



Fakultas Ilmu Komputer

Penilaian Resiko IT

Assoc.Prof. Dr. Muhammad Said Hasibuan, S.Kom., M.Kom
Fakultas Ilmu Komputer IIB Darmajaya
2025



Penilaian Resiko IT

- **Definisi Penilaian Risiko**

- Proses identifikasi, analisis, dan evaluasi risiko yang dapat mempengaruhi penggunaan teknologi informasi dalam organisasi.

- **Pentingnya Penilaian Risiko**

- Melindungi aset informasi.
- Memastikan kontinuitas operasional.



Komponen Utama Penilaian Risiko

1. Identifikasi Risiko

1. Mengidentifikasi potensi ancaman dan kerentanan.
2. Contoh: Serangan siber, kesalahan manusia, bencana alam.

2. Analisis Risiko

1. Menilai kemungkinan dan dampak dari setiap risiko.
2. Contoh: Menggunakan skala 1-5 untuk menilai dampak.

3. Evaluasi Risiko

1. Menentukan tingkat risiko dan prioritas penanganan.
2. Contoh: Menggunakan matriks risiko untuk memprioritaskan tindakan.



Metodologi Penilaian Risiko

- **Metode Kualitatif**

- Menggunakan wawancara dan diskusi kelompok untuk mengidentifikasi risiko.

- **Metode Kuantitatif**

- Menggunakan data statistik dan model matematis untuk mengukur risiko.



Contoh Metodologi

- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- **INDEKS KAMI** (Keamanan Informasi)
- **FAIR** (Factor Analysis of Information Risk)
- **NIST Risk Management Framework**
- **ISO/IEC 27005** (Standar Manajemen Risiko Keamanan Informasi)
- **COBIT** (Control Objectives for Information and Related Technologies)



Study Kasus

- **Perusahaan Teknologi**
 - Menghadapi risiko serangan siber yang dapat mengakibatkan kebocoran data pelanggan.
- **Langkah Penilaian:**
 - Identifikasi: Serangan phishing, malware.
 - Analisis: Dampak finansial dan reputasi.
 - Evaluasi: Prioritaskan mitigasi serangan phishing.



Manfaat Penilaian Resiko

- **Perlindungan Aset Informasi**
 - Mengurangi kemungkinan kehilangan data penting.
- **Perencanaan Kontinjensi**
 - Mempersiapkan langkah-langkah untuk mengatasi insiden.
- **Kepatuhan Regulasi**
 - Memastikan kepatuhan terhadap peraturan dan standar industri.



Tantangan Penilaian Resiko

- **Perubahan Teknologi**
 - Risiko baru muncul seiring dengan kemajuan teknologi.
- **Sumber Daya Terbatas**
 - Keterbatasan waktu dan anggaran untuk melakukan penilaian menyeluruh.
- **Kesadaran Karyawan**
 - Pentingnya pelatihan untuk meningkatkan kesadaran akan risiko.



Kesimpulan

- Penilaian risiko teknologi informasi adalah langkah krusial dalam melindungi organisasi dari ancaman.
- Proses ini harus dilakukan secara berkala untuk menyesuaikan dengan perkembangan teknologi dan ancaman baru.



Diskusi

- **Pertanyaan untuk Diskusi:**

- Apa tantangan terbesar yang Anda hadapi dalam penilaian risiko di organisasi Anda?
- Bagaimana Anda mengintegrasikan hasil penilaian risiko dalam strategi bisnis?



Fakultas Ilmu Komputer

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Metode OCTAVE melakukan penilaian risiko berdasarkan pada tiga prinsip dasar :

1. Confidentiality (Kerahasiaan)
2. Integrity
3. Availability.



Fakultas Ilmu Komputer

OCTAVE method

- OCTAVE method
- OCTAVE-S, dan
- OCTAVE Allegro.



OCTAVE method

- Metode OCTAVE merupakan versi OCTAVE yang pertama kali dikembangkan.
- Metode OCTAVE dilakukan dengan cara diadakannya rangkaian workshop dan difasilitasi oleh tim analisis yang dibuat dari unit bisnis yang ada didalam perusahaan dan departemen IT.
- Metode OCTAVE ditujukan untuk perusahaan besar yang memiliki lebih dari 300 orang staf.



Varian OCTAVE - S

- Pengembangan OCTAVE-S didukung oleh program Technology Insertion, Demonstration, and Evaluation (TIDE) pada SEI (Software Engineering Institute), yang bertujuan untuk membawa pendekatan OCTAVE pada perusahaan kecil.
- Versi terkini dari OCTAVE-S (versi 1.0) dirancang secara spesifik untuk perusahaan yang memiliki 100 staf atau kurang.



Varian OCTAVE Allegro

- Tujuan yang ingin dicapai oleh OCTAVE Allegro adalah penilaian yang luas terhadap lingkungan risiko operasional suatu organisasi dengan tujuan menghasilkan hasil yang lebih baik tanpa perlu pengetahuan yang luas dalam hal penilaian risiko.
- Pendekatan ini berbeda dari pendekatan OCTAVE, dimana OCTAVE Allegro lebih berfokus terhadap aset informasi dalam konteks bagaimana mereka digunakan, dimana mereka disimpan, dipindahkan, dan diolah, dan bagaimana mereka terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan.



Fakultas Ilmu Komputer

OCTAVE

Kata allegro: (al-leg-ro) berarti dalam tempo yang cepat dan lincah. Hal ini menggambarkan kinerja OCTAVE Allegro yang lincah dan cepat.

Keating (2014)

menyatakan metode penilaian risiko OCTAVE Allegro dibuat oleh Carnegie Mellon University Software Engineering Institute (SEI)



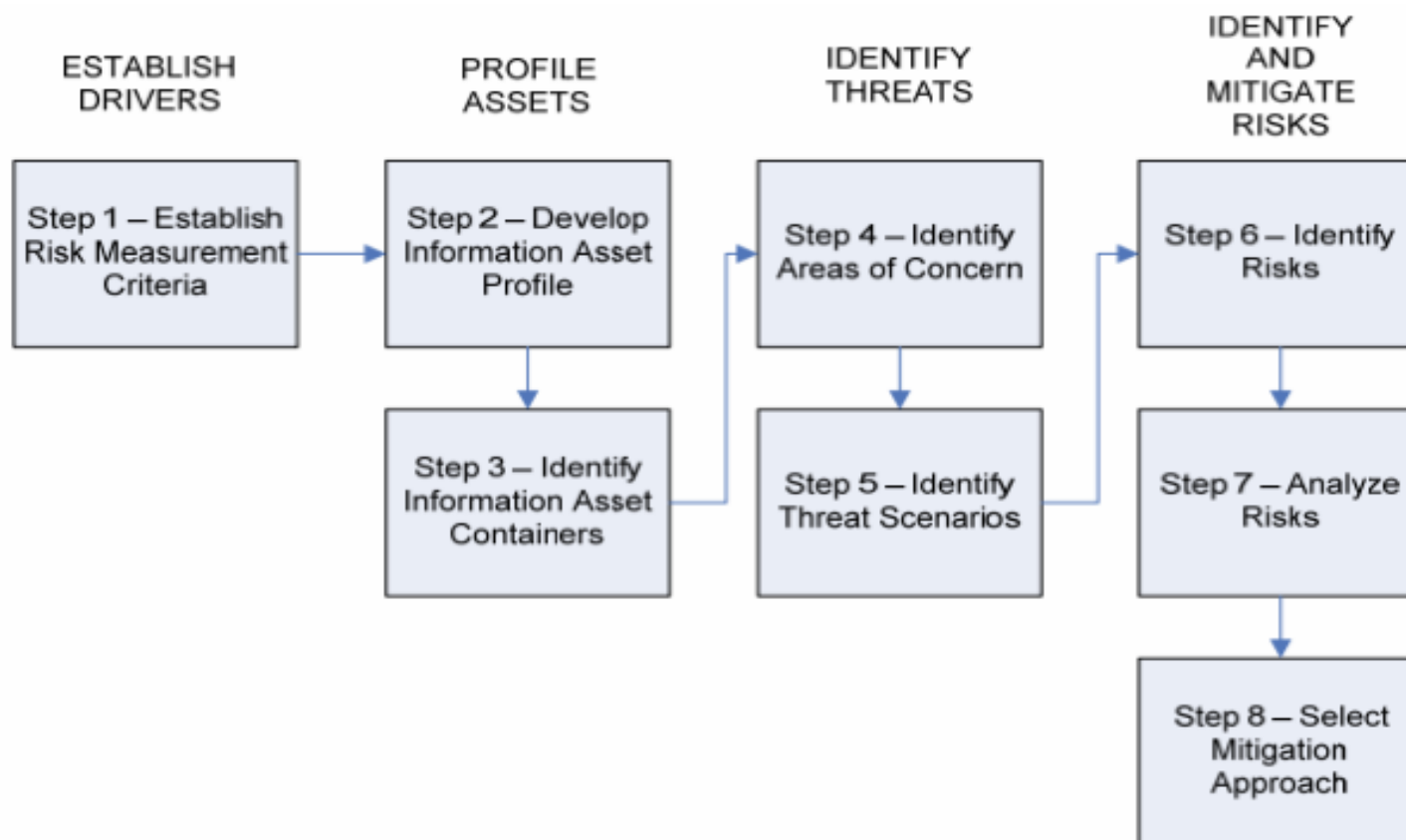
Fakultas Ilmu Komputer

OCTAVE

OCTAVE Allegro dapat dilaku-kan dalam bentuk workshop, settingbersama yang didukung dengan panduan, lembar kerja, dan kuesioner, yang terdapat dalam lampiran OCTAVE Allegro.



OCTAVE





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	<ul style="list-style-type: none">• Kriteria pengukuran risiko terhadap arahan organisasi• Peringkat area dampak dari yang paling penting hingga yang tidak penting	<i>Allegro Worksheet 1-6 dan 7</i>
2	Mengembangkan profil aset informasi	Profil aset informasi kritis	<i>Allegro Worksheet 8</i>



Fakultas Ilmu Komputer

3	Mengidentifikasi <i>container</i> aset informasi	Pemetaan lingkungan risiko aset informasi	<i>Worksheets 9a, 9b, dan 9c</i>
4	Mengidentifikasi <i>area of concern</i>	Peta lingkungan risiko aset informasi	<i>Worksheet 10</i>
5	Mengidentifikasi skenario ancaman	<ul style="list-style-type: none"> • Informasi detail dan hasil pengembangan skenario ancaman dari <i>area of concern</i> • Daftar risiko aset informasi • Deskripsi tambahan untuk kolom 6 <i>worksheets</i> aset informasi dan <i>container</i> 	<ul style="list-style-type: none"> • Output tahap 4 (<i>Information Aset Risk Environment Maps</i>) • <i>Worksheet 10</i> • <i>Information Aset Risk Worksheets</i> • <i>Column (6) worksheets</i> aset informasi dan <i>container</i>
6	Mengidentifikasi risiko	<p>Konsekuensi dari skenario ancaman (kondisi) Tahap 6</p> <p>Risiko Total = Ancaman kondisi dan konsekuensi di tahap [4 + 5] + [6]</p>	<i>Information Aset Risk Worksheet</i>
7	Menganalisis risiko	<ul style="list-style-type: none"> • Tabel nilai area dampak • Tabel skor risiko 	<ul style="list-style-type: none"> • <i>Risk Measurement Criteria Step 1</i> • <i>Information Aset Risk Worksheets 10</i>
8	Memilih pendekatan mitigasi	<ul style="list-style-type: none"> • 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
<i>Reputation</i>	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.
<i>Customer Loss</i>	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
<i>Other:</i>			

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



Fakultas Ilmu Komputer

Allegrо Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	Low	Moderate	High
<i>Operating Costs</i>	Increase of less than _____% in yearly operating costs	Yearly operating costs increase by _____ to _____%.	Yearly operating costs increase by more than _____%.
<i>Revenue Loss</i>	Less than _____% yearly revenue loss	_____ to _____% yearly revenue loss	Greater than _____% yearly revenue loss
<i>One-Time Financial Loss</i>	One-time financial cost of less than \$ _____	One-time financial cost of \$ _____ to \$ _____	One-time financial cost greater than \$ _____
<i>Other:</i>			



Fakultas Ilmu Komputer

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	Low	Moderate	High
<i>Staff Hours</i>	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).
<i>Other:</i>			



Fakultas Ilmu Komputer

Allegrо Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	Low	Moderate	High
<i>Life</i>	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
<i>Health</i>	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
<i>Safety</i>	Safety questioned	Safety affected	Safety violated



Fakultas Ilmu Komputer

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	Low	Moderate	High
<i>Life</i>	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
<i>Health</i>	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
<i>Safety</i>	Safety questioned	Safety affected	Safety violated



Fakultas Ilmu Komputer

Allegro Worksheet 5		RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	Low	Moderate	High	
<i>Fines</i>	Fines less than \$ _____ are levied.	Fines between \$ _____ and \$ _____ are levied.	Fines greater than \$ _____ are levied.	
<i>Lawsuits</i>	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.	
<i>Investigations</i>	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.	



Fakultas Ilmu Komputer

Allegro Worksheet 5		RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	Low	Moderate	High	
<i>Fines</i>	Fines less than \$ _____ are levied.	Fines between \$ _____ and \$ _____ are levied.	Fines greater than \$ _____ are levied.	
<i>Lawsuits</i>	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.	
<i>Investigations</i>	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.	



Fakultas Ilmu Komputer

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



Fakultas Ilmu Komputer

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



Fakultas Ilmu Komputer

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



Fakultas Ilmu Komputer

(5) Security Requirements			
<i>What are the security requirements for this information asset?</i>			
<input type="checkbox"/> Confidentiality	Only authorized personnel can view this information asset, as follows:		
<input type="checkbox"/> Integrity	Only authorized personnel can modify this information asset, as follows:		
<input type="checkbox"/> 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.		
<input type="checkbox"/> Other	This asset has special regulatory compliance protection requirements, as follows:		
(6) Most Important Security Requirement			
<i>What is the most important security requirement for this information asset?</i>			
<input type="checkbox"/> Confidentiality	<input type="checkbox"/> Integrity	<input type="checkbox"/> Availability	<input type="checkbox"/> Other



Fakultas Ilmu Komputer

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.			



Fakultas Ilmu Komputer

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.			



Fakultas Ilmu Komputer

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.			



Fakultas Ilmu Komputer

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



Fakultas Ilmu Komputer

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



Fakultas Ilmu Komputer

Terima Kasih