IT Security and Risk Management

Risk Assessment

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

ربيع 2024

https://t.me/+xavNMXu7DyM5Yjc0

Introduction to Risk Assessment

- The goal is to create a method to evaluate the relative risk of each listed vulnerability.
- Simple model – risk R, probability of risk event P and value lost by risk event V satisfy R = PV

More complex model

- Extended risk formula

$R = P_a P_s V$

- Where P_a = Probability of attack and

P_s = Probability that the attack successfully exploits the vulnerability

V = value lost by successful exploitation of vulnerability

Another formula

- Extended Whitman's Risk Formula

R = P*V*(1 – CC + UK)

where P = probability that a vulnerability is exploited,

V = value of asset,

CC = fraction of risk mitigated by current control,

UK = fraction of risk not fully known (uncertainty of knowledge)

In words…

Risk is

The **likelihood** of the occurrence of a vulnerability

Multiplied by

The **value** of the information asset

Minus

The percentage of risk mitigated by **current controls**

Plus

The **uncertainty** of current knowledge of the vulnerability

Uncertainty: Impossible to know everything about every vulnerability

•The degree to which a current control can reduce risk is also subject to estimation error

•Uncertainty is estimated by the manager using judgment/experience

Risk Determination Example

- Asset A has a value of 50 and has one vulnerability, which has a likelihood of 1.0 with no current controls. Your assumptions and data are 90% accurate
- Asset B has a value of 100 and has two vulnerabilities: vulnerability #2 has a likelihood of 0.5 with a current control that addresses 50% of its risk; vulnerability # 3 has a likelihood of 0.1 with no current controls. Your assumptions and data are 80% accurate
- The resulting ranked list of risk ratings for the three vulnerabilities is as follows:
  - Asset A: Vulnerability 1 rated as 55 = (50 × 1.0) – 0% + 10%
  - Asset B: Vulnerability 2 rated as 35 = (100 × 0.5) – 50% + 20%
  - Asset B: Vulnerability 3 rated as 12 = (100 × 0.1) – 0 % + 20%

Documenting the Results of Risk Assessment

- Goals of the risk management process
  - To identify information assets and their vulnerabilities
  - To rank them according to the need for protection
- In preparing this list, a wealth of factual information about the assets and the threats they face is collected
- Information about the controls that are already in place is also collected
- The final summarized document is the ranked vulnerability risk worksheet

Sample of Documenting the Results of Risk Assessment

Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via Secure Sockets Layer (SSL) (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Webserver denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.01	1

Risk Control

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas
- Three general categories of controls exist:
  - Policies
  - Programs
  - Technical controls

Risk Control Strategies

- four basic strategies to control risks
  - Avoidance
    - Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
  - Transference
    - Shifting the risk to other areas or to outside entities
  - Mitigation
    - Reducing the impact if the vulnerability is exploited
  - Acceptance
    - Understanding the consequences and accepting the risk without control or mitigation

Avoidance

- The risk control strategy that attempts to prevent the exploitation of the vulnerability
- Avoidance is accomplished through:
  - Application of policy
  - Application of training and education
  - Countering threats
  - Implementation of technical security controls

Transference

- The control approach that attempts to shift the risk to other assets, other processes, or other organizations
- May be accomplished by rethinking how services are offered
  - Revising deployment models
  - Outsourcing to other organizations
  - Purchasing insurance
  - Implementing service contracts with providers

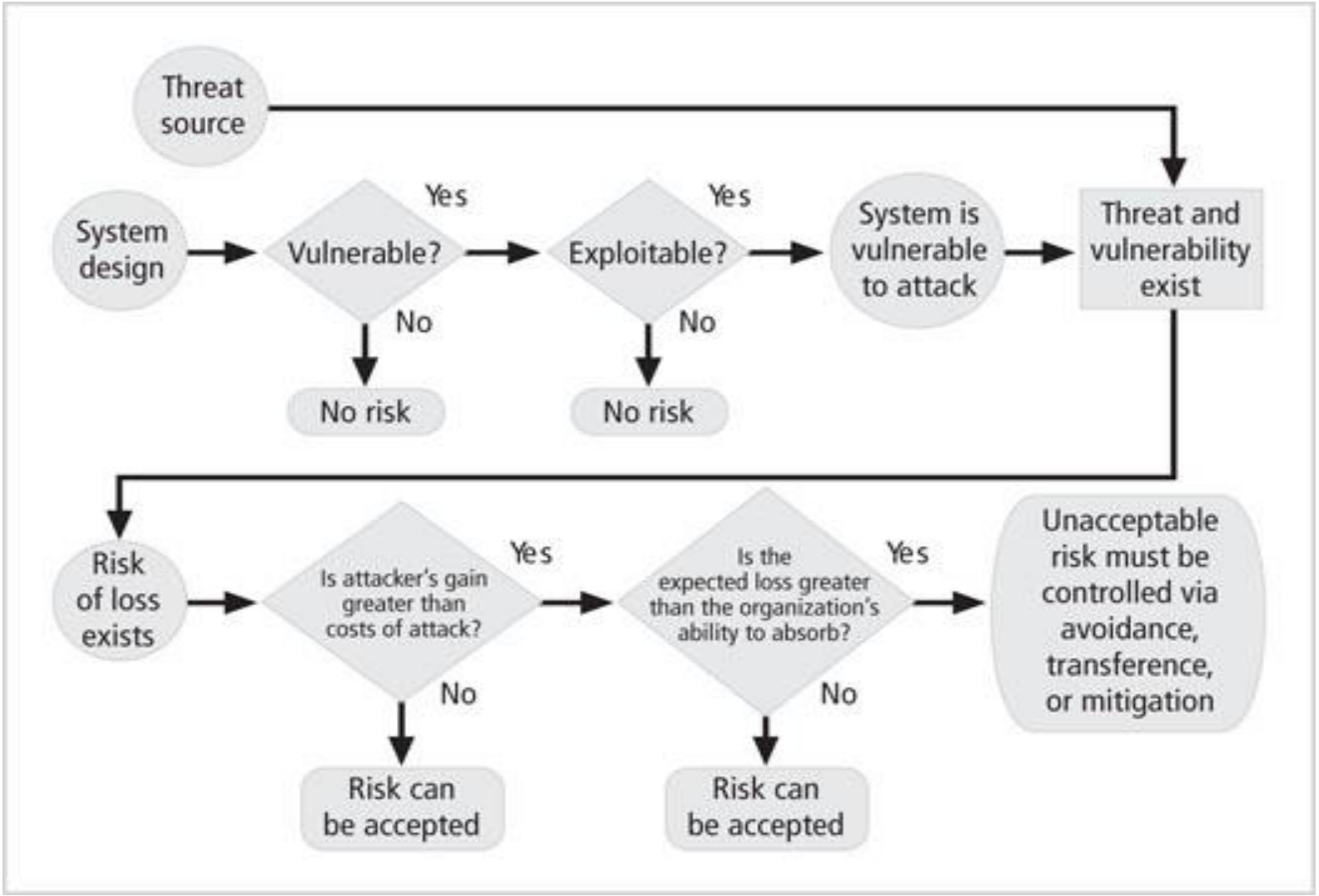
Mitigation

- The control approach that attempts to reduce the damage caused by the exploitation of vulnerability
  - Using planning and preparation
  - Depends upon the ability to detect and respond to an attack as quickly as possible
- Types of mitigation plans
  - Disaster recovery plan (DRP)
  - Incident response plan (IRP)
  - Business continuity plan (BCP)

Acceptance

- Do nothing to protect an information asset just accept the loss when it occurs.
- the organization must:
  - Determine the level of risk to the information asset
  - Assess the probability of attack and the likelihood of a successful exploitation of a vulnerability
  - Estimate the potential loss from attacks
  - Perform a thorough cost benefit analysis
  - Evaluate controls using each appropriate type of feasibility

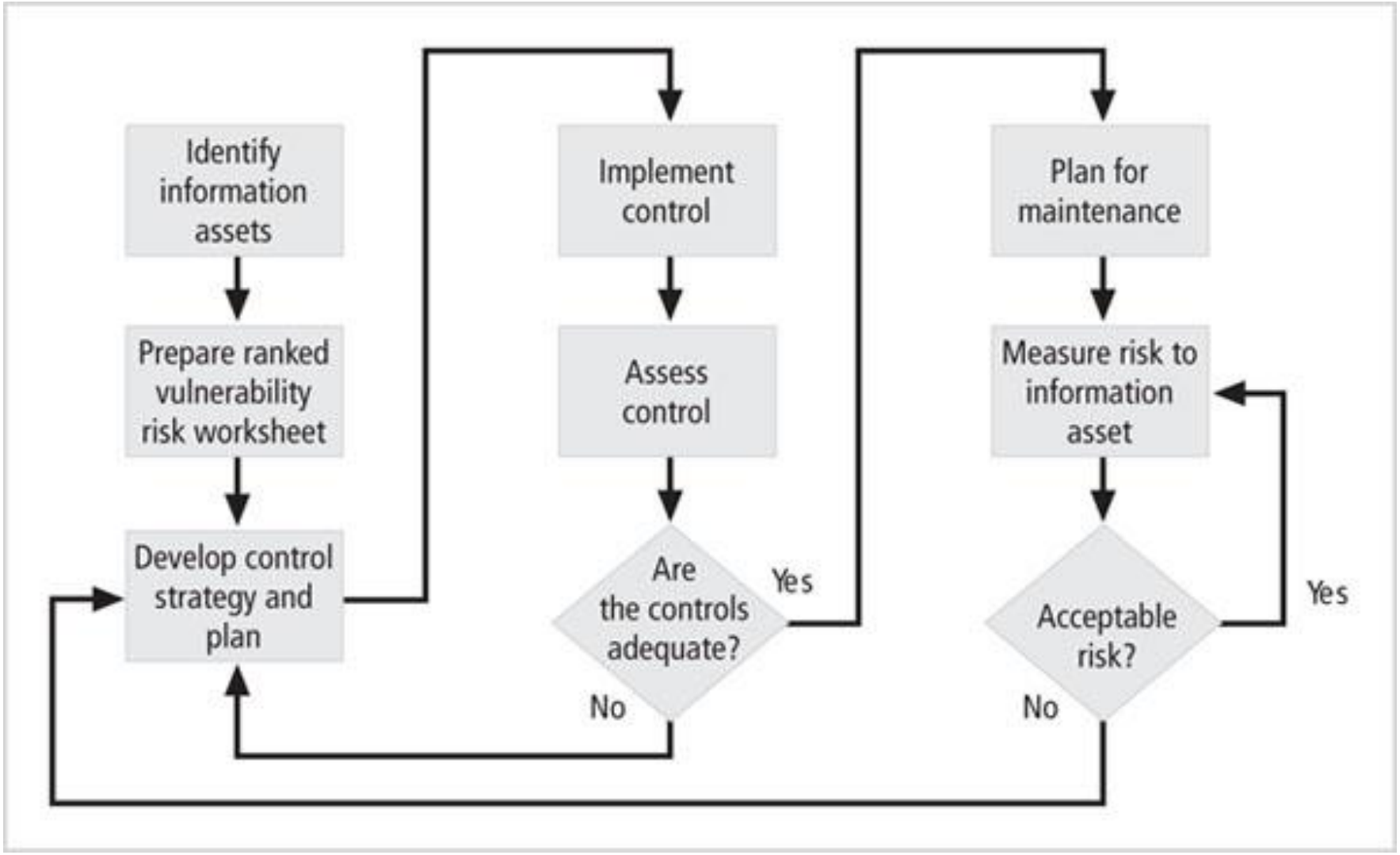
Risk handling action points



Guidelines for risk control strategy selection

- When a vulnerability exists
  - Implement security controls to reduce the likelihood of a vulnerability being exercised
- When a vulnerability can be exploited
  - Apply layered controls to minimize the risk or prevent occurrence
- When the attacker's potential gain is greater than the costs of attack
  - Apply technical or managerial controls to increase the attacker's cost, or reduce his gain
- When potential loss is substantial
  - Apply design controls to limit the extent of the attack, thereby reducing the potential for loss

Risk control cycle



THANK YOU

ANY QUESTION?