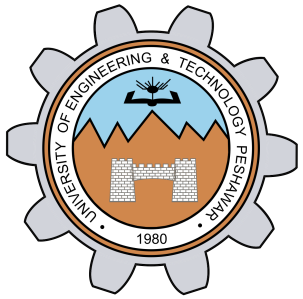
Computer Security

Lecture 13: Security Policies/Mechanisms and Risk Management

Prof. Dr. Sadeeq Jan

Department of Computer Systems Engineering

University of Engineering and Technology Peshawar



Lecture Outline

- IT Security Management
- IT Security Management Process
- PDCA Cycle
- Polices and Mechanisms
- Objective of Polices
- Why Policy?
- Bulls-Eye Model
- Types of Information Security Policy
- Trust and Assumptions
- Assurance
- Operational & Human Issues
- Policy, Standards, and Practices
- Risk
- Risk Analysis
- Risk Management vs. Cost of Security
- CIA Risk and Control
- Security as Risk Management
- Risk Identification and assessment
- Risk Control
- Risk Communication / Documenting Results
- Security Through Obscurity (STO)

Overview

- Security requirements means asking
  - what assets do we need to protect?
  - how are those assets threatened?
  - what can we do to counter those threats?
- IT security management answers these
  - determining security objectives and risk profile
  - perform security risk assessment of assets
  - select, implement, monitor controls

IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the site/system/*etc*.
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

Policies and Mechanisms (Cont'd)

- **Policy:** may be expressed in
  - natural language, which is usually imprecise but easy to understand;
  - mathematics, which is usually precise but hard to understand;
  - policy languages, which look like some form of programming language and try to balance precision with ease of understanding
- **Mechanisms:** may be
  - technical, in which controls in the computer enforce the policy; for example, the requirement that a user supply a password to authenticate herself before using the computer
  - procedural, in which controls outside the system enforce the policy; for example, firing someone for ringing in a disk containing a game program obtained from an untrusted source
- *The composition problem requires checking for inconsistencies among policies. If, for example, one policy allows students and faculty access to all data, and the other allows only faculty access to all the data, then they must be resolved*

Objective of Policies

REDUCED RISK

COMPLIANCE WITH LAWS AND REGULATIONS

ASSURANCE OF OPERATIONAL CONTINUITY, INFORMATION INTEGRITY, AND CONFIDENTIALITY

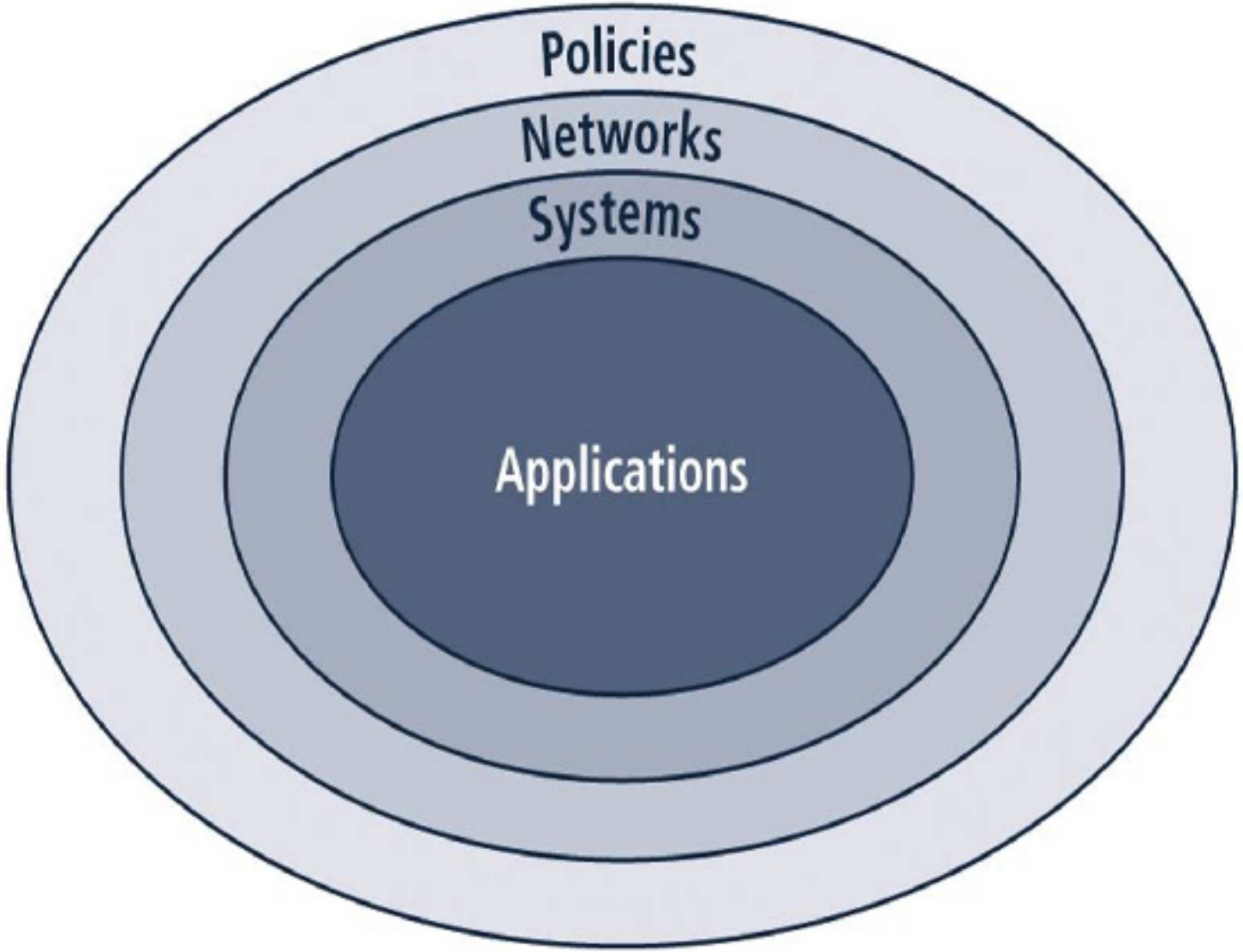
Why Policies?

Policies are the least expensive means of control and often the most difficult to implement

Basic rules for shaping a policy

- ✓ Policy should never conflict with law
- ✓ Policy must be able to stand up in court if challenged
- ✓ Policy must be properly supported and administered

Bulls-Eye Model



Types of Information Security Policy

- Enterprise information security program policy
- Issue-specific information security policies
- Systems-specific policies

Types of Information Security Policy (Cont'd)

- **Enterprise information security program policy**

  Describes the whole organization's security objectives and its commitment to information security. It can be thought of as the primary document from which other security policies are derived. Also, it often informs the organization's compliance goals.

Types of Information Security Policy (Cont'd)

- **Issue-specific information security policies**

  Provide guidelines for particular threats or categories of threats.

  For example, an organization may create a security policy that focuses on phishing attacks or general email security.

Types of Information Security Policy (Cont'd)

- **Systems-specific policies**

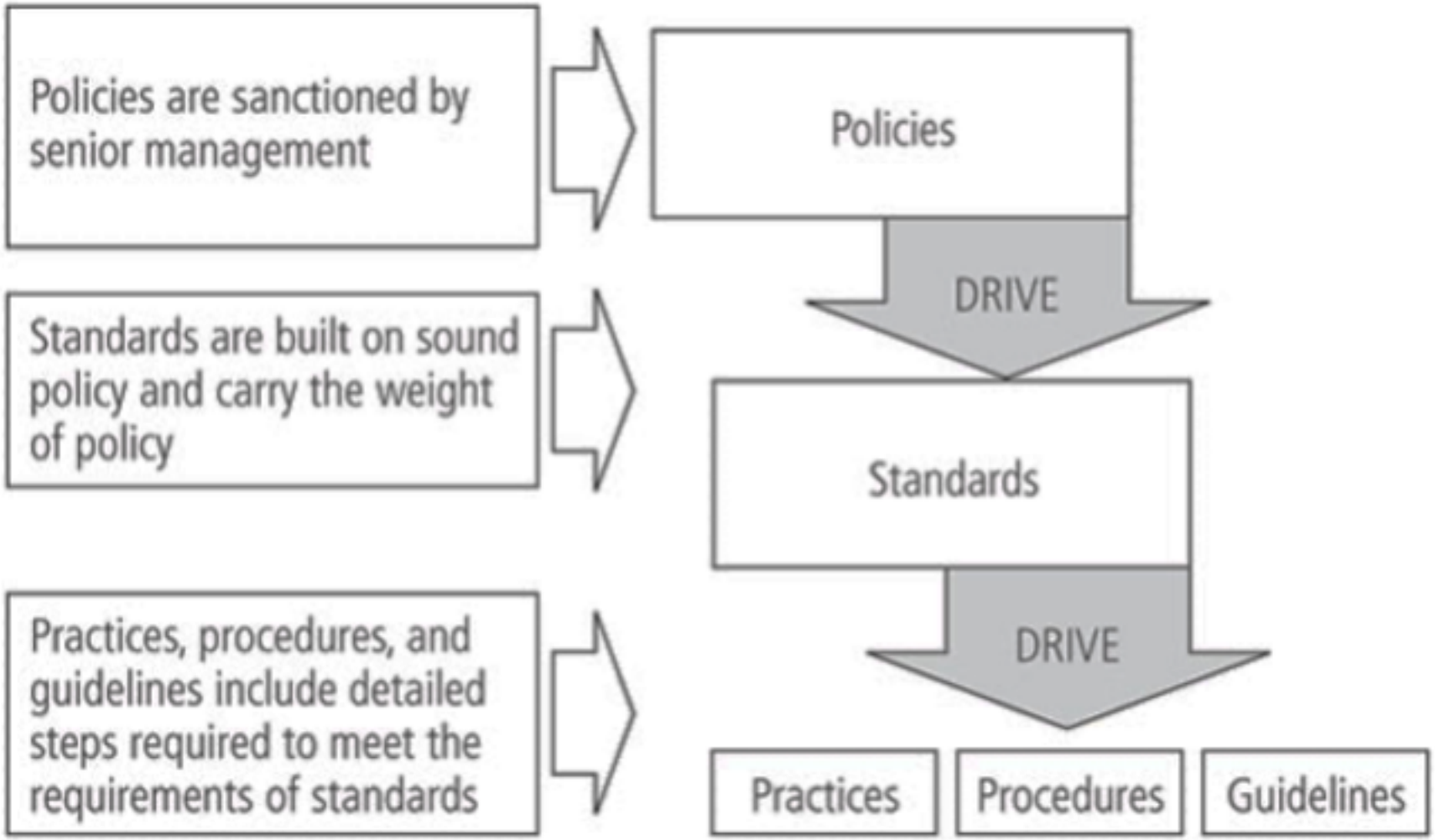
A system-specific security policy is concerned with specific systems or types of system. It describes hardware and software approved for that system and how that system is to be protected.

For example, policies for customer-facing applications, payroll systems, or data archive systems. They typically articulate security objectives and the operational security rules intended to support them.

Policy, Standards, and Practices (Cont'd)

- **Policy:** A plan or course of action that influences decisions
  - must be properly disseminated, read, understood, agreed-to, and uniformly enforced
  - require constant modification and maintenance
- **Standards**
  - A more detailed statement of what must be done to comply with policy
- **Practices**
  - Procedures and guidelines explain how employees will comply with policy

Policy, Standards, and Practices



Seven Elements of an Effective Security Policy

1. Clear purpose and objectives

2. Scope and applicability

3. Commitment from senior management

4. Realistic and enforceable policies

6. Tailored to the organization's risk appetite

5. Clear definitions of important terms

7. Up-to-date information

Security Policy examples

Program or organizational policy

Acceptable use policy

Remote access policy

Data security policy

Firewall policy

Email policy

Trust

- Tools of computer security are resident on computers
- Just as mutable as any other information on computers
- Can we trust our computer?
- Can we trust our software?
- Can we trust our suppliers?
- Can we trust our people?
- Trust, but verify

Trusting Our Computer

- Hardware bugs
- Hardware features
- Peripheral bugs/features

Trusting Our Software

- Operating system bugs and features
- System software back-doors
- Who wrote the software?
- Who maintains the software?

Trusting Our Suppliers

- Development process
- Bugs
- Testing
- Configuration control
- Distribution control
- Hacker challenges

Trust, but Verify

- Trust with a suspicious attitude
- Ask questions
- Do background checks
- Test code
- Get written assurances
- Anticipate problems and attacks

Trust and Assumptions

Underlie *all* aspects of security

Policies

- Unambiguously partition system states
- Correctly capture security requirements

Mechanisms

- Assumed to enforce policy
- Support mechanisms work correctly

Example of lock picker

Assurance

- **Assurance** is a measure of how well the system meets its requirements; more informally, how much you can trust the system to do what it is supposed to do. It does not say what the system is to do; rather, it only covers how well the system does it
- System specification, design, and implementation can provide a basis for determining "how much" to trust a system
- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

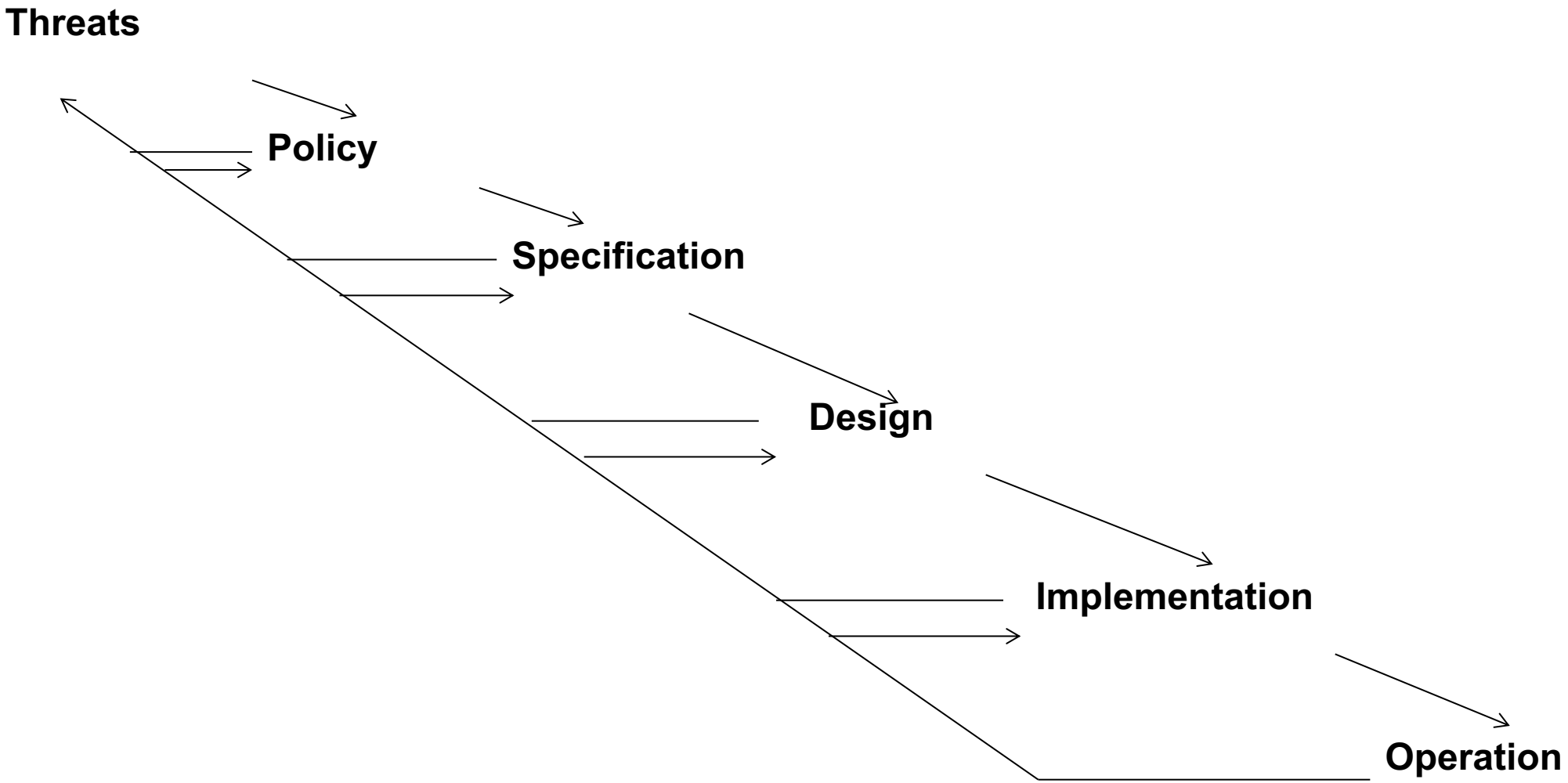
Operational Issues

- Security does not end when the system is completed. Its operation affects security
  - Cost-Benefit Analysis
    - Is it cheaper to prevent or recover?
  - Risk Analysis
    - Should we protect something?
    - How much should we protect this thing?
  - Laws and Customs
    - Are desired security measures illegal?
    - Will people do them?

Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits (security does not bring in revenue, it merely prevents the loss of revenue)
- People problems
  - Heart of any security system is people
  - Outsiders and insiders
  - Social Engineering

Tying Together



Risk

- The possibility that a particular vulnerability will be exploited
- IT-related risks arise from:
  - Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
  - Unintentional errors or omissions
  - IT disruptions due to natural or man-made disasters
  - Failure to exercise due care and diligence in implementation and operation of the IT system

Risk = Threat * Vulnerability (* Impact)

Risk Analysis

- Identification, assessment and reduction of risks to an acceptable level
- The process of identifying security risks and probability of occurrence, determining their impact, and identifying areas that require protection
- Three parts:
  - Risk assessment – determine the possible risks
  - Risk management – evaluating alternatives for mitigating the risk
  - Risk communication – presenting the material in an understandable way to decision makers and/or the public

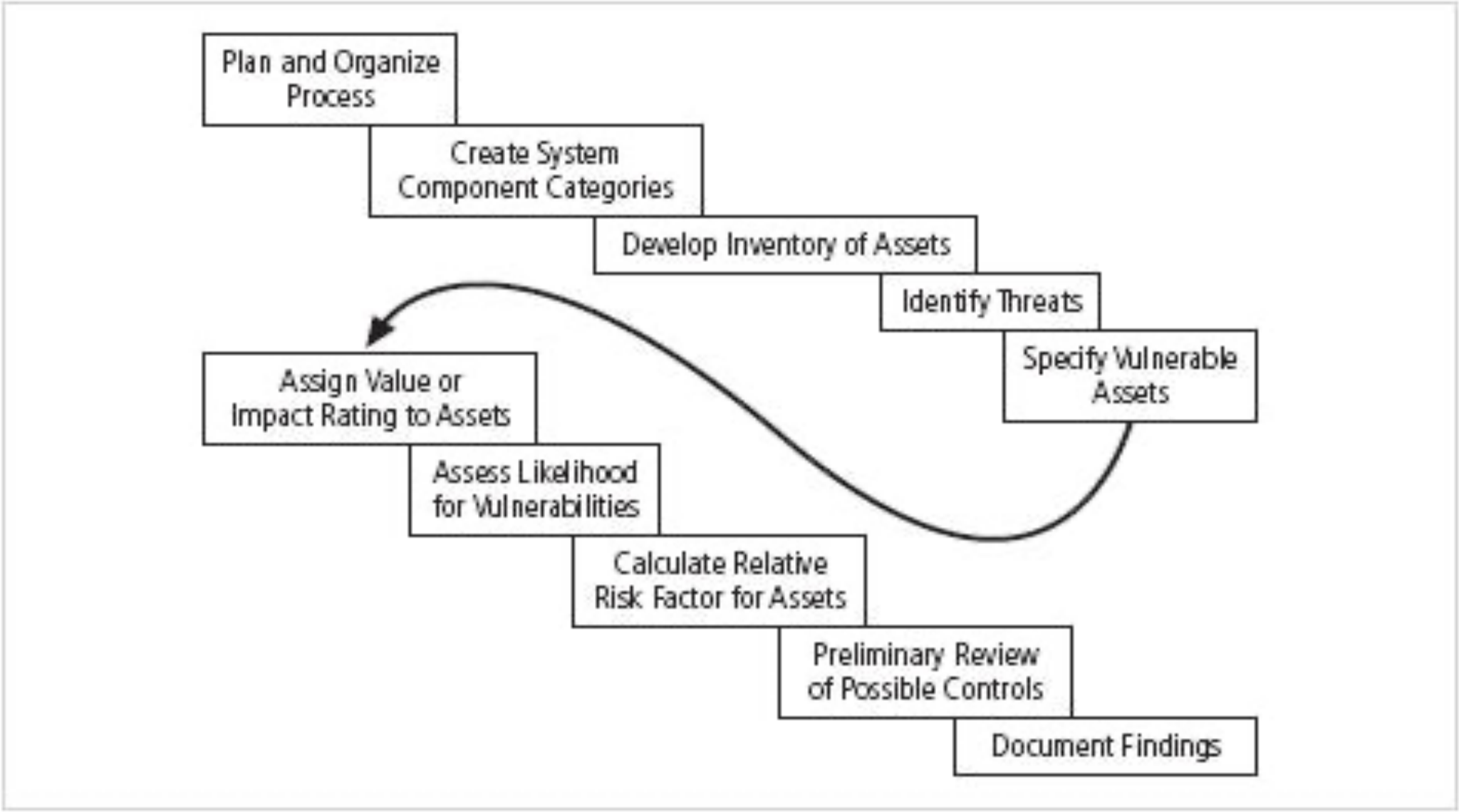
Risk Management vs. Cost of Security

- **Risk mitigation**
  - The process of selecting appropriate controls to reduce risk to an acceptable level
- The level of acceptable risk
  - Determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy
- Trade-offs between safety, cost, and availability

Risk Management

- Managing a risk is one of the key responsibilities of every manager within the organization
- In any well-developed security risk management program, two formal processes are at work:
  - Risk identification and assessment
  - Risk control

Risk Identification Process



Organizational Assets Used in Systems

IT system components	Risk management components	
People	People inside an organization People outside an organization	Trusted employees Other staff People at organizations we trust 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 component	Intranet components Internet or Extranet components

Assessing Values for Information Assets

- As each information asset is identified, categorized, and classified, assign a relative value
- Relative values are comparative judgments made to ensure that the most valuable information assets are given the highest priority, for example:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the highest profitability?
  - Which information asset is the most expensive to replace?
  - Which information asset is the most expensive to protect?
  - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

Sample Asset Classification Worksheet

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
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-maill (inbound)	Private	Medium
DMZ Assets:		
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 Example

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)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Deviations in quality of service by service provides	Power and WAN quality of service issues from service providers
Forces of nature	Fire, flood, earthquake, lightning
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Source: ©2003 ACM, inc., included here by permission.

Vulnerability Assessment

- Vulnerability---weakness of system
- Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat
- This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization
- **Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset**

Risk Identification Estimate Factors

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

Access Controls

- Access controls specifically address admission of a user into a trusted area of the organization
- These areas can include information systems, physically restricted areas such as computer rooms, and even the organization in its entirety
- Access controls usually consist of a combination of policies, programs, and technologies

Risk Control Strategies

- An organization must choose one of 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 should the vulnerability be exploited
  - **Acceptance**: understanding the consequences and accepting the risk without control or mitigation

CIA Risk and Control

CIA	RISK	CONTROL
Confidentiality	Loss of privacy, Unauthorized access to information, Identity theft.	Encryption, Authentication, Access Control
Integrity	Information is no longer reliable or accurate, Fraud.	Maker/Checker, Quality Assurance, Audit Logs
Availability	Business disruption, Loss of customer's confidence, Loss of revenue.	Plans and test, Backup storage, Sufficient capacity.

Risk and Its Protection by Implementing CIA

END