# Information Security Governance and Risk Management

## Domain 3

# Overview

**The information security governance and risk management domain entails the identification of an organization's information assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability.**

# Key Areas of Knowledge

**A. Understand and align security function to goals, mission and objectives of the organization**

**B. Understand and apply security governance**

**C. Understand and apply concepts of confidentiality, integrity and availability**

**D. Develop and implement security policy**

**E. Manage the information life cycle**

# Key Areas of Knowledge (continued)

F. Manage third party governance

G. Understand and apply risk management concepts

H. Manage personnel security

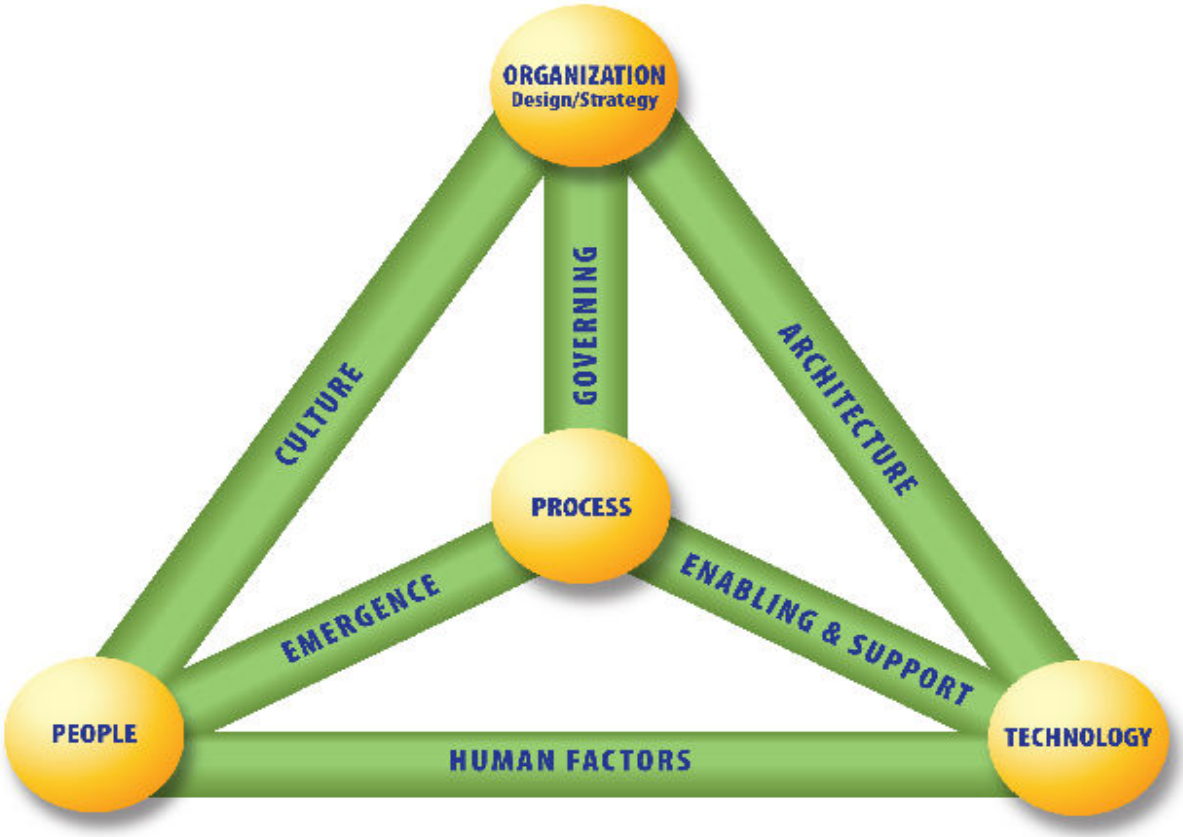
I. Develop and manage security education, training and awareness

J. Manage the security function

# Agenda

- **Understand and align security function to goals, mission and objectives of the organization**
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# Business model for information security



# Business model for information security

The four elements of the model are:

1. Organization Design/Strategy
2. People
3. Process
4. Technology

# Business model for information security

The dynamic interconnections link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium. The six dynamic interconnections of the model are:

1. Governance
2. Culture
3. Enablement & Support
4. Emergence
5. Human Factors
6. Architecture

# Business Case for Information Security

- Information security management practices protect the assets of the organization through the implementation of physical, administrative, managerial, technical, and operational controls.

- Information security management ensures that appropriate policies, procedures, standards and guidelines are implemented to provide the proper balance of security controls with business operations.

- The security professionals who lead the information security program are relied upon for their knowledge of security and risk management principles.

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- **Understand and apply security governance**
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# Security Governance

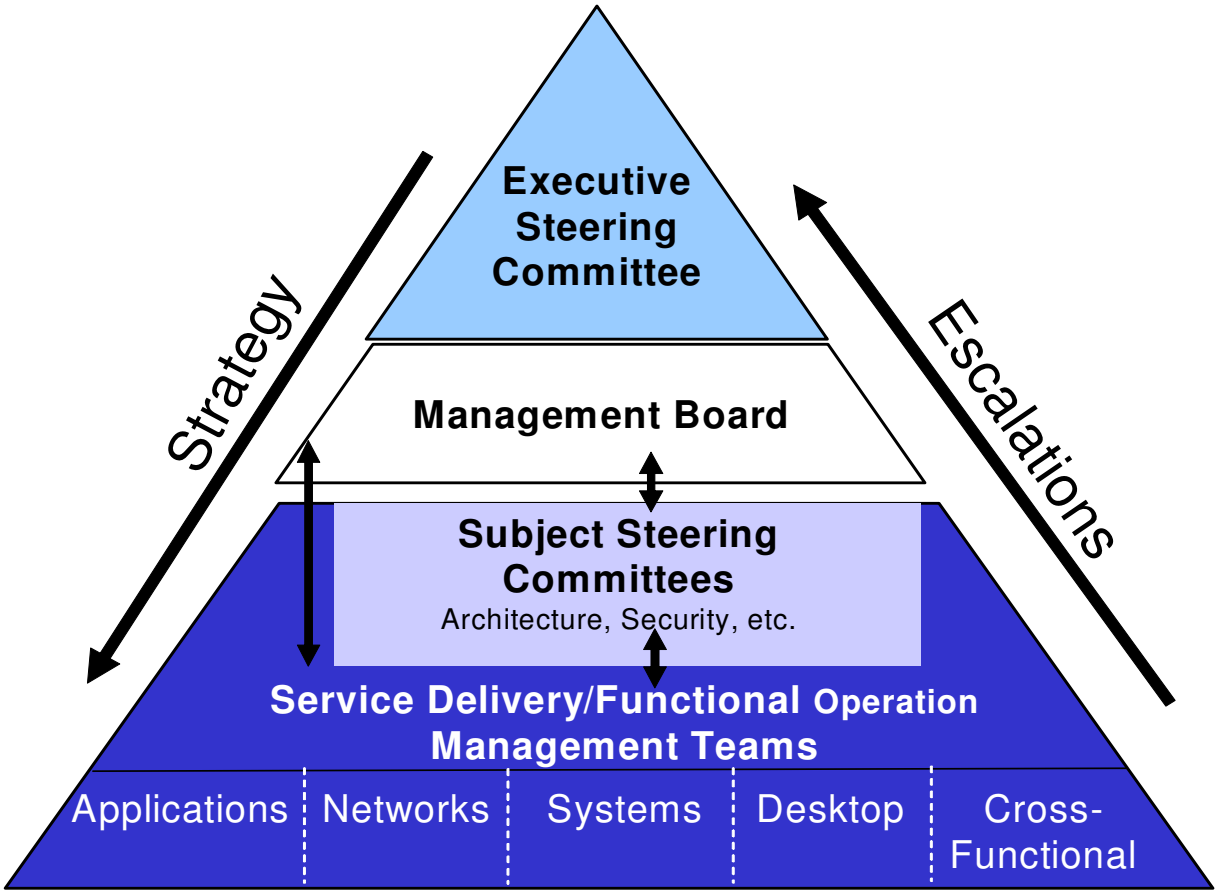
**Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.**

# Security Governance (continued)

## Information Security Governance

- Subset of corporate governance
- Provides strategic direction for security activities
- Ensures that objectives are achieved
- Ensures that information security risks are appropriately managed
- Ensures that enterprise information resources are used responsibly

# Integrated Information Security Governance



# Legislative and Regulatory compliance

Sarbanes-Oxley – Under Section 404, management is required to produce an “internal control report.” To do this, managers are generally adopting an internal control framework such as that described in COSO.

Gramm-Leach Bliley – compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

# Control Framework

## A TOOL for Communication and Security Management

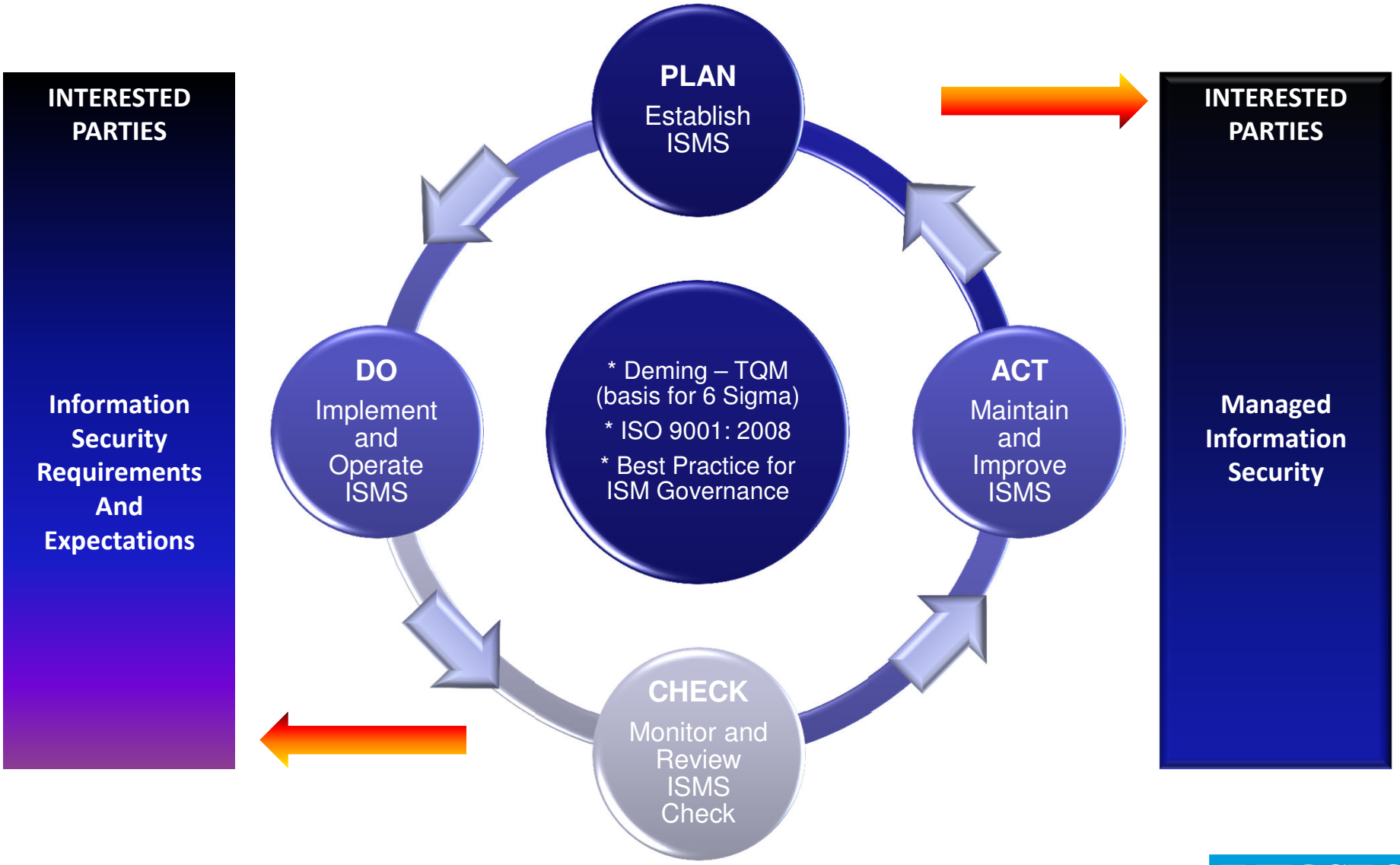
- **A framework for all administrative, technical, and physical controls**


- **A framework allows a company to apply different procedures and technologies to achieve its goals**

# Control Frameworks and Methodologies

- **Committee of Sponsoring Organizations (COSO)**
  - Emphasis on identifying and managing risks
- **IT Infrastructure Library (ITIL®)**
  - Emphasis on IT services and IT service management
  - Can be used as a complement to COBIT
- **Control Objectives for Information and related Technology (COBIT®)**
  - Acts as a model for IT Governance and focuses more on operational goals and regulatory compliance
- **ISO/IEC 27000 Series**

# The Plan Do Check Act (PDCA) Model - CobiT



# CobiT

- **Control Objectives for Information and related Technology (CobiT)**
- **Focuses on IT related processes and provides a security management lifecycle**
- **A process model that subdivides IT into four domains**
  - Plan and Organize
  - Acquire and implement
  - Deliver and support
  - Monitor and evaluate
- **These four domains are further subdivided into 34 processes**

# ISO/IEC 27000 Series

- **International Organization for Standardization**
- **International Electro-technical Commission**
- **Joint Technical Committee**
  - ISO/IEC JTC 1
  - Subcommittee SC 27, IT Security techniques
- **Includes International Standards:**
  - ISO 27000 – Glossary of Terms
  - ISO 27001 – IS Management Systems (ISMS) Requirements
  - ISO 27002 – Code of IS Practice
    - (P.K.A. BS 7799 & ISO 17799)
  - ISO 27005 – IS Risk Management (ISRM)
  - ISO 27799 – IS for Health Care Organizations

# ISO/IEC 27001 Controls

- Physical and Environmental Security
- Human Resources Security
- Organizing Information Security
- Asset Management
- Communications and Operations Management
- Information Security Incident Management
- Business Continuity Management
- Security Policy
- Access Control
- Compliance
- Information Systems Acquisition, Development, and Maintenance

# Goals of the Model – Planning Horizon

- **Strategic Goals**
  - Over-arching - supported by tactical goals and operational
- **Tactical Goals**
  - Mid-Term - lay the necessary foundation to accomplish Strategic Goals
- **Operational Goals**
  - Day-to-day - focus on productivity and task-oriented activities

# Due Care and Due Diligence

## Due Care

- Do the right thing to protect assets
- Functional requirements

## Due Diligence

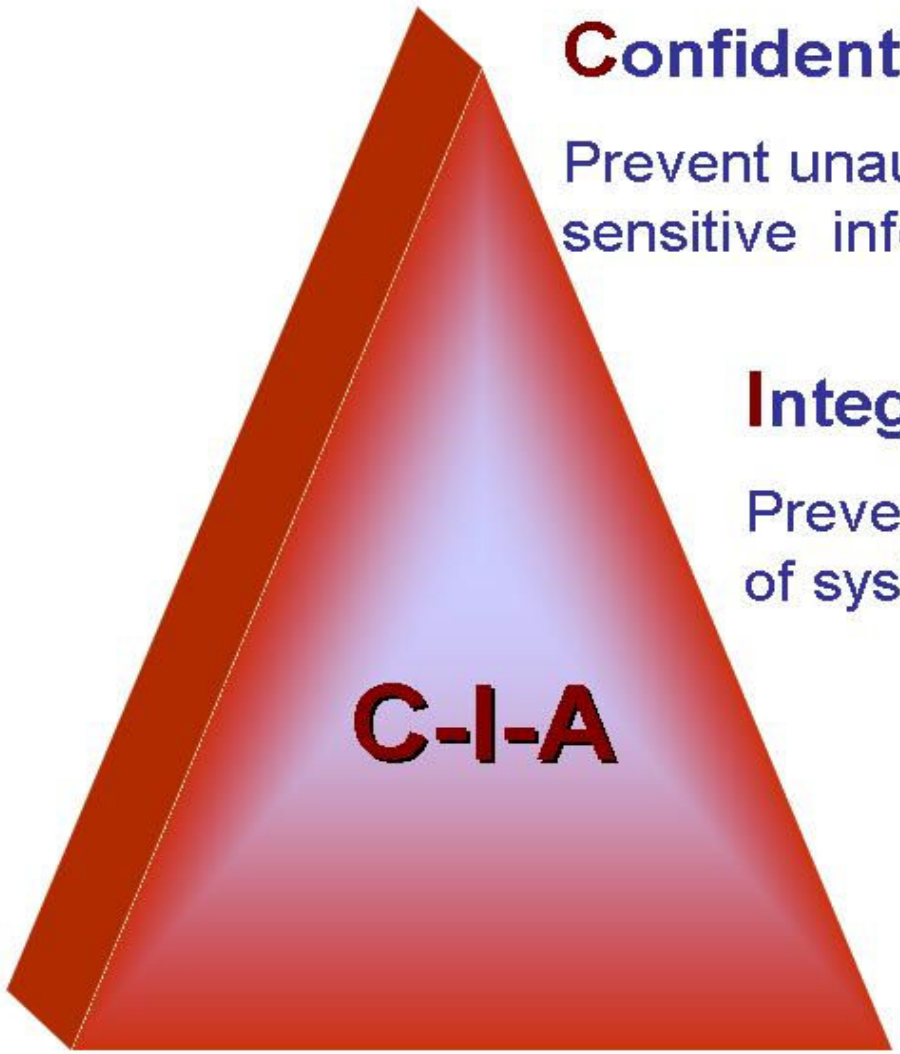
- To investigate actual threats and risks
- Assurance requirements

***This is how liability is determined***

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- **Understand and apply concepts of confidentiality, integrity and availability**
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# “The Center of (ISC)$^2$’s CBK”: C-I-A Triad




**Confidentiality**

Prevent unauthorized disclosure of sensitive information

**Integrity**

Prevent unauthorized modification of systems and information

**Availability**

Prevent disruption of service and productivity

# Confidentiality (opposite: disclosure)

- Only authorized individuals, processes, or systems have access to information on a need-to-know basis.

- This level of access, also known as the principle of least privilege, is at the level necessary for the individual to do their job.

- Confidentiality ensures that the necessary level of security is enforced at each instance of data processing; while the data is at rest and while the data is in transit.

# Integrity (opposite: alteration)

- This principle implies that data should be protected from intentional, unauthorized, and/or accidental changes.

- Controls are put in place to ensure that information is only modified through approved and accepted practices.

- Hardware, software, and communication mechanisms should work in concert to maintain and process data correctly and to move data to intended destinations without unexpected alteration.

# Availability (opposite: destruction)

- Availability ensures reliability and timely access to data and resources to authorized individuals.

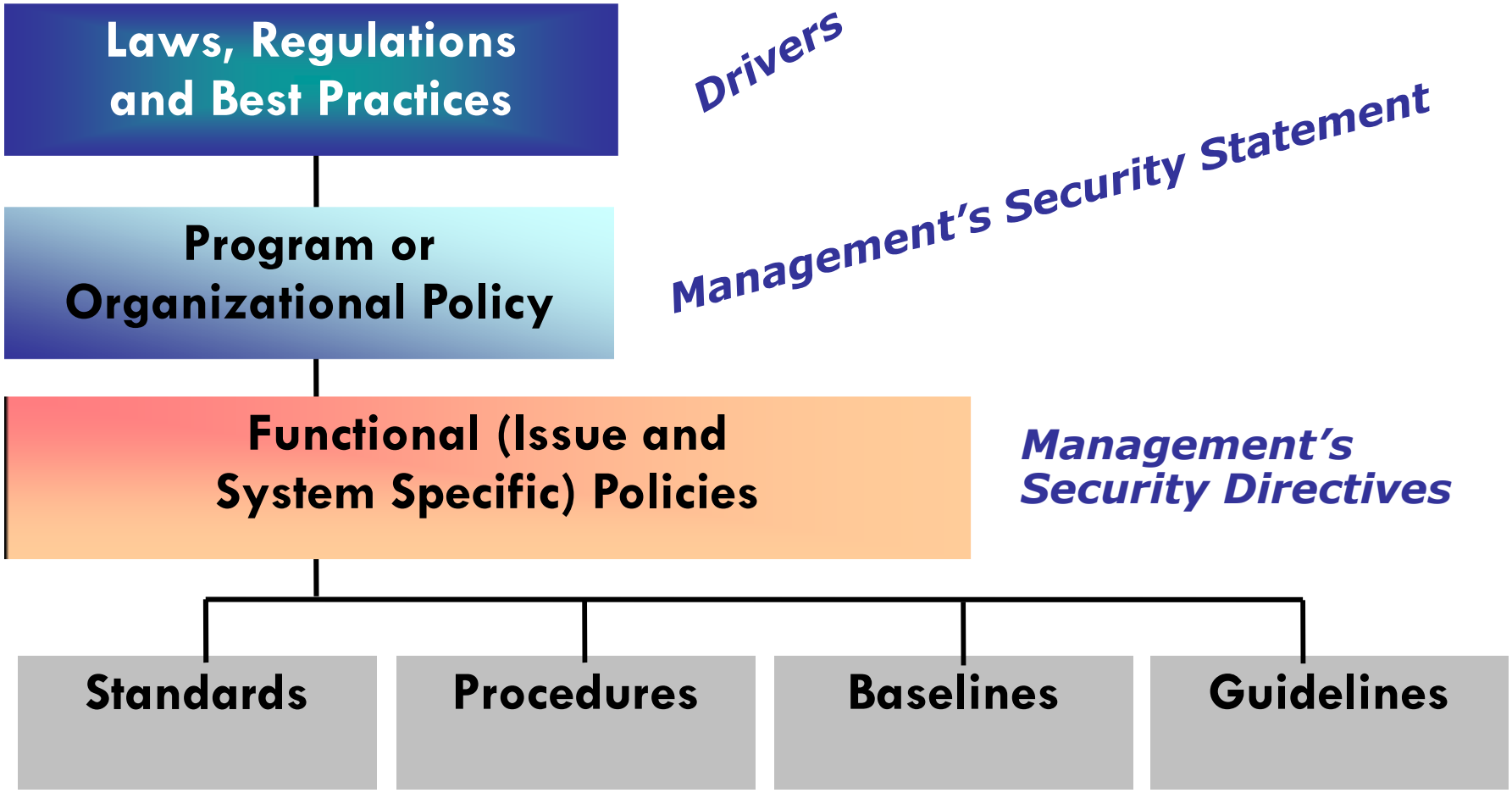
- The two primary areas affecting the availability of systems are (1) denial of service attacks and (2)loss of service due to a disaster.

- Disaster recovery ensures that all or parts of information technology processing systems can be recovered. Disaster recovery and business continuity work together to minimize the impact of critical events

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- **Develop and implement security policy**
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# Security Policy Document Relationships



# NIST SP 800-12: Program Policy

- **Drivers:**
  - Laws
  - Regulations
  - Liabilities
- **Senior Management:**
  - Establishes the computer security program
  - Assigns responsibilities
- **Components:**
  - Compliance Issues
  - Goal
  - Scope

# NIST SP 800-12: Issue-Specific Policies

## Organizational

- Internet Access
- Email Privacy
- AUP

## Basic Components

- Compliance
- Issue Statement
- Position Statement Of Organization
- Applicability
- Roles and Responsibilities
- Points of Contact and Supplementary Information

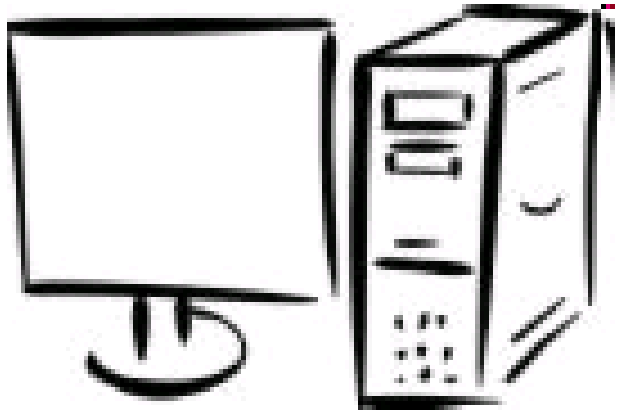
# NIST SP 800-12: System-Specific Policies

## Management Official

- Security Objectives
- Constraints
  - Costs
  - Operational
  - Technical

## Technical Administrators

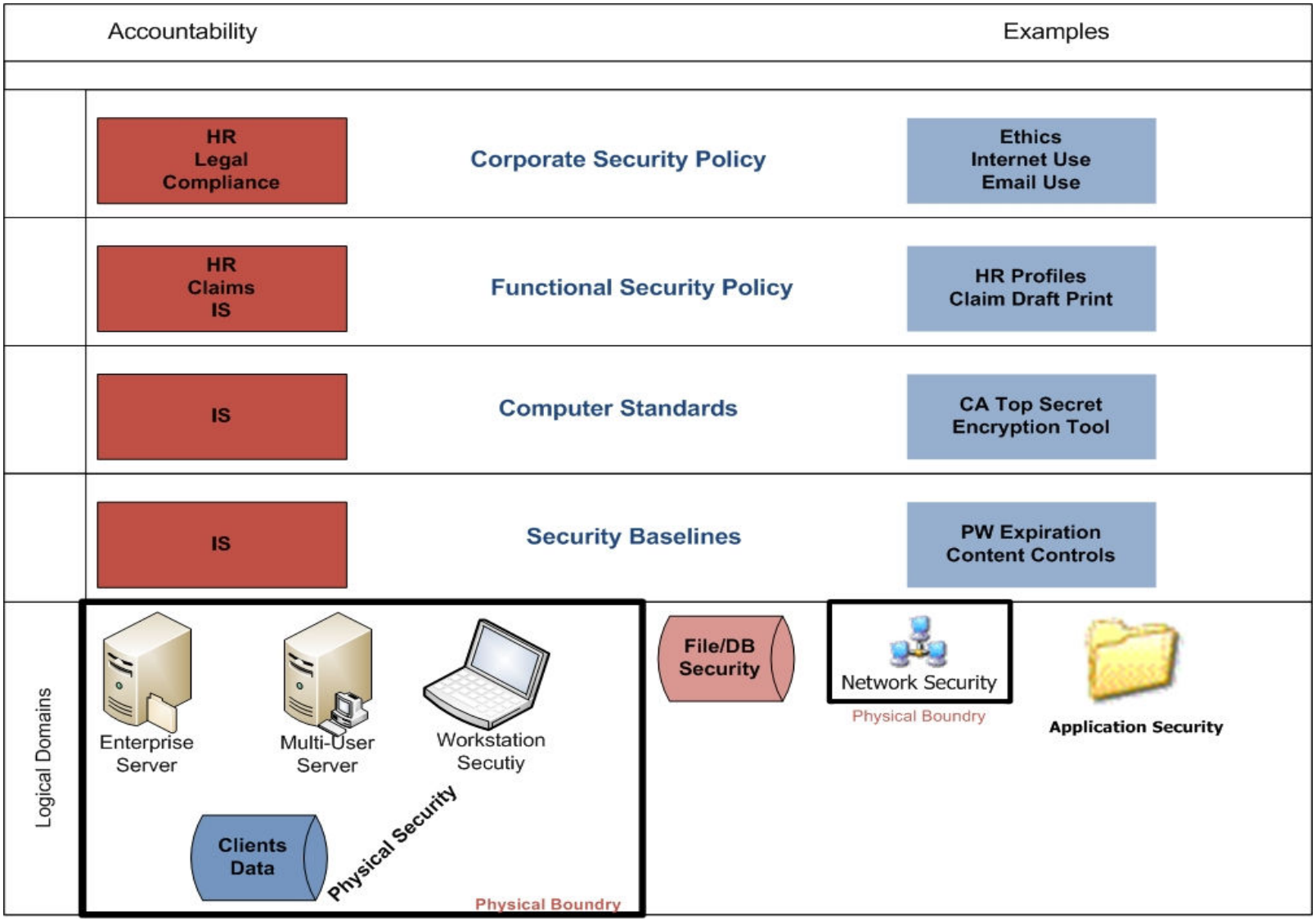
- Operational Security Rules
- Balancing Level of Detail



# Functions for Supporting Policies

- **Standards – binding**
  - Compulsory rules that dictate how hardware and software are to be used and expected behavior of employees
- **Baselines – binding**
  - A minimum level of security that is required throughout the organization
- **Procedures – binding**
  - Detailed step-by-step actions to be taken to achieve a specific task
- **Guidelines – non-binding**
  - Recommended actions and operational guides for users and staff members where standards do not apply

# Support Functions Example



# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- **Manage the information life cycle**
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

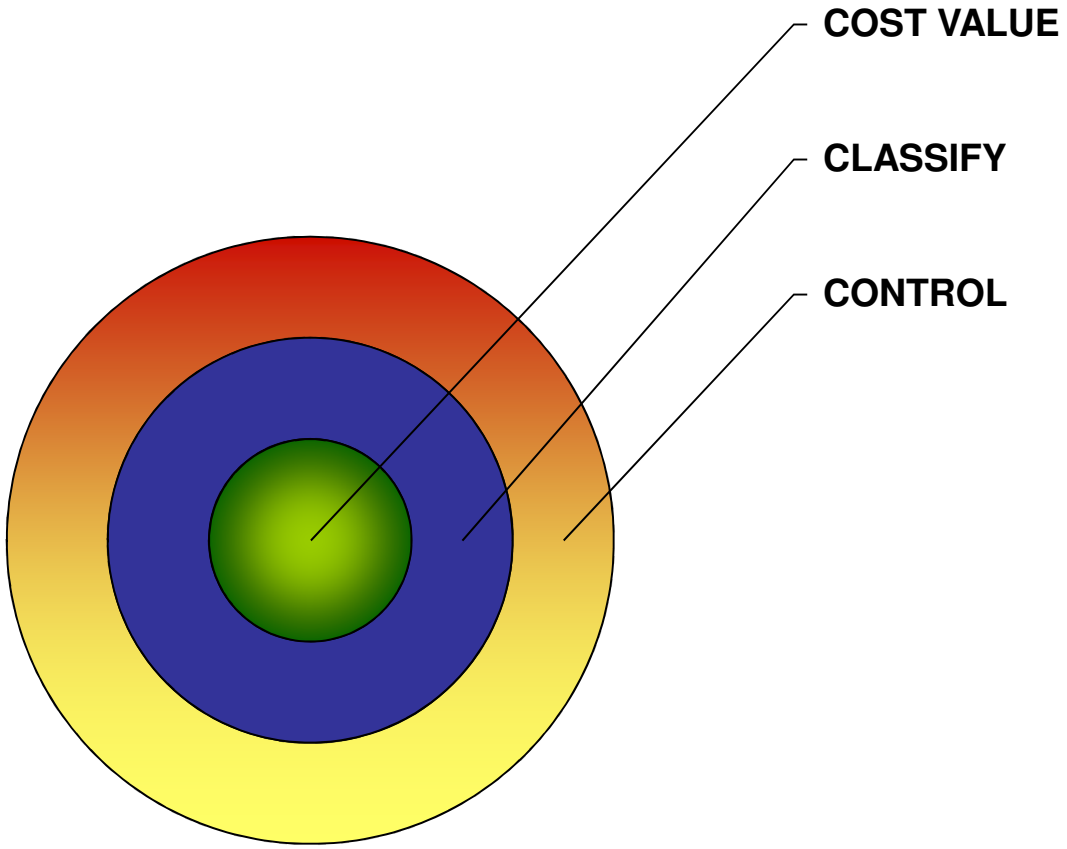
# A$$ET VALUATION: What's the Value?

- Acquisition or Development Costs
- Replacement Costs
- Maintenance and Protection Costs
- Productivity and Operational Losses: if asset is unavailable
- Owner's Value
- Outside/Other's Valuation: price others are willing to pay
- Liability: if the asset is compromised

***Value*: Initial, Internal, External**

# Data Classification Process – 3 Cs

- **Cost Value**
  - Identified during risk analysis
- **Classify**
  - Organize according to sensitivity to loss or disclosure
- **Control**
  - Data is segmented according to sensitivity level
  - Each classification of data should have different security controls



# Classification Types

## Commercial

- Confidential
- Private
- Sensitive
- Public

## Military

- Top secret
- Secret
- Confidential
- Sensitive but unclassified
- Unclassified

**Example: Info may require High level of Integrity and Availability, but no Confidentiality**

# Data Classification Procedure

- Custodian - *identify*
- Classification Criteria - *specify*
- Controls - *per classification*
- Exceptions - *document*
- Transfer Custody - *methods*
- Declassification - *reclassification/termination*
- Awareness - *of security program*

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- **Manage third party governance**
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# Manage third party governance

An important aspect of information security governance is the rules and processes employed when dealing with third-party relationships and may include:

- Service providers
- Outsourced operations
- Trading partners
- Merged or acquired organizations

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- **Understand and apply risk management concepts**
- Manage personnel security
- Develop and manage security education, training and awareness
- Manage the security function

# Risk Management

***The process of identifying, analyzing, and reducing the risk to an acceptable level.***

## Risk Assessment

- **A method of identifying a company's assets, their associated risks, and the potential loss that the organization could suffer.**
- **Detailed estimate of likelihood and impact of particular events.**
- **Suggested countermeasures**

## Risk Mitigation

- **Management selects countermeasures**

## Controls Evaluation

- **Ongoing process**

# Risk Management Models

- ANZ 4360:  Australian-New Zealand's risk management framework
- NIST SP 800-30:  U.S. government's risk management standard
- OCTAVE®  Operationally Critical Threat, Asset, and Vulnerability Evaluations
- Basel II:  Financial risk management framework adopted by the EU as a minimum acceptable standard of practice

# Risk Management Process

# Risk Management – How to Handle?

***Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.***

- **A**sset – Any resource of value to the organization
- **T**hreat – Potential danger (accidental trigger or intentional exploit) to an asset should a threat-agent take advantage of an asset's vulnerability.
- **T**hreat-Source/Threat-Agent – Anything and/or anyone that has the potential to cause a threat.
- **V**ulnerability – A flaw or weakness of an asset

# Identifying Threats and Vulnerabilities

- The risk analysis team must identify the threats and vulnerabilities associated with possible losses:
  - Potential loss
  - Delayed loss
- Some threats are not so easily identified:
  - Buffer overflows
  - Employee fraud
  - Illogical processing

# Possible Threats

- **Confidentiality**
  - Shoulder surfing
  - Interception of a message
  - Social engineering
- **Integrity**
  - Disabling the alert mechanism in an IDS
  - Modifying a message in transmission
  - Changing accounting records or system logs
  - Modifying configuration files
- **Availability**
  - Man-made or natural disaster
  - Failure of components within a device
  - Terrorist attacks
  - Denial of service attacks

# Security/Risk Definitions

- **Risk – Likelihood of a threat agent exploiting a vulnerability**
- **Exposure – An opportunity for a threat to cause loss**
- **Event / Exploit – Instance of loss experienced**
- **Loss – Real or perceived devaluation of an asset**
- **Controls – technical and nontechnical risk mitigation mechanisms**
  - Safeguards – Preventive and deterrent (proactive) controls
  - Countermeasures – Detective and corrective (reactive) controls

# Purpose of Risk Assessment

- Identify company assets and the potential loss for each and every threat recognized

- Ensure that a security program is cost-effective, relevant, and appropriate for the real risks it faces

**IDENTIFY & PRIORITIZE**

# Four Main Goals of a Risk Assessment

1. **Assets:** identify, valuate, and classify
2. **Risks:** identify
3. **Quantify:** the impact of potential threats
4. **Economic Balance:** between the impact of the risk and the cost of the control

**Characterize - Qualify - Quantify - Calculate**

# NIST 800-30: Risk Assessment Activities

1. System Characterization
2. Threat ID
3. Vulnerability ID
4. Control Analysis
5. Likelihood
6. Impact Analysis
7. Risks
8. Control Recommendations
9. Documentation

# Risk Approach: Quantitative vs. Qualitative

## Quantitative

- Numeric and Monetary values

***Management usually needs monetary values to make decisions.***

## Qualitative

- Subjective rating assigned
- "Intuition"
- Delphi method

***An informal analysis can be performed through qualitative means, which would be followed by a more formal quantitative analysis.***

# Pure Quantitative Analysis

- **A purely quantitative risk analysis is very difficult; it is trying to "quantify" issues that are more accurately evaluated from a "qualitative" perspective.**

- **Most decisions typically include elements of both quantitative and qualitative techniques.**

# Annualized Loss Expectancy (ALE)

## Single Loss Expectancy (SLE)

AV * EF = SLE

- Asset Value (AV) x Exposure Factor (EF) = **SLE**
- The exposure factor represents the percentage of loss a realized threat could have on a certain asset

## Annualized Loss Expectancy (ALE)

SLE * ARO = ALE

- SLE x Annualized Rate of Occurrence (ARO) = **ALE**
- The annualized rate of occurrence (**ARO**) is the value that represents the estimated possibility of a specific threat taking place

# ALE Example

1. **Tornado is estimated to damage 50% (.50) of a facility if it hits, and the value of the facility is $200,000.**

2. **The probability is one in ten (.10) years:**

   AV x EF = SLE = 200,000 x .50 = 100,000
   SLE x ARO = ALE = 100,000 x .10 = 10,000

   **ALE is $10,000**

3. **Management should not spend over $10,000 in countermeasures trying to protect against this risk.**

# Other ALE Examples

- This sample analysis presents several threats, accompanied by their SLE and ALE values.
- The goal: provide the team and management an idea of the risks they should address and indicate which threat could be most damaging.

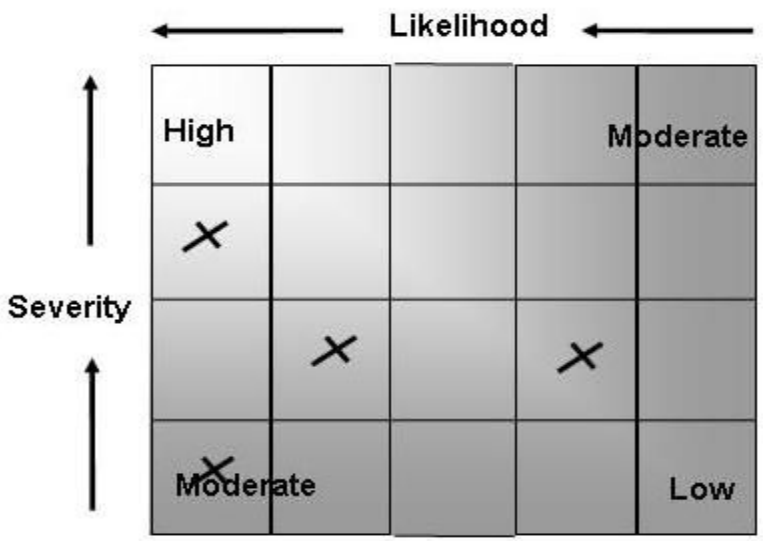
| Asset | Threat | Asset Value | (EF) | Potential Loss (SLE) | Annualized Frequency | Annual Loss Expectancy (ALE) |
|---|---|---|---|---|---|---|
| Facility | Fire | $560,000 | 40% | $224,000 | .25 | $56,000 |
| Trade Secret | Stolen | $43,500 | 92% | $40,020 | .75 | $30,015 |
| File Server | Failed | $11,500 | 100% | $11,500 | .50 | $5,750 |
| Data | Virus | $8,900 | 70% | $6,230 | .80 | $4,984 |
| Customer Credit Card Info | Stolen | $325,500 | 83% | $270,165 | .60 | $162,099 |

# Qualitative Risk Analysis Steps

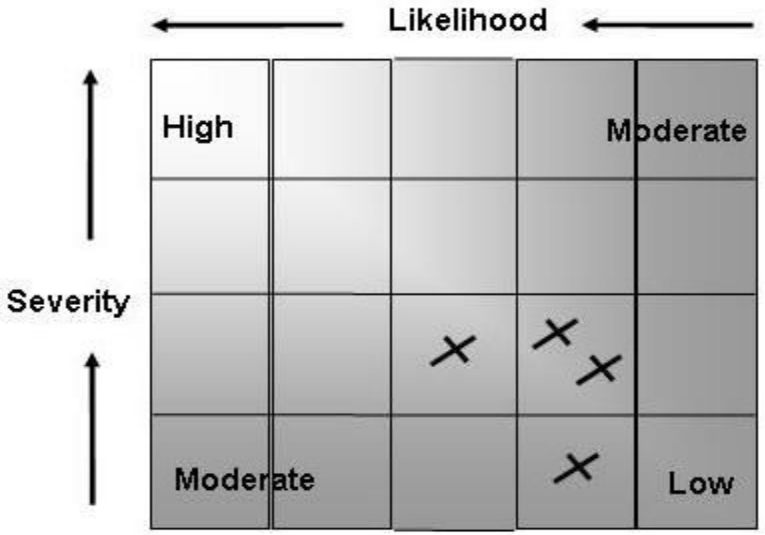
1. Develop Risk Scenarios
2. Gather company "Subject Matter Experts"
3. Walk through scenario to determine results
4. Prioritize risks and threats to assets
5. Build consensus for best countermeasures

# Qualitative Risk Assessment

**Inherent (Initial) Risk**
**(before controls)**




**Residual Risk**
**(after controls)**




**Exposure areas:**
**Information Integrity Loss**
**Disclosure**
**Availability Loss**

**Regulations or Ethics Violations**
**Network Impact**
**Financial Impact**

# Types of Risk

- **TOTAL RISK:** *risk that exists before controls*
- **RESIDUAL RISK:** *risk after countermeasures or safeguards*
- **ACCEPTED RISK:** *If a company chooses not to implement countermeasures, they make the choice of the total risk of a threat*

**Risk Calculations**

**Threats * Vulnerability * Asset Value = Total Risk**

**Total Risk * Controls Gap = Residual Risk**

# Risk Assessment Component

## RISK TEAM

### Ensure business managers maintain accountability for their decisions

**Identified assets must have values assigned to them**

**Identify company assets by interviewing individuals, reviewing documentation, and tours.**

**Representatives from each department should be on the team or at least interviewed.**

**Many factors play into estimating the value of an asset, not just the value on a purchase order.**

# Risk Management Process Review

- **Follow the steps of risk assessment**
  - Risk Assessment is usually the most difficult to accomplish
  - Many unknowns
  - Necessary effort of gathering the right data
  - Risk Analysis can be done qualitatively and/or quantitatively
- **Take steps to reduce risk to acceptable level**
- **Maintain that risk level**
- **Remember - Risk must be managed, since it cannot be totally eliminated**

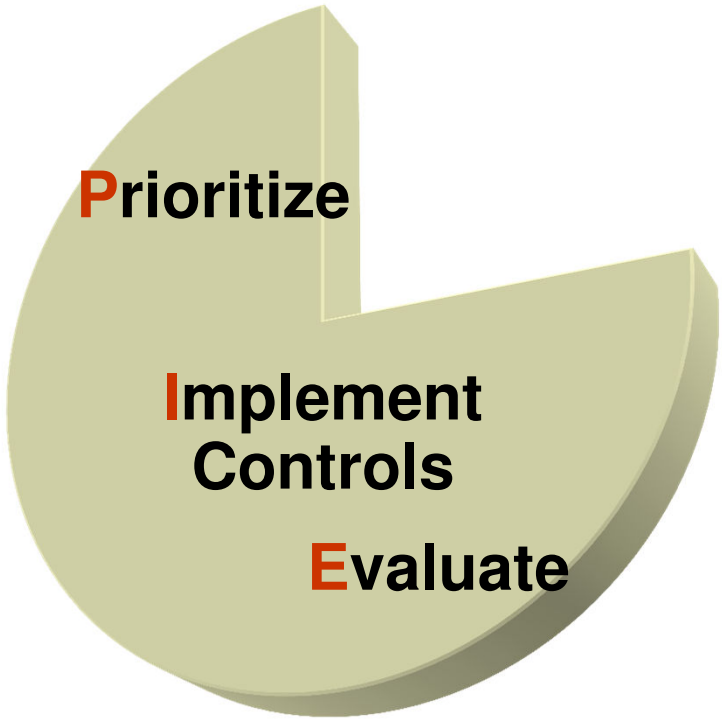
# Mitigation - Dealing With Risk

## Mitigate Risk

- Be Aware: By now, risk analysis is complete and management is aware of the team's findings.
- Set Controls: Present the controls which mitigate each risk.
- Know the Limits: These controls mitigate risk but do not abolish it; complete reduction is impossible to achieve.
- Accept Limits: Establish an acceptable risk, since risk always remains.

# NIST 800-30 Risk Mitigation

- Strategy
- Control Categories
- Cost Benefit Analysis
- Control Implementation
- Options
- Residual Risk



# Risk Mitigation Options

- **Reject (not an acceptable form of mitigation)**
  - Ignore / ignorance
  - Neglect / negligence
- **Reduce**
  - Risk Avoidance
  - Risk Limitation
- **Accept**
  - Risk Assumptions
- **Transfer**
  - Risk Transference

# NIST SP 800-30: Control Implementation

- **Step 1: Prioritize Actions**
  - Feasibility
  - Effectiveness
- **Step 2: Evaluate Recommended Actions**
  - Feasibility,
  - Effectiveness
- **Step 3: Cost Benefit Analysis**
  - Cost of implementation
  - Cost of non-implementation
  - Associated Costs
- **Step 4: Select Controls**
  - Technical Security Controls
  - Management Security Controls
  - Operational Security Controls
- **Step 5: Assign Responsibility**
- **Step 6: Develop Safeguard Implementation Plan**
  - Risks and Related Risks
  - Prioritize Actions
  - Recommended Controls
  - Selected Planned Controls
  - Responsible Persons
  - Start Date
  - Target Complete Date
  - Maintenance Requirements
- **Step 7: Implement Controls**
  - Cost of implementation
  - Cost of non-implementation
  - Associated Costs

# Cost/Benefit Assessment Component

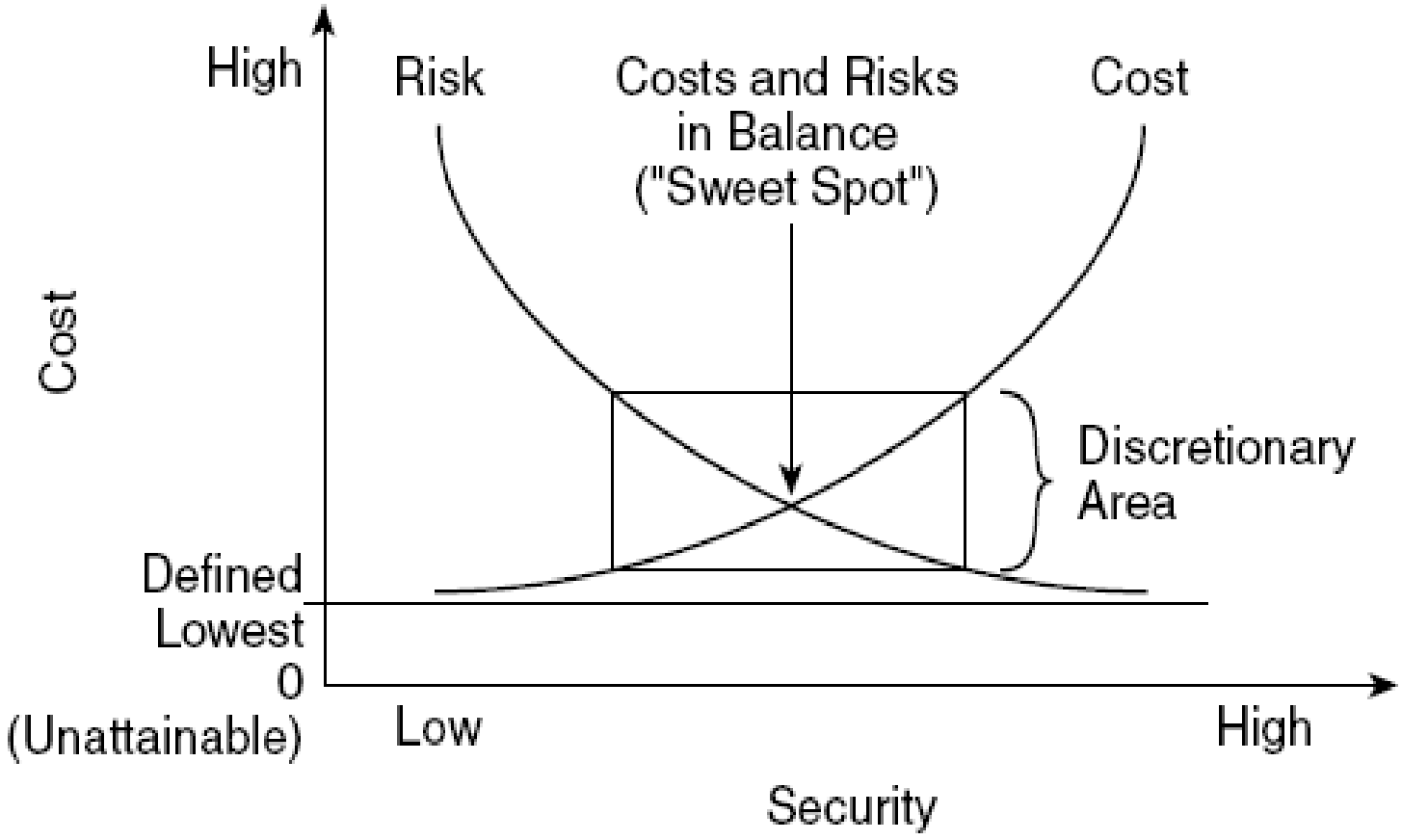
**Compare the** annualized cost of controls **against the expected** cost of potential loss**.**

**If a server is worth $10,000 and one suggested security safeguard would cost the company $12,000, the idea would be discouraged during the cost/benefit analysis**

***annualized control costs vs. potential loss***

- ✓ Variables are involved in cost/benefit analysis and risk analysis
- ✓ Assessments are not always so cut and dry

# Balancing cost and security



# Control Criteria

## Good Security Control:

- Achieves its goal by mitigating the risk
- Makes good business sense because it is cost effective

## Cost-Benefit Analysis Formula:

ALE (before implementing control)
– ALE (after implementing control)
– Annual Cost of Control

---

**= Value of the control to the company**

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- **Manage personnel security**
- Develop and manage security education, training and awareness
- Manage the security function

# Employee Management Policies

- **Employee management policies should address:**
  - Dangerous shortcuts
  - Collusion
  - Fraud
- **Employee management policies should apply to:**
  - Pre-employment
  - Mid-employment
  - Post-employment

# Employees Policies

## Pre-employment

- Background check
- Drug screening
- Security clearance
- Credit check

## Termination Procedures

- Person should leave facility immediately, under supervision
- Person must surrender ID badge, keys, and company property.
- Review the non-disclosure agreement.
- An exit interview must be completed.
- User's accounts should be disabled.
- Change Passwords immediately.
- Be respectful! Friendly versus unfriendly.

# Agenda

- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- **Develop and manage security education, training and awareness**
- Manage the security function

# Knowledge Transfer

Awareness, Training, Education

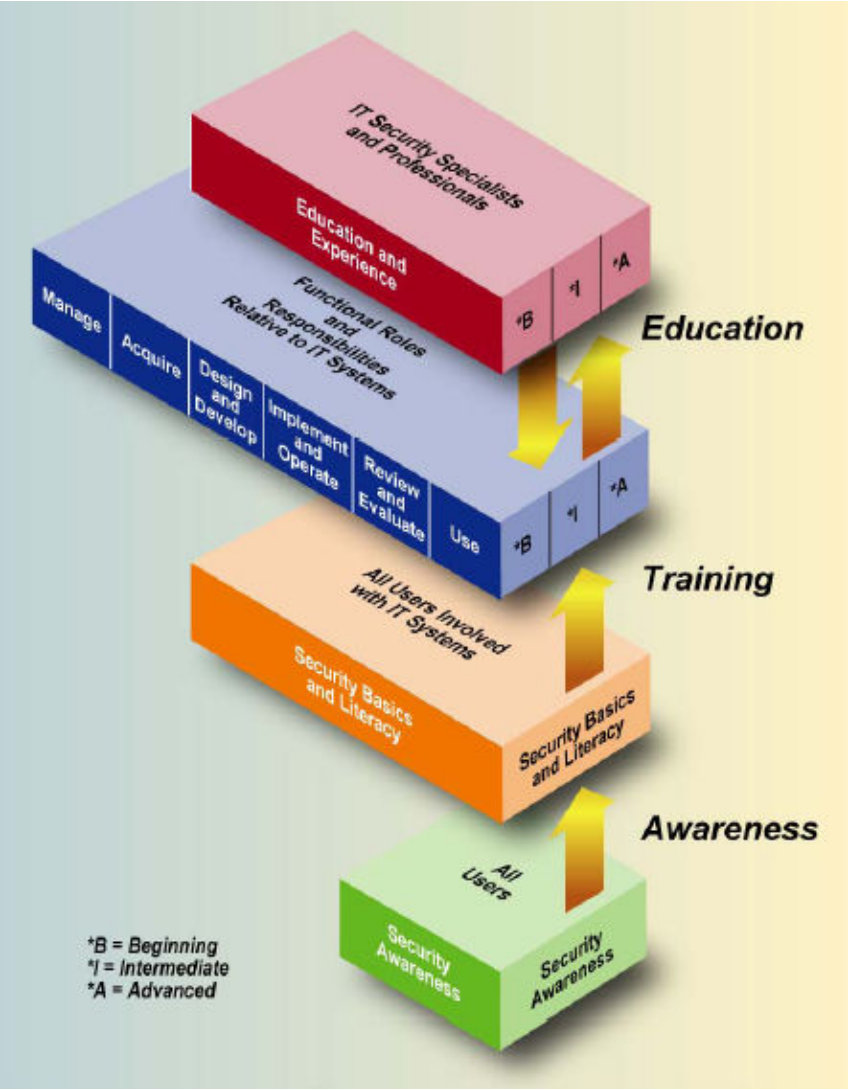
"People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program."

# NIST SP 800-50: Knowledge Transfer

- **Knowledge Transfer**
  - Awareness
  - Training
  - Education

**Groups:**

- IT Security Specialists
- Functional Roles
- All IT Users
- All Users



# Being Aware of the Rules

## Security Awareness Training

- Employees cannot and will not follow the directives and procedures, if they do not know about them
- Employees must know expectations and ramifications, if not met
- Employee recognition award program
- Part of due care
- Administrative control

# Awareness/Training/ Education Benefits

## Overriding Benefits:

- Modifies employee behavior and improves attitudes towards information security
- Increases ability to hold employees accountable for their actions
- Raises collective security awareness level of the organization

# Awareness/Training/ Education Implement

## Implementation:

- Basic security training should be required for all employees.
- Advanced training may be needed for managers.
- Specialized training is necessary for system administrators and information systems auditors.
- Specialized training is normally delivered through external programs.
- Should be regarded as part of career development.

# Agenda

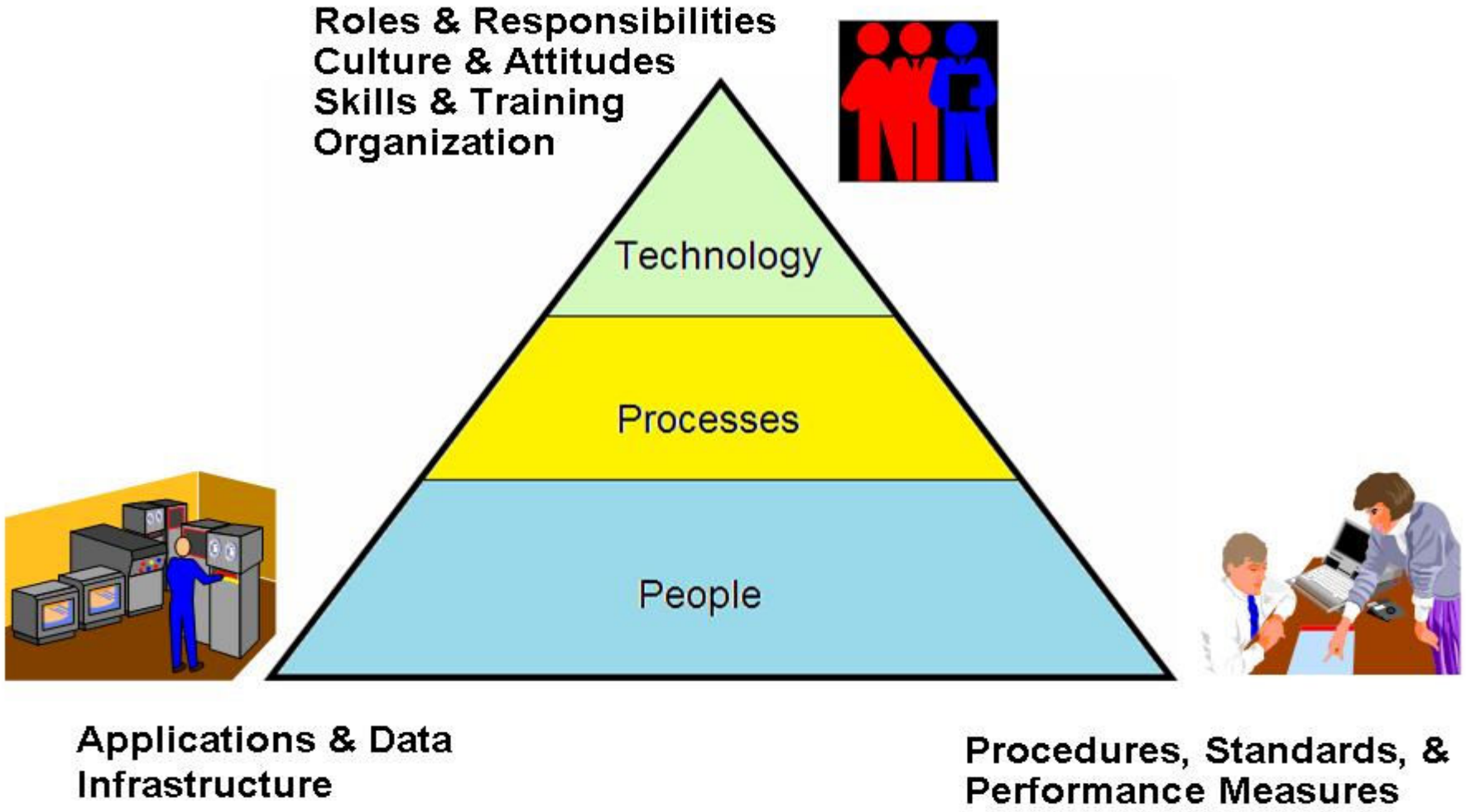
- Understand and align security function to goals, mission and objectives of the organization
- Understand and apply security governance
- Understand and apply concepts of confidentiality, integrity and availability
- Develop and implement security policy
- Manage the information life cycle
- Manage third party governance
- Understand and apply risk management concepts
- Manage personnel security
- Develop and manage security education, training and awareness
- **Manage the security function**

# Security Management

## Set Goal and Scope:

- Asset Management
- Risk Management
  - Assessment
  - Analysis
  - Mitigation
- Policies, Standards, Procedures, and Guidelines
- Knowledge Transfer

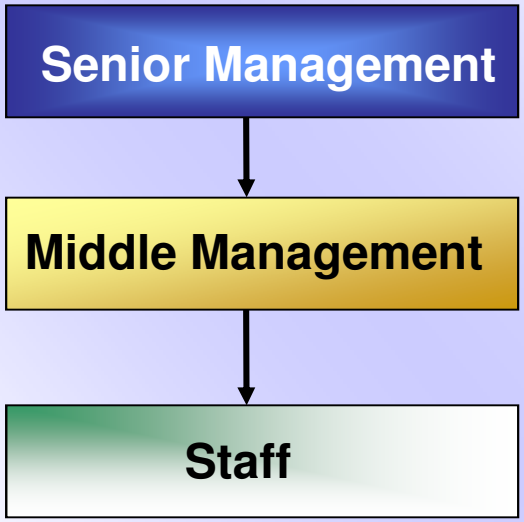
# People – Processes - Technology



# Approach to Security Management

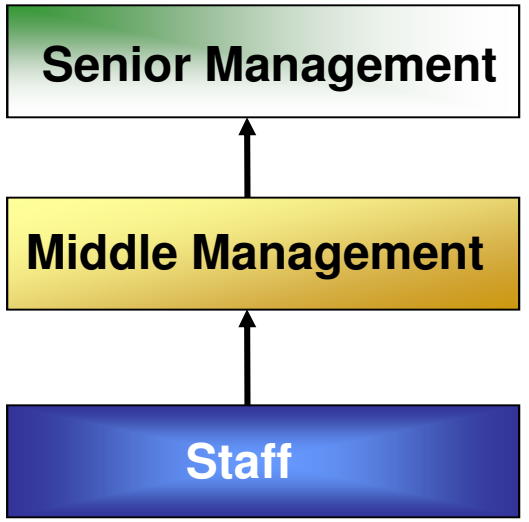
## Top-Down Approach

Security practices are directed and supported at the senior management level




## Bottom-Up Approach

**The IT department tries to implement security**



# Summary

- Senior management is responsible for protecting assets
- Identify assets and assign values
- Identify risks and potential losses
- Implement policies, procedures, standards, and guidelines
- Implement controls to mitigate risks
- Employee management is crucial
- Administrative, technical, physical controls
- Due care and due diligence is key