi risiko	Rencana tindakan prioritas

Contoh Kasus

- Sistem Akademik Universitas
- Aset: Database Mahasiswa
- Ancaman: Kebocoran data, serangan SQL Injection
- Dampak: Reputasi, pelanggaran privasi, hukum
- Mitigasi: Enkripsi data, audit keamanan, pelatihan staf
- → Gunakan *Octave Allegro Template* untuk memetakan ancaman dan dampak.

OCTAVE


ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Rincian Tahapan Metode OCTAVE Allegro

Kategori 1, menetapkan apa yang menjadi arahan organisasi.

Kategori 2, membuat profil aset yang dimiliki organisasi.

Kategori 3, mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadahnya.

Kategori 4, mengidentifikasi dan mitigasi risiko terhadap aset informasi dan pengembangan pendekatan mitigasi.

Rincian Tahapan Metode OCTAVE Allegro

Tahap	Aktivitas	Output	*Worksheet* /Acuan
1	Menetapkan kriteria pengukuran risiko	• Kriteria pengukuran risiko terhadap arahan organisasi • Peringkat area dampak dari yang paling penting hingga yang tidak penting	*Allegro Worksheet* 1-6 dan 7
2	Mengembangkan profil aset informasi	Profil aset informasi kritis	*Allegro Worksheet* 8

3	Mengidentifikasi *container* aset informasi	Pemetaan lingkungan risiko aset informasi	*Worksheets* 9a, 9b, dan 9c
4	Mengidentifikasi *area of concern*	Peta lingkungan risiko aset informasi	*Worksheet* 10
5	Mengidentifikasi skenario ancaman	• Informasi detail dan hasil pengembangan skenario ancaman dari *area of concern* • Daftar risiko aset informasi • Deskripsi tambahan untuk kolom 6 *worksheet*s aset informasi dan *container*	• Output tahap 4 (*Information Aset Risk Environment Maps*) • *Worksheet* 10 • *Information Aset Risk Worksheets* • *Column (6) worksheets* aset informasi dan *container*
6	Mengidentifikasi risiko	Konsekuensi dari skenario ancaman (kondisi) Tahap 6 Risiko Total = Ancaman kondisi dan konsekuensi di tahap [4 + 5] + [6]	*Information Aset Risk Worksheet*
7	Menganalisis risiko	• Tabel nilai area dampak • Tabel skor risiko	• *Risk Measurement Criteria Step 1* • *Information Aset Risk Worksheets 10*
8	Memilih pendekatan mitigasi	• Matriks risiko relatif • Tingkat kerawanan informasi • Mitigasi untuk semua daftar risiko • Strategi mitigasi untuk setiap risiko yang telah diputuskan untuk dilakukan mitigasi	

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Tabel 1 Identifikasi Nilai Dampak

Are Dampak	Prioritas	Nilai Dampak		
		Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi dan Kepercayaan Pengguna	1	5	10	15
Keuangan	2	4	8	12
Produktifitas	3	3	6	9
Keselamatan dan Kesehatan Pegawai	4	2	4	6
Tuntutan Hukum	5	1	2	3

Allegro Worksheet 2	Risk Measurement Criteria – Financial		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than _____% in yearly operating costs	Yearly operating costs increase by _____to _____%.	Yearly operating costs increase by more than _____%.
Revenue Loss	Less than _____% yearly revenue loss	_____to _____% yearly revenue loss	Greater than _____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $_____	One-time financial cost of $_____ to $_____	One-time financial cost greater than $_____
Other:			

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than _____% for _____to _____ day(s).	Staff work hours are increased between _____% and _____% for _____to _____ day(s).	Staff work hours are increased by greater than _____% for _____to _____ day(s).
Other:			

Allegro Worksheet 4	Risk Measurement Criteria – Safety and Health		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

Allegro Worksheet 4	Risk Measurement Criteria – Safety and Health		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

Allegro Worksheet 5	Risk Measurement Criteria – Fines and Legal Penalties		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $_____ are levied.	Fines between $_____ and $_____ are levied.	Fines greater than $_____ are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $_____ and $_____ are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Allegro Worksheet 5	Risk Measurement Criteria – Fines and Legal Penalties		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $_____ are levied.	Fines between $_____ and $_____ are levied.	Fines greater than $_____ are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $_____ and $_____ are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
	Reputation and Customer Confidence
	Financial
	Productivity
	Safety and Health
	Fines and Legal Penalties
	User Defined

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
(4) Owner(s) *Who owns this information asset?*		

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1.	
2.	
3.	

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1.	
2.	
3.	
4.	
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	ORGANIZATION
1.	
2.	

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk — Threat	Information Asset			
	Area of Concern			
	(1) Actor *Who would exploit the area of concern or threat?*			
	(2) Means *How would the actor do it? What would they do?*			
	(3) Motive *What is the actor's reason for doing it?*			
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ Disclosure ❑ Modification	❑ Destruction ❑ Interruption	
	(5) Security Requirements *How would the information asset's security requirements be breached?*			
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High	❑ Medium	❑ Low
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
		Reputation & Customer Confidence		
		Financial		
		Productivity		
		Safety & Health		

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		

Terima Kasih