DASAR AUDIT

Pertemuan 2

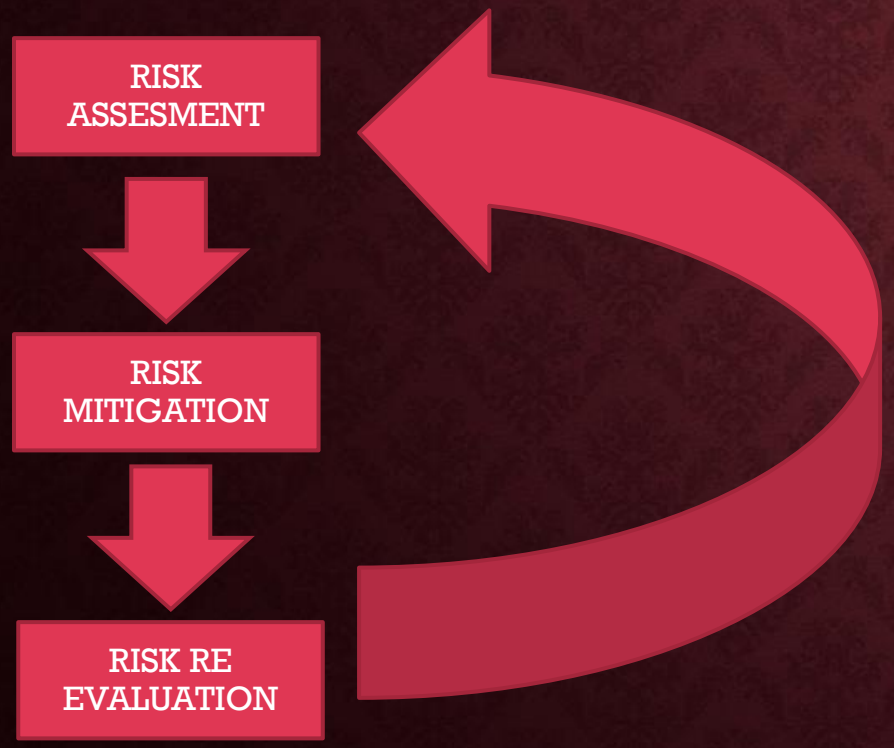
Pitrasacha Adytia, S.T., M.T.

STMIK WICIDA

THREATS DUE TO CYBERCRIME

1. **Embezzlement,** It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose
2. **Fraud,** It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value
3. **Threat of proprietary information,** *:* It is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted, material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
4. **Denial Of Services,** An action or series of actions that prevents access to a software system by its intended/authorized users or causes the delay of its time- critical operations or prevents any part of the system from functioning is termed as ‘DoS’

RISK MANAGEMENT PROCESS



- *Risk management is the process of identifying vulnerabilities and threats to the information* resources used by an organization in achieving business objectives and deciding what countermeasures (safeguards and controls), if any, to take in reducing risk to an acceptable level (i.e. residual risk), based on the value of the information resource/s to the organization
- Step
  - RISK ASSESMENT
  - RISK MITIGATION
  - RISK RE-EVALUATION

RISK ASSESMENT

- *Risk assessment is a step in the risk management procedure*
- *Risk assessment is the determination of quantitative or qualitative value of the risk related to a concrete situation and a recognized threat*
- *Identification of threats and vulnerabilities in the system*
- *Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat;*
- *The identification and analysis of security controls for the information system.*

RISK ASSESMENT

- Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster

1. Define Impact
2. Define Probability Having Risk
3. Risk Matrix
4. Rate The Risk

RISK ASSESSMENT 1 : DEFINE IMPACT

Maginuted Of Impact	Impact Definition
High	may result in the highly costly loss of major tangible assets or resources
	may significantly violate, harm, or impede an organization's mission, reputation, or interest;
	may result in human death or serious injury.
Medium	may result in the costly loss of tangible assets or resources
	may violate, harm, or impede an organization's mission, reputation, or interest;
	may result in human injury.
Low	may result in the loss of some tangible assets or resources
	may noticeably affect an organization's mission, reputation, or interest.

Impact	Definition	
5 **Major**	People	Multiple Fatalities or Permanent Disability
	Asset	Extensive Damage
	Operation	Critical Failure Preventing core Activities from being performed
	Environment	Massive and long term impact
4 **Serious**	People	Single Fatality or permanent Total Disablity
	Asset	Serious and Major Damage
	Operation	Breakdown of key activities leading to reduction performance
	Environment	Major and mid term impact
3 **Moderate**	People	Major Injury / Health Effects
	Asset	Local Damage
	Operation	Target are not met leading to reduction performances
	Environment	Moderate and controllable impact

Impact	Definition	
2 **Minor**	People	Multiple Fatalities or Permanent Disability
	Asset	Extensive Damage
	Operation	Critical Failure Preventing core Activities from being performed
	Environment	Massive and long term impact
1 **Negligible**	People	Single Fatality or permanent Total Disablity
	Asset	Serious and Major Damage
	Operation	Breakdown of key activities leading to reduction performance
	Environment	Major and mid term impact

RISK ASSESSMENT 2 DEFINE PROBABILITY HAVING RISK

Probability	Definition
5. Probable	The event is expected to occur
4. Likely	The event will probably occur
3. Possible	The event might occur at some time
2. Unlikely	The event could occur at some time but is improbable
1. Very Unlikely	The event could have little or no chance of occurance

RISK ASSEMENT 3 RISK MATRIX

		IMPACT				
		1. Negligible	2. Minor	3. Moderate	4. Serious	5. Major
Probability	**5. Probable**	**1**	**2**	**3**	**4**	**5**
	4. Likely	**2**	**4**	**6**	**8**	**10**
	3. Possible	**3**	**5**	**9**	**12**	**15**
	2. Unlikely	**4**	**8**	**12**	**16**	**20**
	1. Very Unlikely	**5**	**10**	**15**	**20**	**25**

RISK ASSESSMENT 4 RATE THE RISK

		IMPACT				
		1. Negligible	2. Minor	3. Moderate	4. Serious	5. Major
Probability	**5. Probable**	**1**	**2**	**3**	**4**	**5**
	4. Likely	**2**	**4**	**6**	**8**	**10**
	3. Possible	**3**	**5**	**9**	**12**	**15**
	2. Unlikely	**4**	**8**	**12**	**16**	**20**
	1. Very Unlikely	**5**	**10**	**15**	**20**	**25**

1-6 : Low	Minor issue of little concern with some small disruptions
7-14: Medium	Requires attention, inconvenience and risk occur
15-25 : High	Requires urgent attention , introduce control to reduce risk

RISK MITIGATION

- Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the **appropriate risk-reducing controls** recommended from the risk assessment process.
- Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the **least-cost approach** and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission

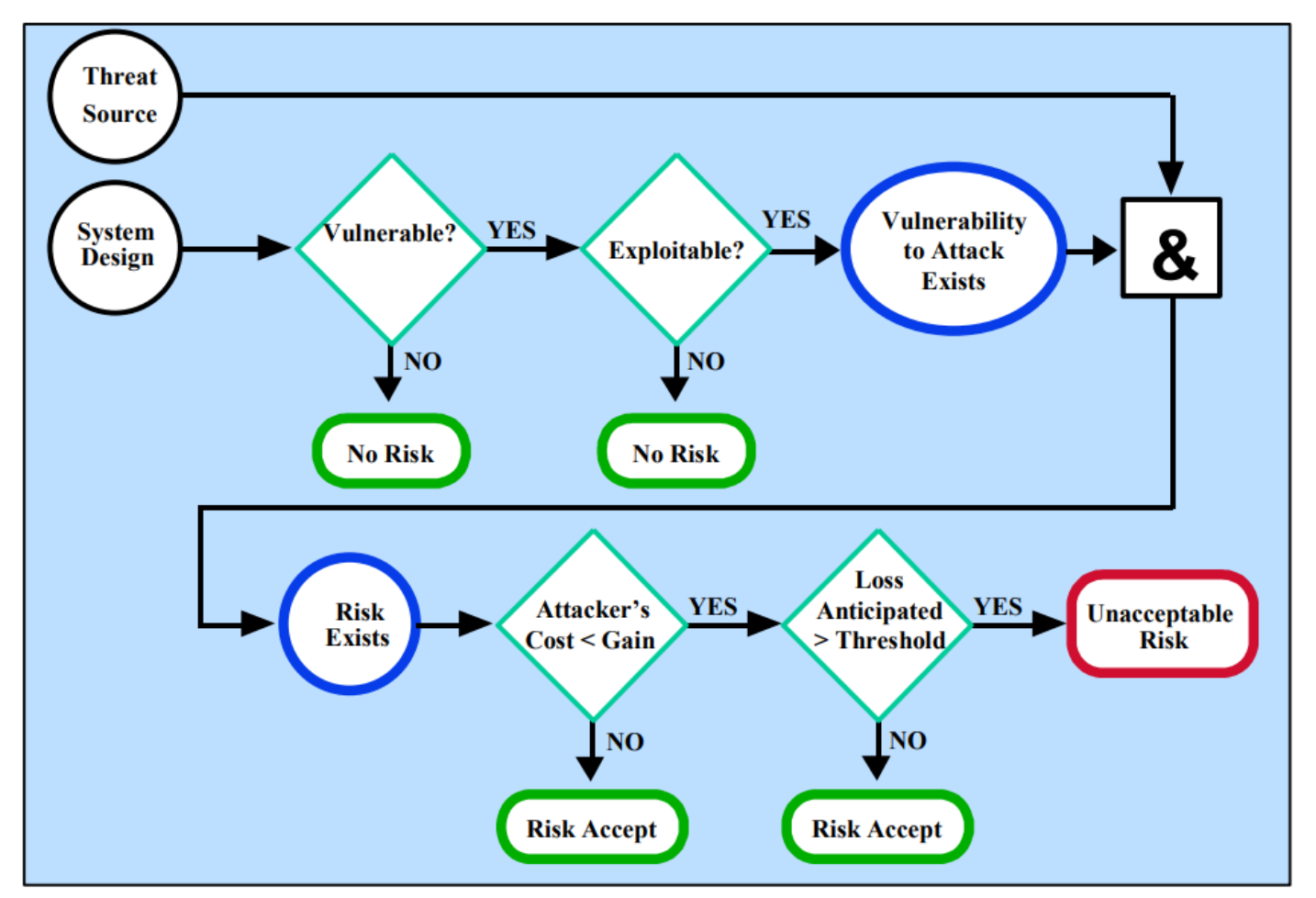
RISK MITIGATION

RISK	CONTROL
0%	X Eliminate risk is impossible
40%	Username + Password + Firewall + Encryption + Biometrics
50%	Username + Password + Firewall + Encryption
60%	Username + Password + Firewall
80%	Username + Password
100%	-

RISK MITIGATION OPTION

- Risk assumption
- Risk avoidance
- Risk limitation
- Risk planning
- Research and Acknowledge
- Risk Transference

RISK MITIGATION STRATEGY



RISK RE EVALUATION

- Time Driven
  - 6 months or 1 Year
- Event Driven
  - Environment Change
- Environment Change
  - Something change within organization
  - Government Regulation
  - Natural Disaster