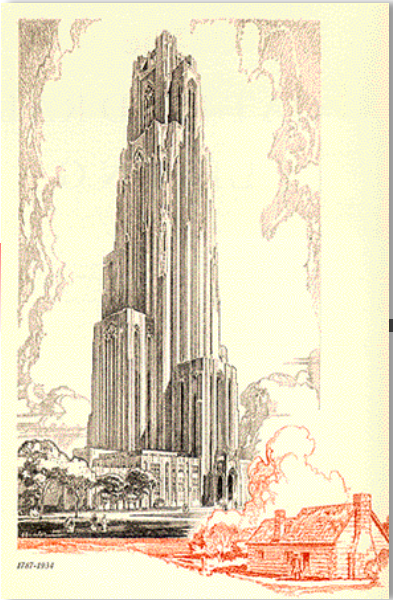


TEL2813/IS2621

Security Management



James Joshi
Associate Professor

Lecture 4
Feb 12, 2014

Risk Management



Introduction

- A Crucial job of InfoSec dept is

Risk management

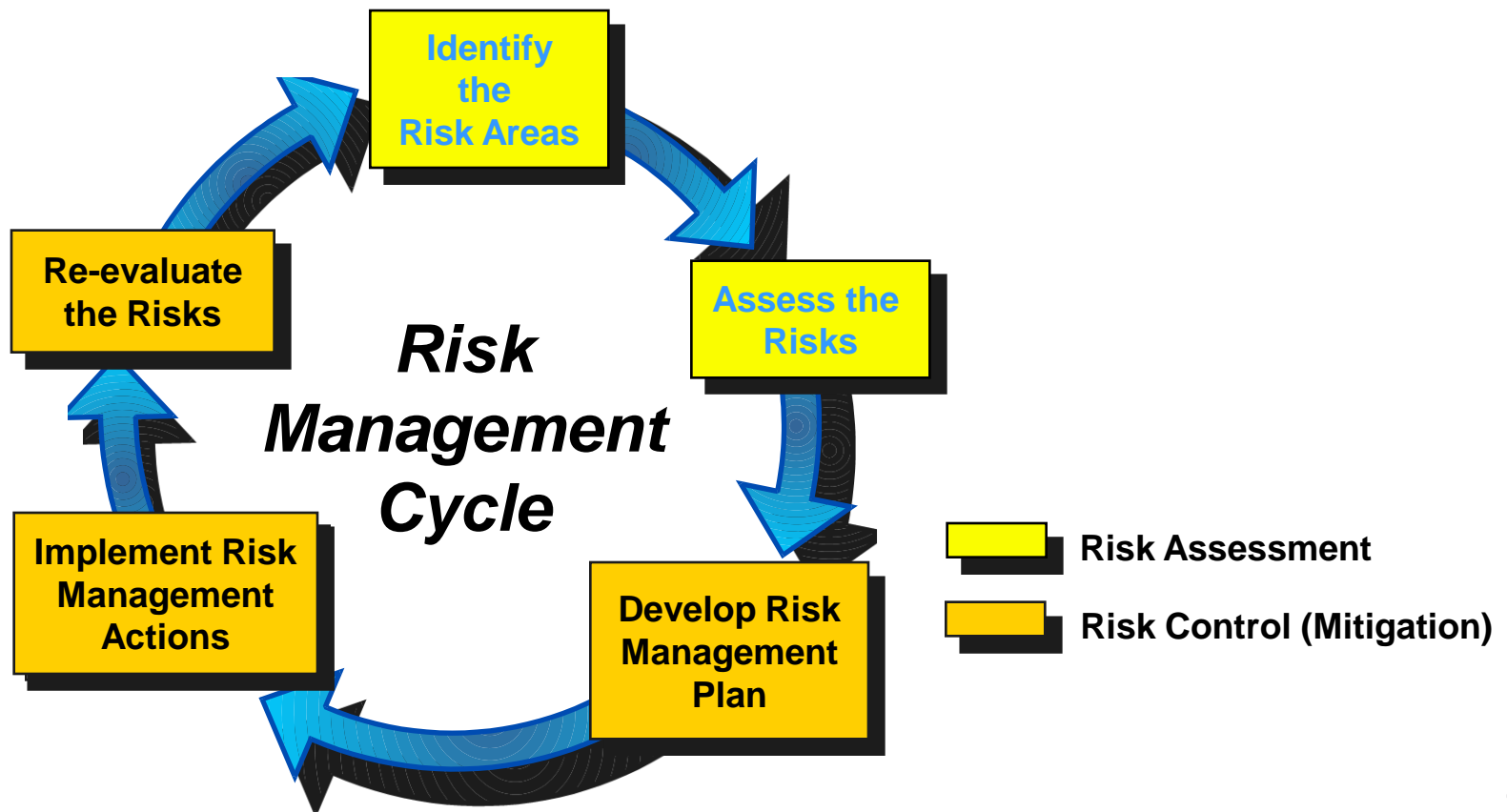
- Risk management is a process

of assessing the risks to an organization's information and determining how those risks can be controlled or mitigated

- Process means - safeguards and controls that are devised and implemented are not install-and-forget
- Two formal processes are at work:
 - Risk identification and assessment
 - Risk control

Risk Management

- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)



Accountability for Risk Management



- All *communities of interest* must work together:
 - Identifying risks
 - Assessing risks
 - Evaluating risk controls
 - Determining cost-effective control options
 - Acquiring or installing appropriate controls
 - Overseeing processes to ensure that controls remain effective
 - Summarizing findings

Risk Identification Process

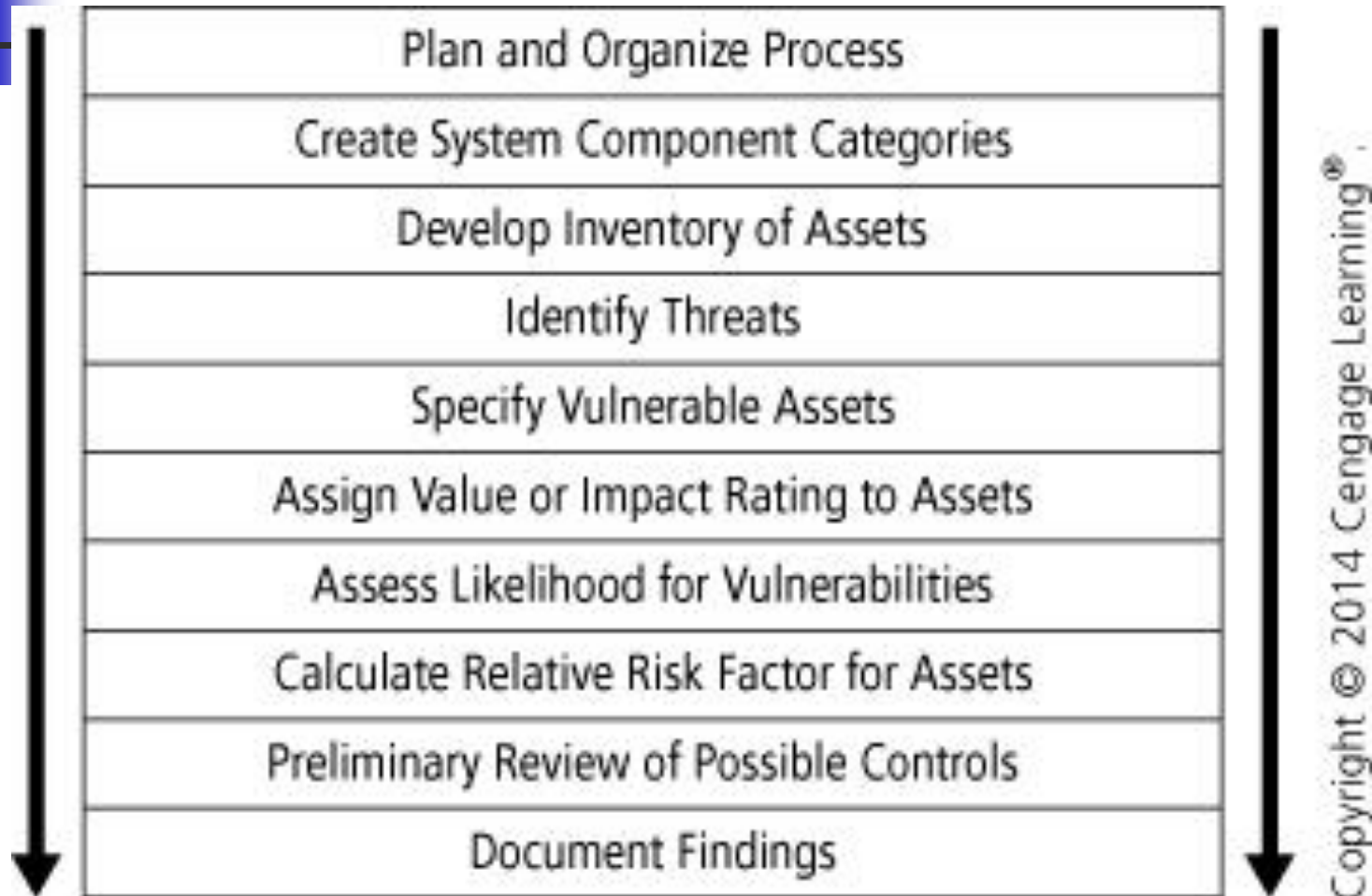


Figure 8-1 Risk identification and assessment process



Risk Identification

- Risk identification
 - begins with the process of self-examination
- Managers
 - Identify information assets,
 - classify and categorize them
 - prioritize them by their overall importance

Identify weaknesses and threats related to them

Creating an Inventory of Information Assets

- Identify information assets:

IT System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking	Local Area Network components Intranet components Internet or extranet components Cloud-based components

Copyright © 2014 Cengage Learning®

Organizational assets used in systems



Identifying Hardware, Software, and Network Assets

- Inventory process
 - *requires a certain amount of planning*
 - Keep track of all components
 - Automatic or manual inventory system
- Determine which attributes of each should be tracked
 - Will depend on the needs of the organization and
 - its risk management efforts



Attributes for Assets

- Potential attributes:
 - Name
 - IP address
 - MAC address
 - Asset type
 - Manufacturer name
 - Manufacturer's model or part number
 - Software version, update revision,
 - Physical location
 - Logical location
 - Controlling entity



Suggested Attributes

■ People

- Position
name/number/ID
- Supervisor
name/number/ID
- Security clearance level
- Special skills

■ Procedures

- Description
- Intended purpose
- Software/hardware/networking elements to which it is tied
- Location where it is stored for reference
- Location where it is stored for update purposes



Suggested Attributes

- Data
 - Classification
 - Owner/creator/manager
 - Size of data structure
 - Data structure used
 - Online or offline
 - Location
 - Backup procedures



Classifying and Categorizing

- Determine whether its asset categories are meaningful
 - After initial inventory is assembled,
- Inventory should also reflect
 - *sensitivity* and *security priority* assigned to each asset
 - A classification scheme uses their sensitivity and security needs



Classifying and Categorizing Assets (Continued)

- Categories
 - designates level of protection needed for a particular information asset
- Classification categories must be:
 - comprehensive and mutually exclusive
- Some asset types, such as personnel,
 - may require an alternative classification scheme that would identify the clearance needed to use the asset type



Assessing Values for Information Assets

- Assign a relative value
 - to ensure that the most valuable information assets are given the highest priority, for example:
 - Which is the most critical to the success of the organization?
 - Which generates the most revenue?
 - Which generates the highest profitability?
 - Which is the most expensive to replace?
 - Which is the most expensive to protect?
 - Whose loss or compromise would be the most embarrassing or cause the greatest liability?
- **Final step:** list the assets in order of importance
 - Can use a weighted factor analysis worksheet

Sample Asset Classification Worksheet

System Name: <u>SLS E-Commerce</u>		
Date Evaluated: <u>February 2008</u>		
Evaluated By: <u>D. Jones</u>		
Information assets	Data classification	Impact to profitability
<u>Information Transmitted:</u>		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
<u>DMZ Assets:</u>		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical
Notes: BOL: Bill of Lading DMZ: Demilitarized Zone EDI: Electronic Data Interchange SSL: Secure Sockets Layer		

Weighted Factor Analysis Worksheet (NIST SP 800-30)

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55



Data Classification Model

- Data owners must
 - classify information assets they are responsible for
 - review the classifications periodically
- Example:
 - Public
 - For official use only
 - Sensitive
 - Classified



Data Classification Model

- U.S. military classification scheme
 - more complex categorization system than the schemes of most corporations
- Uses a five-level classification scheme as defined in Executive Order 12958:
 - Unclassified Data
 - Sensitive But Unclassified (SBU) Data
 - Confidential Data
 - Secret Data
 - Top Secret Data



Security Clearances

- Personnel Security Clearance Structure:
 - Complement to data classification scheme
 - Each user of information asset is assigned an authorization level that indicates level of information classification he or she can access
- Most organizations have developed a set of roles and corresponding security clearances
 - Individuals are assigned into groups/roles that correlate with classifications of the information assets they need
- Need-to-know principle



Management of Classified Information Assets

- Managing an information asset includes
 - considering the [storage](#), [distribution](#), [portability](#), and [destruction](#) of that information asset
- Clean Desk policy
 - To maintain confidentiality of classified documents, managers can implement a clean desk policy
- Destruction of sensitive material
 - care should be taken to destroy asset properly to discourage [dumpster diving](#)



Threat Identification

- Threat identification –
 - process of assessing potential weaknesses in each information asset
- Each threat presents a unique challenge
 - Must be handled with specific controls that directly address particular threat and threat agent's attack strategy
- Threat assessment
 - each threat must be examined to determine its potential to affect targeted information asset



Threats to InfoSec

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, backdoors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Threats to Information Security (whitman survey)

Weighted Ranks of Threats to Information Security				
Threat	Mean	Standard Deviation	Weight	Weighted Rank
1. Deliberate software attacks	3.99	1.03	546	2178.3
2. Technical software failures or errors	3.16	1.13	358	1129.9
3. Acts of human error or failure	3.15	1.11	350	1101.0
4. Deliberate acts of espionage or trespass	3.22	1.37	324	1043.6
5. Deliberate acts of sabotage or vandalism	3.15	1.37	306	962.6
6. Technical hardware failures or errors	3.00	1.18	314	942.0
7. Deliberate acts of theft	3.07	1.30	226	694.5
8. Forces of nature	2.80	1.09	218	610.9
9. Compromises to intellectual property	2.72	1.21	182	494.8
10. Quality-of-service deviations from service providers	2.65	1.06	164	433.9
11. Technological obsolescence	2.71	1.11	158	427.9
12. Deliberate acts of information extortion	2.45	1.42	92	225.2



Weighted Ranking of Threat-Driven Expenditures

Top Threat-Driven Expenses	Rating
Deliberate software attacks	12.7
Acts of human error or failure	7.6
Technical software failures or errors	7.0
Technical hardware failures or errors	6.0
QoS deviations from service providers	4.9
Deliberate acts of espionage or trespass	4.7
Deliberate acts of theft	4.1
Deliberate acts of sabotage or vandalism	4.0
Technological obsolescence	3.3
Forces of nature	3.0
Compromises to intellectual property	2.2
Deliberate acts of information extortion	1.0



Vulnerability Assessment

- Steps revisited
 - Identify the information assets of the organization and
 - Document some threat assessment criteria,
 - **Begin to review every information asset for each threat**
 - Leads to creation of list of vulnerabilities that remain potential risks to organization
- At the end of the risk identification process,
 - a list of assets and their vulnerabilities has been developed
- The goal: to evaluate relative risk of each listed vulnerability

Methods of Assessing Threats

- A 2012 survey of computing executives asked “In your organization’s risk management efforts, what basis do you use to assess threats?”

Threat (Based on Money and Effort Spent to Defend Against or React to It)	2012 Rating Average	2012 Ranking	2003 CACM Ranking
Espionage or trespass	4.07	1	6
Software attacks	3.94	2	1
Theft	3.18	3	7
Quality-of-service deviations by service providers	3.10	4	5
Forces of nature	3.06	5	10
Sabotage or vandalism	3.00	6	8
Technological obsolescence	2.99	7	9
Technical software failures or errors	2.71	8	3
Technical hardware failures or errors	2.64	9	4
Compromises to intellectual property	2.55	10	11
Human error or failure	2.25	11	2
Information extortion	2.00	12	12

Copyright © 2014 Cengage Learning®.

Basis of threat assessment



The TVA Worksheet

- At the end of the risk identification process, there should be two lists:
 - Prioritized list of assets and their vulnerabilities
 - Prioritized list of threats facing the organization based on a weighted table
- These two lists can be combined into a Threats-Vulnerabilities-Assets (TVA) worksheet
 - Prioritized set of assets are placed along the horizontal axis
 - Prioritized list of threats is placed along the vertical axis



The TVA Worksheet

- Vulnerabilities are identified between threats and assets and are categorized as follows:
 - T1V1A1 –
 - Vulnerability 1 that exists between Threat 1 and Asset 1
 - T1V2A1 –
 - Vulnerability 2 that exists between Threat 1 and Asset 1
 - T2V1A1 –
 - Vulnerability 1 that exists between Threat 2 and Asset 1

Cataloging and categorizing controls is the next step



Risk Assessment

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

Likelihood of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event



Assessing Potential Loss

- To be effective, the likelihood values must be assigned by considering various questions:
 - Which threats present a danger to the organization's assets in the given environment?
 - Which threats represent the *most danger* to the organization's information?
 - How much would it *cost to recover* from a successful attack?
 - Which threats would require *the greatest expenditure* to prevent?
 - Which of the aforementioned questions is the most important to the protection of information from threats within this organization?



Mitigated Risk / Uncertainty

- If it is partially controlled,
 - Estimate what percentage of the vulnerability has been controlled
- **Uncertainty**
 - is an estimate made by the manager using judgment and experience
 - It is not possible to know everything about every vulnerability
 - The degree to which a current control can reduce risk is also subject to estimation error



Risk Determination Example

- **Asset A** has a value of 50 and has vulnerability #1,
 - likelihood of 1.0 with no current controls
 - assumptions and data are 90% accurate
- **Asset B** has a value of 100 and has two vulnerabilities
 - Vulnerability #2
 - likelihood of 0.5 with a current control that addresses 50% of its risk
 - Vulnerability # 3
 - likelihood of 0.1 with no current controls
 - assumptions and data are 80% accurate



Risk Determination Example

- Resulting ranked list of risk ratings for the three vulnerabilities is as follows:
 - Asset A: Vulnerability 1 rated as 55 =
 - $(50 \times 1.0) - 0\% + 10\%$
 - Asset B: Vulnerability 2 rated as 35 =
 - $(100 \times 0.5) - 50\% + 20\%$
 - Asset B: Vulnerability 3 rated as 12 =
 - $(100 \times 0.1) - 0\% + 20\%$



Risk determination

- Another approach: Australian & New Zealand RM Standard 360
 - Uses qualitative methods to determine risk based on a threat's probability of occurrence and expected results of an attack

Level	Descriptor	Example of Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, onsite release immediately contained, medium financial loss
3	Moderate	Medical treatment required, onsite release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, offsite release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release offsite with detrimental effect, huge financial loss

Consequence levels for organizational threats

Risk determination

- Australian & New Zealand RM Standard 360

Level	Descriptor	Explanation
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

Copyright © 2014 Cengage Learning®

Likelihood levels for organizational threats

Risk Level	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood					
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

Source: Risk management plan templates and forms from www.treasury.act.gov.au/actia/risk.htm

Qualitative risk assessment matrix



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



Access Controls

- Access controls address the admission of users into trusted areas of the organization
 - Usually consist of a combination of policies, programs, and technologies
- A number of approaches to, and categories of, access controls exist:
 - Mandatory
 - Nondiscretionary
 - Discretionary



Documenting the Results of Risk Assessment

- The final summarized document is the ranked vulnerability risk worksheet
- The columns in the worksheet are used as follows:
 - *Asset* - list each vulnerable asset
 - *Asset impact* - show the results for this asset from the weighted factor analysis worksheet
 - *Vulnerability* - list each uncontrolled vulnerability
 - *Vulnerability likelihood* - the likelihood of the realization of the vulnerability by a threat agent
 - *Risk-rating factor* - the figure calculated by multiplying the asset impact and its likelihood

Ranked Vulnerability Risk Worksheet

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 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 or 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	0.1	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.1	1

Ranked vulnerability risk worksheet

Copyright © 2014 Cengage Learning®



Documenting the Results of Risk Assessment (Continued)

- What are the deliverables from this stage of the risk management project?
- The risk identification process should designate
 - what function the reports serve,
 - who is responsible for preparing them, and
 - who reviews them

Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
TVA worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization and identifies potential vulnerabilities in the "triples"; also incorporates extant and planned controls
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset-vulnerability pair



Risk Management: Assessing and Controlling Risk



Risk Control Strategies

- Choose basic risk control strategy :
 - **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 should the vulnerability be exploited
 - **Acceptance:**
 - understanding the consequences and accept the risk without control or mitigation



Avoidance

- Attempts to prevent the exploitation of the vulnerability
- Accomplished through:
 - Application of policy
 - Application of training and education
 - Countering threats
 - Implementation of technical security controls and safeguards



Transference

- 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

- Attempts to reduce the damage caused by the exploitation of vulnerability
 - by means of planning and preparation,
- Includes three types of plans:
 - Disaster recovery plan (DRP)
 - Incident response plan (IRP)
 - Business continuity plan (BCP)
- Depends upon
 - the ability to detect and respond to an attack as quickly as possible



Risk Control Strategy Selection

- Risk control involves
 - selecting one of the four risk control strategies for the vulnerabilities present within the organization
- Acceptance of risk
 - If the loss is within the range of losses the organization can absorb, or
 - if the attacker's gain is less than expected costs of the attack,
- Otherwise, one of the other control strategies will have to be selected

Risk Handling Action Points

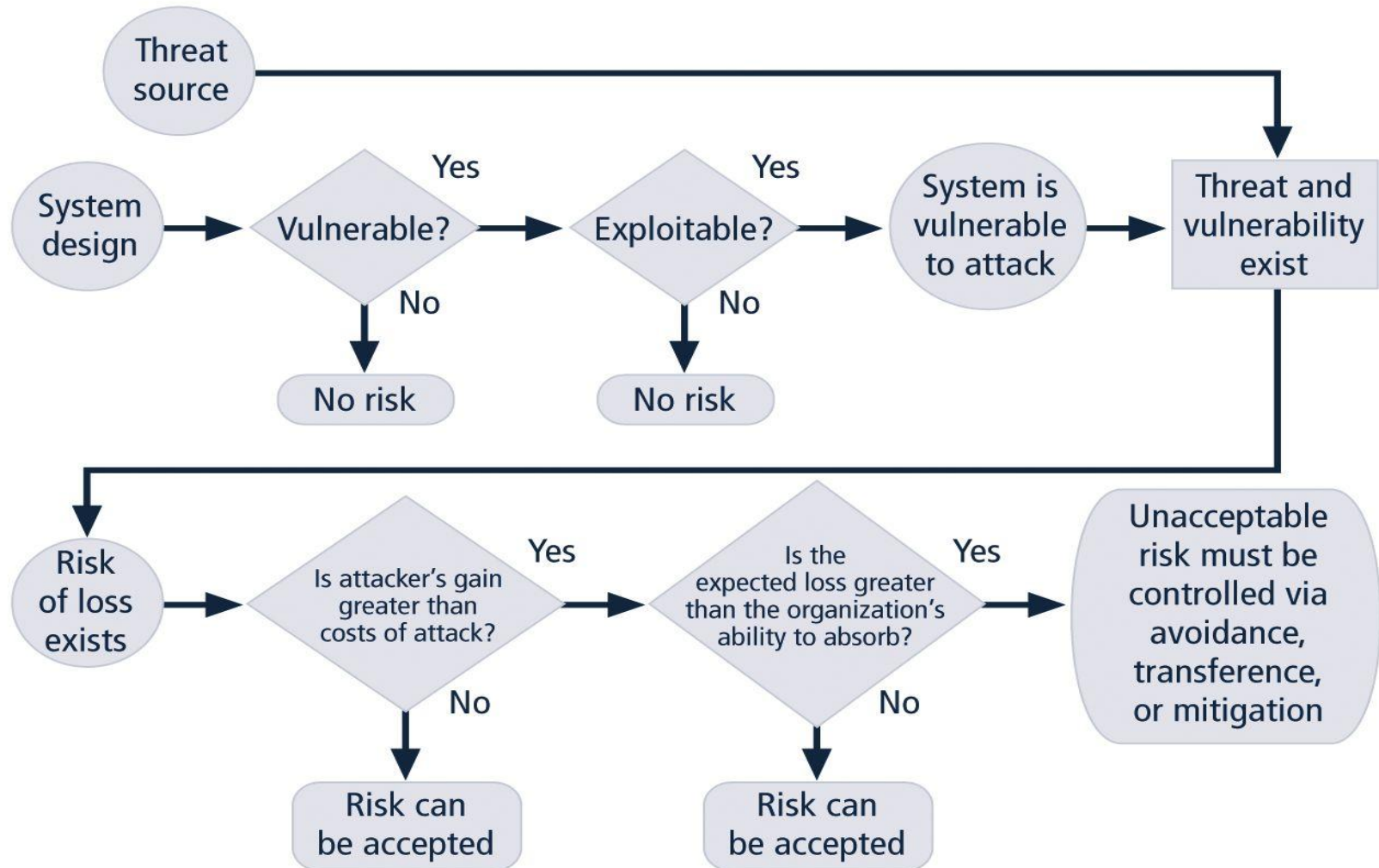


FIGURE 8-2 Risk-Handling Action Points

The Risk Control Cycle

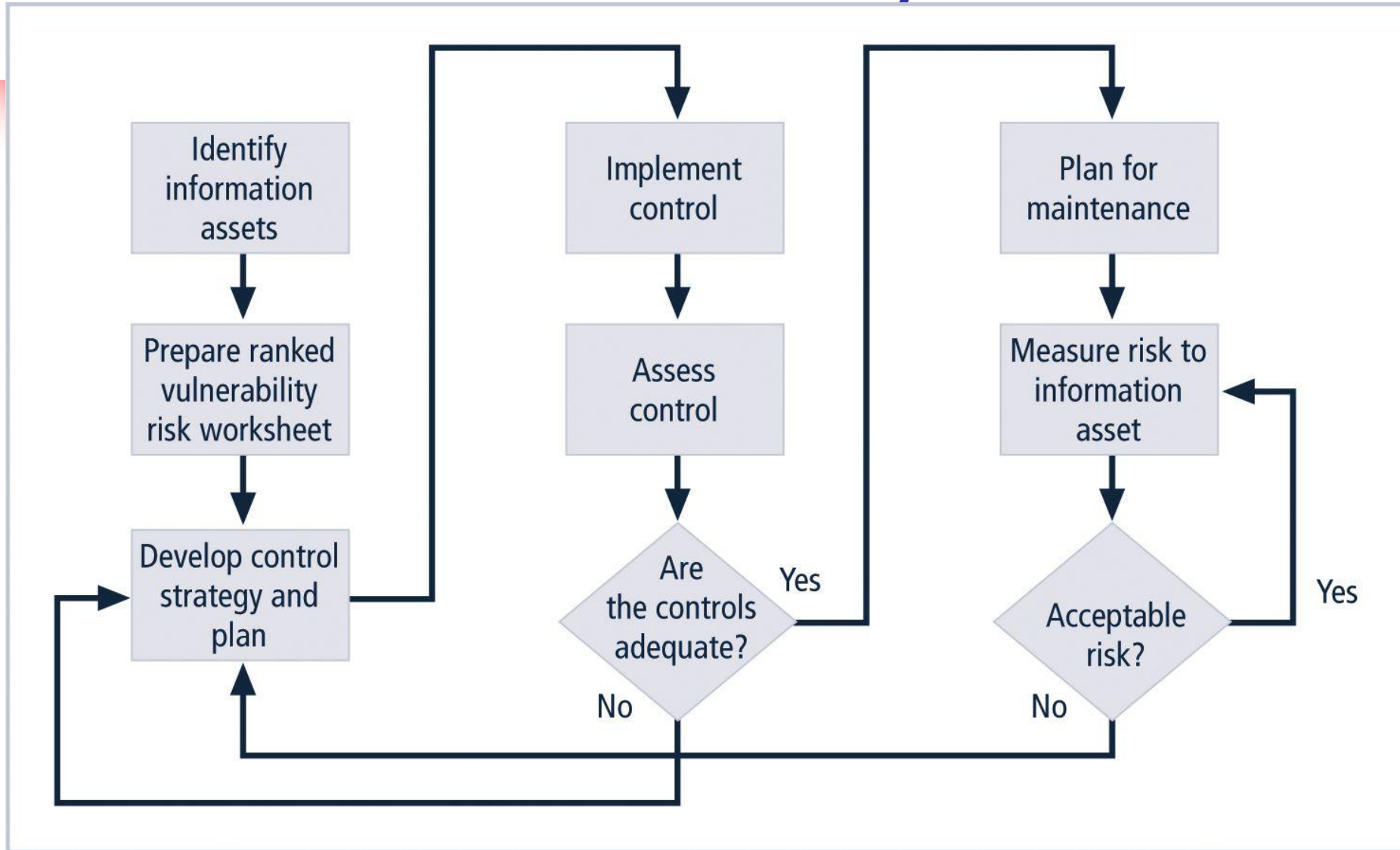


FIGURE 8-3 Risk Control Cycle



Feasibility Studies and Cost Benefit Analysis

- Information about the consequences of the vulnerability must be explored
 - Before deciding on the strategy for a specific vulnerability,
- Determine advantage or disadvantage of a specific control
 - Primary means are based on the value of information assets that control is designed to protect



Cost Benefit Analysis (CBA)

- Economic Feasibility
 - criterion most commonly used when evaluating a project that implements information security controls and safeguards
- Should begin a CBA by evaluating
 - Worth of the information assets to be protected
 - Loss in value if those information assets are compromised

Cost Benefit Analysis or *Economic Feasibility Study*



Cost

- It is difficult
 - to determine the value of information,
 - to determine the cost of safeguarding it
- Some of the items that affect the cost of a control or safeguard include:
 - Cost of development or acquisition of hardware, software, and services
 - Training fees
 - Cost of implementation
 - Service costs
 - Cost of maintenance



Benefit

- Benefit is
 - the value to the organization of using controls to prevent losses associated with a specific vulnerability
- Usually determined by
 - Valuing the information assets exposed by vulnerability
 - Determining how much of that value is at risk and how much risk there is for the asset
- This is expressed as
 - Annualized Loss Expectancy (ALE)



Asset Valuation

■ Asset valuation is

- a challenging process of assigning financial value or worth to each information asset
- Valuation of assets involves:
 - Estimation of real and perceived costs associated with design, development, installation, maintenance, protection, recovery, and defense against loss and litigation



Asset Valuation Techniques

- **Single loss expectancy (SLE):**

- value associated with most likely loss from an attack
- Based on estimated asset value and expected percentage of loss that would occur from attack:

$$\text{SLE} = \text{asset value (AV)} \times \text{exposure factor (EF)}$$

- *EF = the percentage loss that would occur from a given vulnerability being exploited*

- **Annualized rate of occurrence (ARO)**

- probability of an attack within a given time frame, annualized per year

- **Annualized loss expectancy (ALE)**

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

The Cost Benefit Analysis (CBA) Formula

- CBA determines whether or not a control alternative is worth its associated cost
 - CBAs may be calculated
 - Before a control or safeguard is implemented to determine if the control is worth implementing
 - OR**
 - After controls have been implemented and have been functioning for a time:
- $CBA = ALE(\text{prior}) - ALE(\text{post}) - ACS$**
- ACS is
 - the annual cost of the safeguard



Other Feasibility Approaches

- Organizational feasibility analysis
 - examines how well the proposed information security alternatives will contribute to operation of an organization
- Operational (behavioral) feasibility analysis
 - Addresses user acceptance and support, management acceptance and support, and overall requirements of organization's stakeholders
- Technical feasibility analysis
 - examines whether or not the organization has or can acquire the technology to implement and support the alternatives
- Political feasibility analysis
 - defines what can and cannot occur based on the consensus and relationships between the communities of interest



Alternative to CBA: Benchmarking

- Benchmarking:
 - Seeking out and studying practices of other organizations that produce desired results
 - Measuring differences between how organizations conduct business
- When benchmarking, an organization typically uses one of two measures to compare practices:
 - Metrics-based measures
 - comparisons based on numerical standards
 - Process-based measures
 - generally less focused on numbers and are more strategic



Benchmarking (Continued)

- In the field of information security, two categories of benchmarks are used:
 - Standards of **due care** and **due diligence**, and
 - Best practices
- Best practices,
 - the gold standard is a subcategory of practices that are typically viewed as “the best of the best”



Due Care and Due Diligence

- For legal reasons, an organization may be forced to adopt a certain minimum level of security
- Due Care
 - adopt levels of security for legal defense,
 - need to show that they have done what any prudent organization would do in similar circumstances
- Due diligence
 - demonstration that organization is persistent in ensuring implemented standards continue to provide required level of protection



Applying Best Practices

- Address the following questions:
 - Does your organization **resemble** the organization that is implementing the best practice under consideration?
 - Is your organization in a similar industry?
 - Does your organization face similar challenges?
 - Is your **organizational structure similar** to the organization from which you are modeling the best practices?
 - Can your organization **expend resources** that are in line with the requirements of the best practice?
 - Is your organization in a similar threat environment as the one cited in the best practice?



Problems with Benchmarking and Best Practices

- Organizations don't talk to each other
- No two organizations are identical
- Best practices are a moving target
- Simply knowing what was going on a few years ago does not necessarily indicate what to do next



Risk Appetite

- Risk appetite
 - defines the quantity and nature of risk that organizations are willing to accept, as they evaluate the trade-offs between perfect security and unlimited accessibility
- Reasoned approach to risk is one that
 - balances expense against possible losses if exploited



Residual Risk

- When vulnerabilities have been controlled as much as possible, there is often remaining risk that has not been completely accounted for residual risk →
- **Residual Risk:**
 - Risk from a threat less the effect of threat-reducing safeguards plus
 - Risk from a vulnerability less the effect of vulnerability-reducing safeguards plus
 - Risk to an asset less the effect of asset value-reducing safeguards



Residual Risk

- The significance of residual risk
 - must be judged within the context of an organization's **risk appetite**
- The goal of information security
 - is not to bring residual risk to zero,
 - but to bring it in line with an organization's **risk appetite**



Documenting Results

- When risk management program has been completed,
 - Series of proposed controls are prepared
 - Each justified by one or more feasibility or rationalization approaches
- At minimum, each **information asset-threat pair** should have a documented control strategy that
 - Clearly identifies any residual risk remaining after the proposed strategy has been executed

Recommended Risk Control Practices



- Each time a control is added to the matrix
 - It changes the ALE for the associated asset vulnerability as well as others
 - One safeguard can decrease risk associated with all subsequent control evaluations
 - May change the value assigned or calculated in a prior estimate.



Qualitative Measures

- Quantitative assessment performs asset valuation with actual values or estimates
- An organization could determine that it cannot put specific numbers on these values
- Organizations could use qualitative assessments instead, using scales instead of specific estimates



Delphi Approach

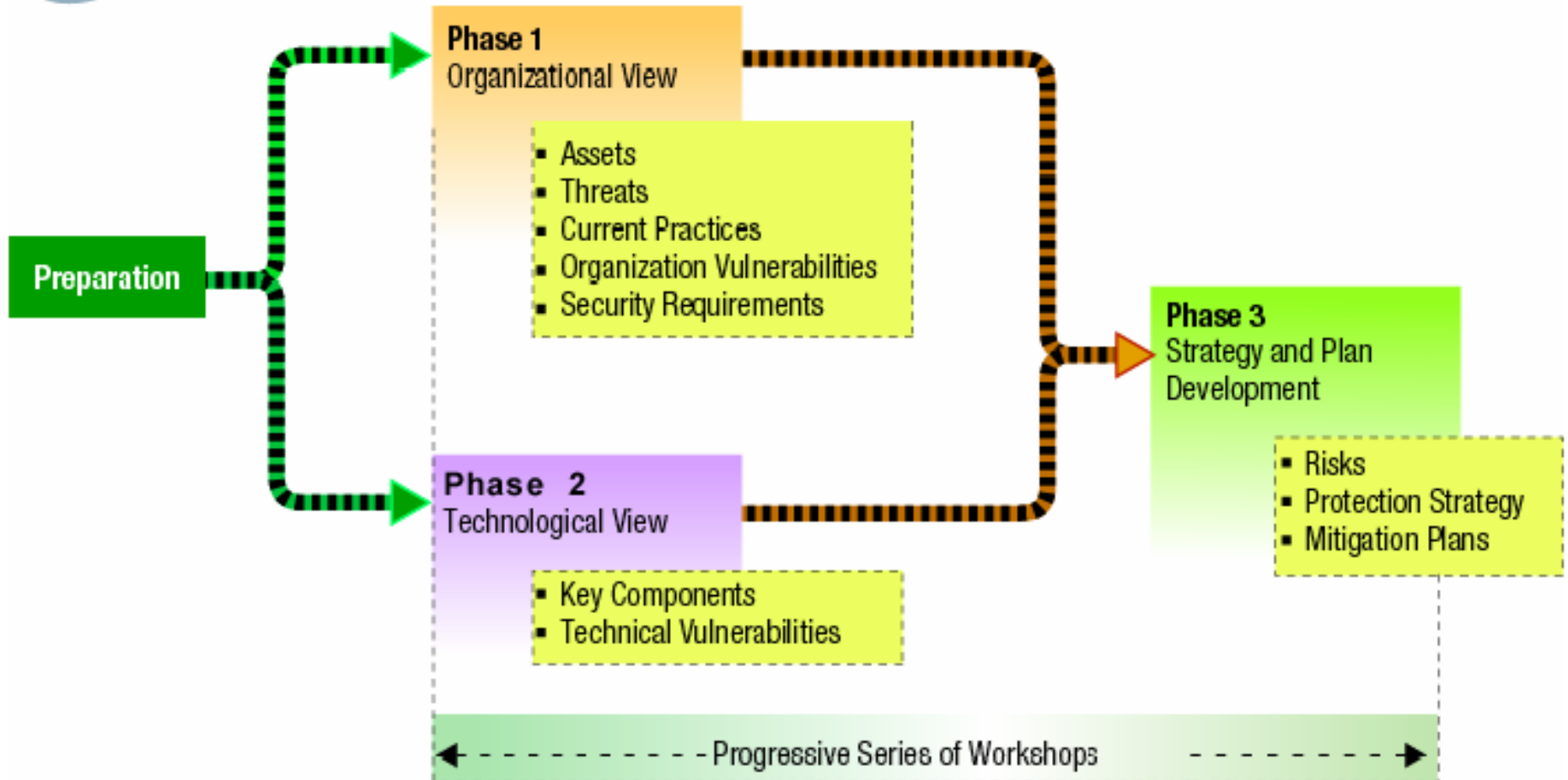
- A group rates and ranks assets
- The individual responses are compiled and sent back to the group
- Reevaluate and redo the rating/ranking
- Iterate till agreements reached



The OCTAVE Method

- **Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method:**
 - Defines essential components of a comprehensive, systematic, context-driven, self-directed information security risk evaluation
- **By following OCTAVE Method, organization can**
 - make information-protection decisions based on risks to
 - confidentiality, integrity, and availability of critical information technology assets
- **Three variations of the OCTAVE Method:**
 - The original OCTAVE Method
 - OCTAVE-S, for smaller organizations
 - OCTAVE-Allegro, a streamlined approach for InfoSec assessment and assurance

Octave[®] Process





Important Aspects of the OCTAVE Method

- The OCTAVE Method:
 - Self directed
 - Requires **analysis team** to conduct evaluation and analyze information
- Basic tasks of the team are to:
 - Facilitate knowledge elicitation workshops of Phase 1
 - Gather any necessary supporting data
 - Analyze threat and risk information
 - Develop a protection strategy for the organization
 - Develop mitigation plans to address risks to the organization's critical assets



Important Aspects of the OCTAVE Method (Continued)

- OCTAVE Method:
 - Uses workshop-based approach for gathering information and making decisions
 - Relies upon the following major catalogs of information:
 - Catalog of practices: collection of good strategic and operational security practices
 - Threat profile: range of major sources of threats that an organization needs to consider
 - Catalog of vulnerabilities: collection of vulnerabilities based on platform and application
 - www.cert.org/octave/omig.html



Phases & Processes of the OCTAVE Method

- Each phase of the OCTAVE Method contains two or more processes. Each process is made of activities.
- Phase 1: Build Asset-Based Threat Profiles
 - Process 1: Identify Senior Management Knowledge
 - Process 2: Identify Operational Area Management Knowledge
 - Process 3: Identify Staff Knowledge
 - Process 4: Create Threat Profiles



Phases & Processes of the OCTAVE Method (Continued)

- Phase 2: Identify Infrastructure Vulnerabilities
 - Process 5: Identify Key Components
 - Process 6: Evaluate Selected Components
- Phase 3: Develop Security Strategy and Plans
 - Process 7: Conduct Risk Analysis
 - Process 8: Develop Protection Strategy



Preparing for the OCTAVE Method

- Obtain senior management sponsorship of OCTAVE
- Select analysis team members.
- Train analysis team
- Select operational areas to participate in OCTAVE
- Select participants
- Coordinate logistics
- Brief all participants



The OCTAVE Method

- For more information, you can download the OctaveSM method implementation guide from www.cert.org/octave/omig.html



Microsoft Risk Management Approach

- Microsoft asserts that risk management is not a stand-alone subject
 - Should be part of a general governance program
- Microsoft RM process four phases :
 - Assessing risk
 - Conducting decision support
 - Implementing controls
 - Measuring program effectiveness



FAIR

- *Factor Analysis of Information Risk (FAIR)* (by Jack A. Jones)
- The FAIR framework includes:
 - A taxonomy for information risk
 - Standard nomenclature for information risk terms
 - A framework for establishing data collection criteria
 - Measurement scales for risk factors
 - A computational engine for calculating risk
 - A modeling construct for analyzing complex risk scenarios



FAIR

- FAIR analysis comprises 10 steps in four stages:
 - Stage 1-Identify Scenario Components
 - Identify the asset at risk
 - Identify the threat community under consideration
 - Stage 2-Evaluate Loss Event Frequency (LEF)
 - Estimate the probable Threat Event Frequency (TEF)
 - Estimate the Threat Capability (TCap)
 - Estimate the Control Strength (CS)
 - Derive Vulnerability (Vuln)
 - Derive Loss Event Frequency (LEF)



FAIR

- FAIR analysis comprises 10 steps in four stages (cont'd):
 - Stage 3-Evaluate Probable Loss Magnitude (PLM)
 - Estimate the worst-case loss
 - Estimate probably loss
 - Stage 4-Derive and Articulate Risk
 - Derive and articulate risk



Source: Copyright © 2014 Cengage Learning®.
 (Based on concepts from Jack A. Jones)®

Figure 9-4 Factor analysis of information risk (FAIR)

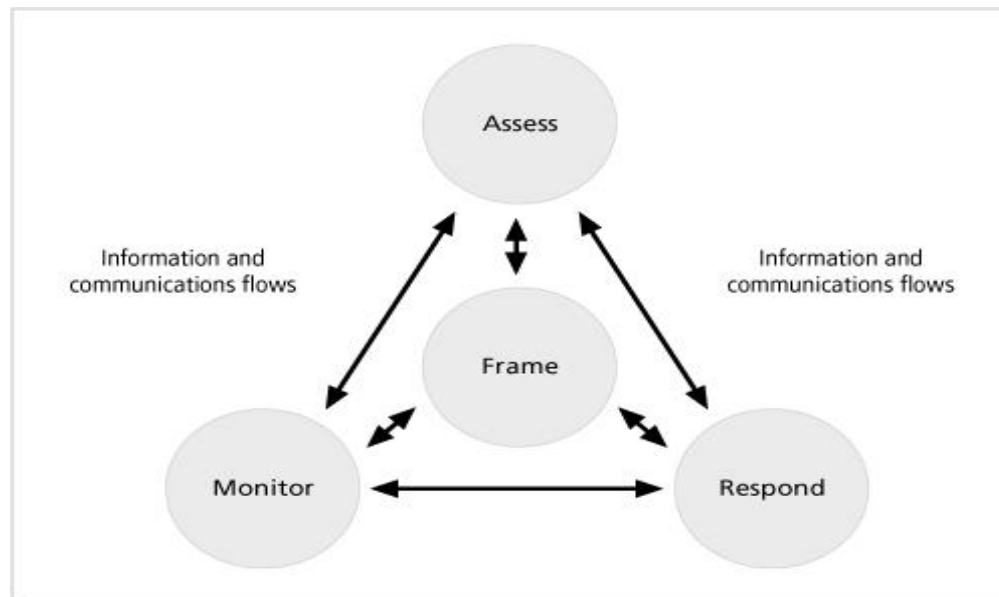


ISO 27005 Standard for InfoSec Risk Management

- ISO 27000 series includes a standard for the performance of risk management: ISO 27005
- Includes a five-stage risk management methodology:
 - Risk assessment
 - Risk treatment
 - Risk acceptance
 - Risk communication
 - Risk monitoring and review

NIST Risk Management Model

- This approach is illustrated below:



NIST risk management process



Other Methods

- There are two organizations that compare methods and provide recommendations for risk management tools that the public can use:
 - *European Network and Information Security Agency (ENISA)*
- ranks 12 tools using 22 different attributes
 - *New Zealand's IsecT Ltd* - a Web site that describes a large number of risk management methods

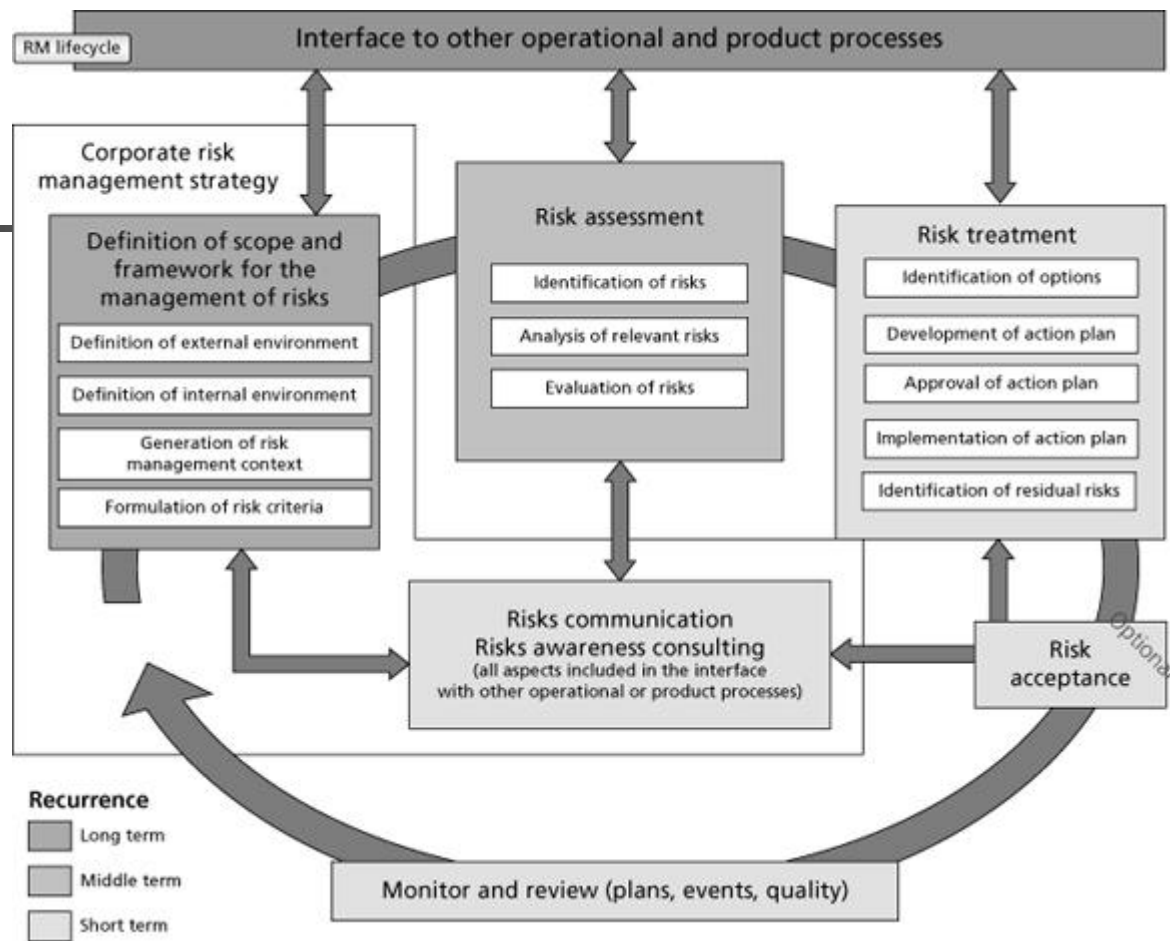
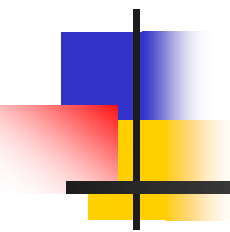


Figure 9-6 ENISA risk management process



Summary

- Introduction
- Risk Control Strategies
- Risk Control Strategy Selection
- Categories of Controls
- Feasibility Studies and Cost-Benefit Analysis
- Risk Management Discussion Points
- Recommended Risk Control Practices
- The OCTAVE and other Methods



Cost-Benefit Analysis, Net Present Value Model,
Internal Rate of Return Model
Return on Investment
(Based on Book by Gordon and Loeb)



Cost-benefit framework

- CBA

- widely accepted economic principle for managing organizational resources
- Requires **cost** of activity compared with the **benefit**
 - $\text{Cost} > \text{Benefit?}$
 - $\text{Cost} < \text{Benefit?}$
 - $\text{Cost} = \text{Benefit?}$



Cyber security Cost

- Operating Cost
 - Expenditure that will benefit a single period's operations (one fiscal year)
 - E.g., cost of patching software to correct breaches in the fiscal year
- Capital Investment
 - Expenditure that will benefit for several periods (Appears in balance sheet)
 - E.g., purchase of an IDS system (+ personnel cost)
 - Expect to work at least next few years



Cyber security Cost

- Capital investments lose their economic values
 - Portion of the investment that has been lost during a particular period is charged to that period
- In practice,
 - the distinction is not straightforward
 - Some argue
 - Most Cyber security expenditure are **operating costs**
 - However, they have spill over effect – hence could be treated as **capital investment**

Middle ground!!

Cyber security Cost :

In practice

- Most org. treat cyber security expenditure as Operating costs
 - Accounting and tax rules allow/motivate
 - By expensing these costs in the year of expenditure, tax savings are realized immediately
- Distinction is good (recommended)
 - From planning perspective
- A good approach
 - View all as capital investments with varying time horizons
 - OC becomes a special case of CI



Cost (C) vs. Benefit (B)

- Assume
 - B and C can be assessed for different level of cyber security activities
- Organization's goals should be
 - Implement security procedures up to the point where (B-C) is *maximum*
 - Implementing beyond that point means
 - The incremental costs > the incremental benefits
 - Net benefit beyond that maximum point is negative



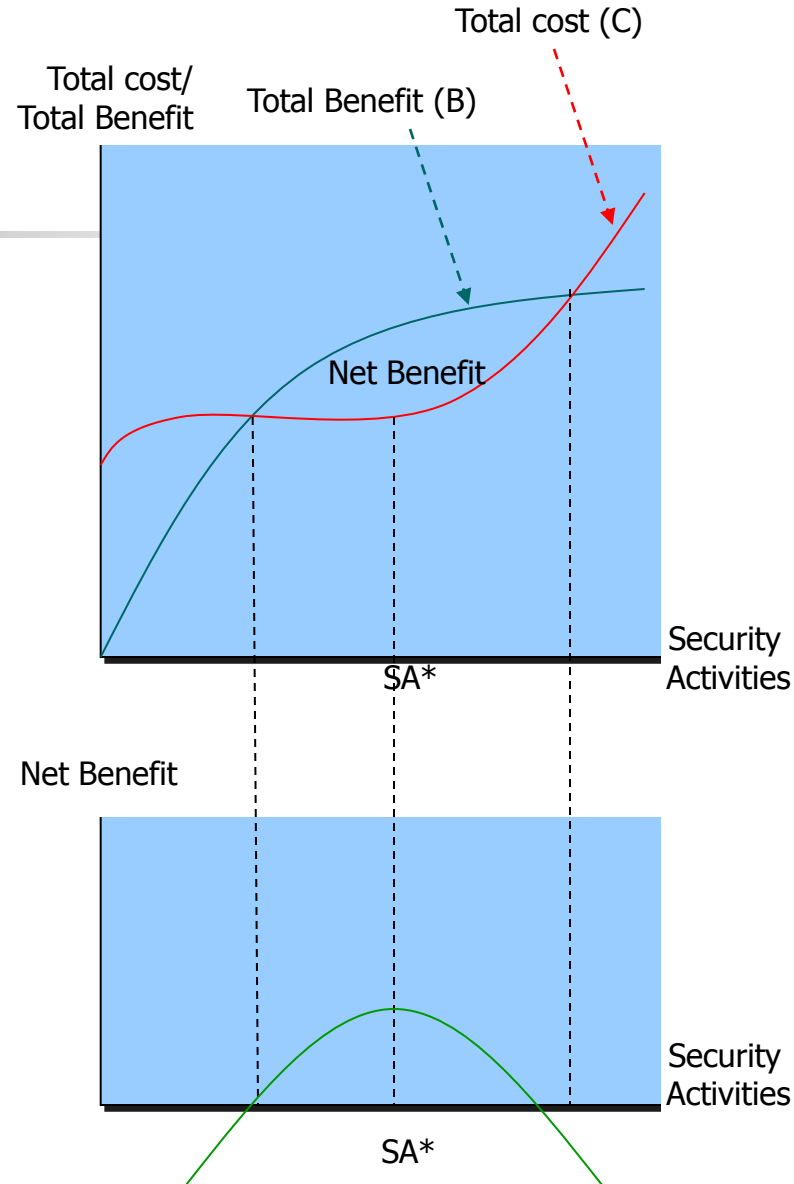
Cost (C) vs. Benefit (B)

- Cost-Benefit principle
 - Keep increasing security activities as long as the incremental benefits exceed their incremental costs
- If security activities can be increased in small amounts
 - Such activities should be set at the point where the incremental (cost = benefit)

Cost vs Benefit

- Security activities are increasing at decreasing rate
 - There are diminishing associated marginal benefits
- Can assume that C has
 - Fixed portion (irrespective of levels of activities)
 - Variable portion (varies with the level of activities)
 - Assume to initially increase at decreasing rate and then increase at increasing rate

Would increase security activities till SA^*





Net Present Value Model

- C and B can be quantified in terms of **Net Present Value (NPV)**
- NPV
 - Financial tool for comparing anticipated benefits and costs over different time periods
 - Good way to put CBA into practice



Net Present Value Model

- To compute NPV,
 - First discount all anticipated benefits and costs to today's value or **present value** (PV)
 - $NPV = PV - \text{Initial cost of the project}$
- Key aspect of NPV model
 - Compare the discounted cash flows associated with the future benefits and costs to the initial cost of an investment
 - All costs are in monetary unit



Net Present Value Model

$$NPV = -C_o + \sum_{t=1}^n (B_t - C_t) / (1 + k)^t$$

- C_o :
 - Cost of initial investment
- B_t and C_t :
 - anticipated benefits and costs, resp., in time period t from the additional security activities
- k :
 - Discount rate, which is usually considered an organization's cost of capital
 - It indicates the minimum rate a project needs to earn in order that the organization's value will not be reduced
- NPV model is most easily considered in terms of incremental investments
- Realistic situation is
 - Some level of security is already in place (e.g., basic firewalls, access controls)
 - It can be used to compare the incremental costs with incremental benefits associated with increases in SA



Net Present Value Model

- NPV greater than zero
 - Accept the incremental security activities
- NPV less than zero
 - Reject the incremental security activities
- NPV = zero
 - Indifference
- k can be used to model risk

Internal Rate of Return (IRR) Model

- Also known as economic rate of return
- *IRR*: Is the discount rate that makes the NVP = zero, thus:
- Decision
 - $IRR > k$, accept the SA
 - $IRR < k$, reject
 - $IRR = k$, indifference
- To select security investments
 - NVP ranking is preferred than IRR ranking

$$C_o = \sum_{t=1}^n (B_t - C_t) / (1 + IRR)^t$$



Must-do Projects

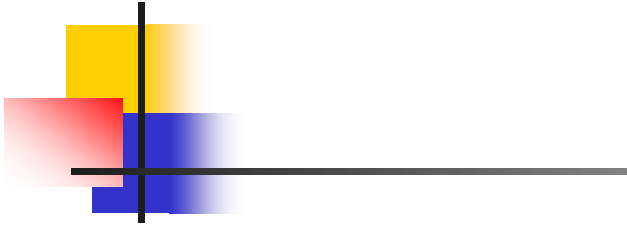
- Some SA are required by law and hence must be done
 - Irrespective of IRR/NVP
- Example
 - HIPAA compliance requirements
 - Safeguards must be in place to provide authorized access to patient information
 - Many outsource SA



Example 1

- Organization wants a new IDS
 - Initial investment is \$200,000
 - Beginning of the first period
 - Expected to have a two-year useful life
 - Annual increment benefits generated from the investment is estimated = \$400,000
 - Annual incremental operating cost for the system is estimated to be \$100,000.
 - Discount rate: 15%

Example 1



What happens if useful life is one year?

A.

Net Present Value (discount rate = 15%)

	C_0	t_1	t_2
Initial investment	-\$200,000		
Annual benefits (i.e., cost savings)		\$400,000	\$400,000
Annual operating costs		<u>-\$100,000</u>	<u>-\$100,000</u>
Net cash flow	-\$200,000	\$300,000	\$300,000
NPV	=	$-\$200,000 + \frac{\$300,000}{(1.15)^1}$	$\frac{\$300,000}{(1.15)^2}$
NPV	=	-\$200,000 +	\$260,870 + \$226,843
NPV = \$287,713			

B.

Internal Rate of Return

	C_0	t_1	t_2
	0	=	$-\$200,000 + \frac{\$300,000}{1 + \text{IRR}} + \frac{\$300,000}{(1 + \text{IRR})^2}$
	$\$200,000 =$	$\frac{\$300,000}{1 + \text{IRR}}$	$+ \frac{\$300,000}{(1 + \text{IRR})^2}$
IRR = 118.61%			

Example 1

A.

Net Present Value (discount rate = 15%)

	C_0	t_1
Initial investment	-\$200,000	
Annual benefits (i.e., cost savings)		\$400,000
Annual operating costs		<u>-\$100,000</u>
Net cash flow	-\$200,000	\$300,000

$$\text{NPV} = -\$200,000 + \frac{\$300,000}{(1.15)^1}$$

$$\text{NPV} = -\$200,000 + \$260,870$$

$$\text{NPV} = \$60,870$$

B.

Internal Rate of Return

	C_0	t_1
	$0 = -\$200,000 +$	$\frac{\$300,000}{1 + \text{IRR}}$

$$\$200,000 = \frac{\$300,000}{1 + \text{IRR}}$$

$$\text{IRR} = 50.00\%$$



Example 2

- Initial investment is \$280,000
 - Beginning of the first period
- Expected to have a two-year useful life
- Annual increment benefits generated from the investment is estimated = \$400,000
- Annual incremental operating cost for the system is estimated to be \$100,000.
- Discount rate: 15%

Example 2

What happens if
useful life is one
year?

A.

Net Present Value (discount rate = 15%)

	C_0	t_1	t_2
Initial investment	-\$280,000		
Annual benefits (i.e., cost savings)		\$400,000	\$400,000
Annual operating costs		<u>-\$100,000</u>	<u>-\$100,000</u>
Net cash flow	-\$280,000	\$300,000	\$300,000
NPV	= -\$280,000	$\frac{\$300,000}{(1.15)^1}$	$\frac{\$300,000}{(1.15)^2}$
NPV	= -\$280,000 +	\$260,870 +	\$226,843
NPV = \$207,713			

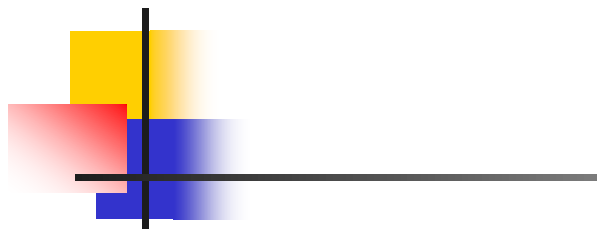
B.

Internal Rate of Return

	C_0	t_1	t_2
	0 = -\$280,000 +	$\frac{\$300,000}{1 + \text{IRR}}$ +	$\frac{\$300,000}{(1 + \text{IRR})^2}$
$\$280,000 = \frac{\$300,000}{1 + \text{IRR}} + \frac{\$300,000}{(1 + \text{IRR})^2}$			

IRR = 70.12%

Example 2



A.

Net Present Value (discount rate = 15%)

	C_0	t_1
Initial investment	-\$280,000	
Annual benefits (i.e., cost savings)		\$400,000
Annual operating costs		<u>-\$100,000</u>
Net cash flow	-\$280,000	\$300,000

$$\text{NPV} = -\$280,000 + \frac{\$300,000}{(1.15)^1}$$

$$\text{NPV} = -\$280,000 + \$260,870$$

$$\text{NPV} = -\$19,130$$

B.

Internal Rate of Return

	C_0	t_1
$0 = -\$280,000 + \frac{\$300,000}{1 + \text{IRR}}$		

$$\$280,000 = \frac{\$300,000}{1 + \text{IRR}}$$

$$\text{IRR} = 7.14\%$$

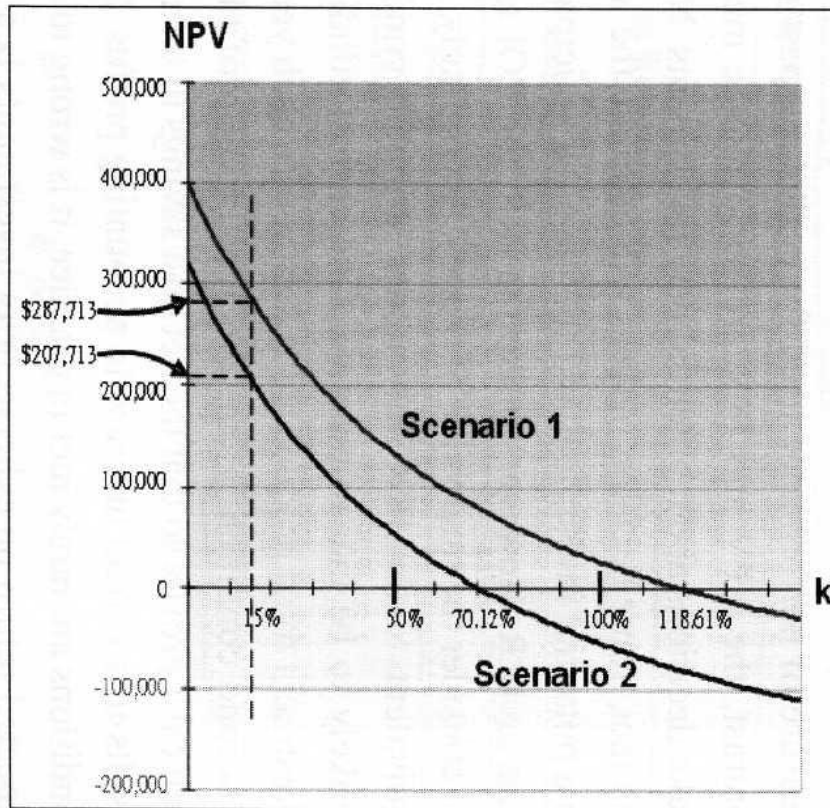


More on k

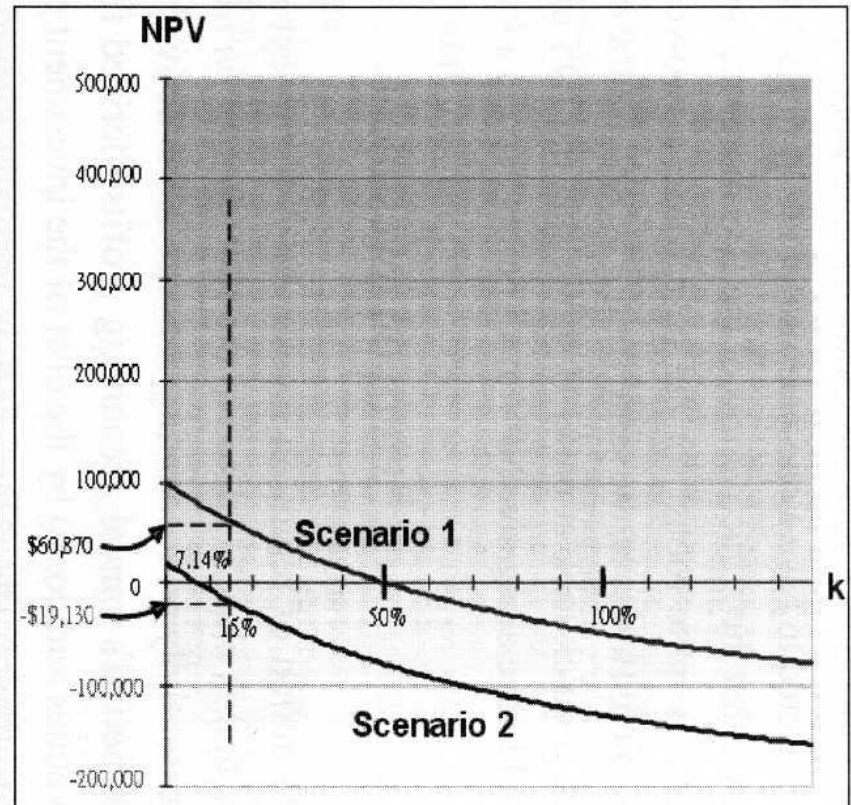
- Higher k means lower NVP
 - Attractiveness of SA will be related to k
- Most corporations use
 - weighted-average cost of capital (WC) in discounting future cash flows
 - For risky projects, some premiums may be added
 - E.g., WC = 15 and k = 20

Example 1 and 2

A. Two-year Useful Life



B. One-year Useful Life





Return on Investment

- ROI is essentially
 - Last period's annual profits
divided by
 - cost of the investment required to generate the profit
- ROI viewed as
 - Historical measure of performance used for evaluating past investments
- NPV & IRR
 - Performance measures used to make decisions about potential new investments
 - Unlike IRR, ROI technically does not consider time value of money

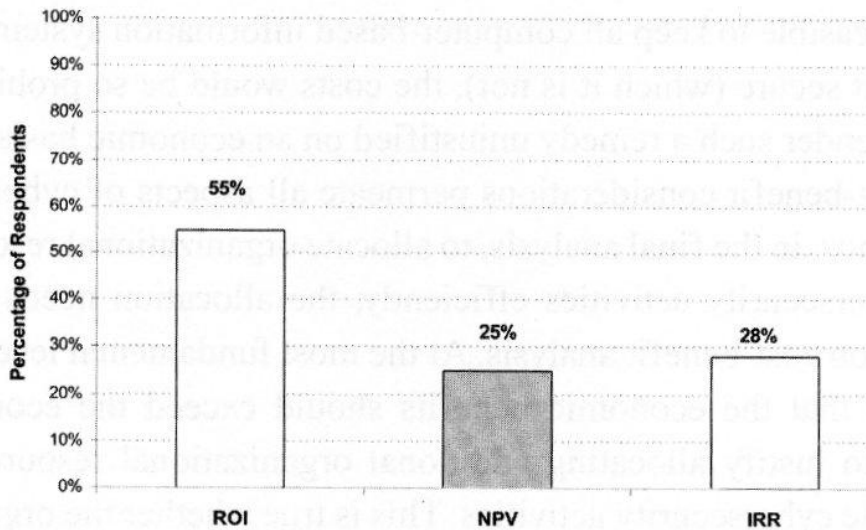


Return on Investment

- ROIs for the two examples
 - Example 1: $300\text{K}/200\text{K} * 100\% = 150\%$
 - Example 2: $300\text{K}/280\text{K} * 100\% = 107\%$
- ROI assumes that
 - The investment will continue to produce returns of \$300 for year 2, 3, 4 & beyond
 - Dramatically overstates the economic rate of return.
 - The more that the returns persist, the better the ROI is an approximation of the IRR
 - If 300K net benefit could go on forever, the ROI = IRR
- Survey shows,
 - Many managers are using ROI acronyms to represent IRR

Survey

Percentage of Organizations Using ROI, NPV, and IRR Metrics



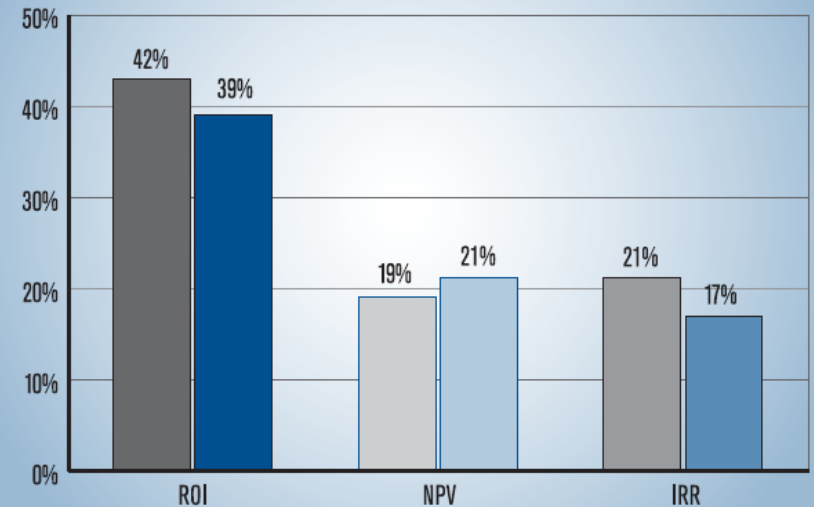
ROI = return on investment

NPV = net present value

IRR = internal rate of return

Figure 8. Percentage of Organizations Using ROI, NPV and IRR Metrics

(2007 figures in blue, 2006 figures in gray.)



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 314 Respondents