Lecture 9: Risk Management: *Controlling Risk*

EECS711 Security Management & Audit

Objectives

- Learn risk control strategy options and be prepared to select when given background information
- Evaluate risk controls and formulate a cost-benefit analysis (CBA) using existing conceptual frameworks
- Explain how to maintain and perpetuate risk controls
- Learn popular approaches used in the industry to manage risk

TOPIC 9.1 RISK CONTROL STRATEGIES

Risk Control Strategies

- **Defense:** Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
- **Transferal:** Shifting the risk to other areas or to outside entities
- **Mitigation:** Reducing the impact of the exploited vulnerability
- **Acceptance:** Understanding the consequences and accept the risk without control or mitigation
- **Termination:** Removing info assets from operating environment

Defense

- **Defense**: also known as "**Avoidance**"
  - The most preferred approach … but somehow impossible
  - Prevent the exploitation of the vulnerability
    - Countering threats
    - Removing vulnerabilities in assets
    - Limiting access to assets
    - Adding protective safeguards
  - In general, accomplished through:
    - Application of **policy**
    - Application of **training and education**
    - Implementation of **technology**

Transferal

- **Transfer**
  - 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
    - Implementing service **contracts** with providers
    - Purchasing **insurance**

Mitigation

- **Mitigation**
  - Reduce the damage caused by a realized incident/disaster
  - Depends on the ability to detect and respond to an attack
    - boundary protection, defense-in-depth, agile defense
  - The primary link between risk management program and InfoSec program
    - Organization's mission and business processes are designed with regard to information protection needs
    - Enterprise structures including InfoSec structure are designed with considerations for risk mitigation
    - Risk mitigation measures are implemented by consistent safeguards
    - InfoSec programs, processes, and safeguards are flexible and agile in recognizing the diversity in organizational missions

Mitigation

- **Mitigation**
  - Reduce the damage caused by a realized incident/disaster *by means of planning and preparation*

TABLE 8-1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Timeframe
Incident Response Plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan (DRP)	■ Preparations for recovery should a disaster occur ■ Strategies to limit losses before and during disaster ■ Step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

Acceptance

- **Acceptance**
  - The decision to do nothing to protect an information asset from risk and accept the outcome
    - Cost of protection outweighs cost of asset replacement
  - Risk acceptance vs. risk false positive
  - Risk acceptance vs. laziness and carelessness
    - This control, or lack of control, assumes that it may be a prudent business decision to
      - Examine alternatives
      - Conclude the cost of protecting an asset does not justify the security expenditure

Acceptance

- **Acceptance** is recognized as a valid strategy only when the organization has
  - Determined the level of risk posed to an info asset
  - Assessed the probability of attack and the likelihood of a successful exploitation of a vulnerability
  - Estimated the potential damage or loss that could result from attacks
  - Evaluated potential controls using each appropriate type of feasibility
  - Performed a thorough CBA
  - Determined the costs to control the risk an info asset do not justify the cost of implementing/maintaining controls

Termination

- **Termination**
  - based on the organization's need or choice *not to protect an asset*
    - Cost of protection outweighs asset value
  - The organization does not wish the asset to remain at risk so it is **removed from** the environment that represents risk
- Termination must be a conscious business decision
  - Not simply the abandonment of an asset
  - Would technically qualify as acceptance

TOPIC 9.2 MANAGE RISK

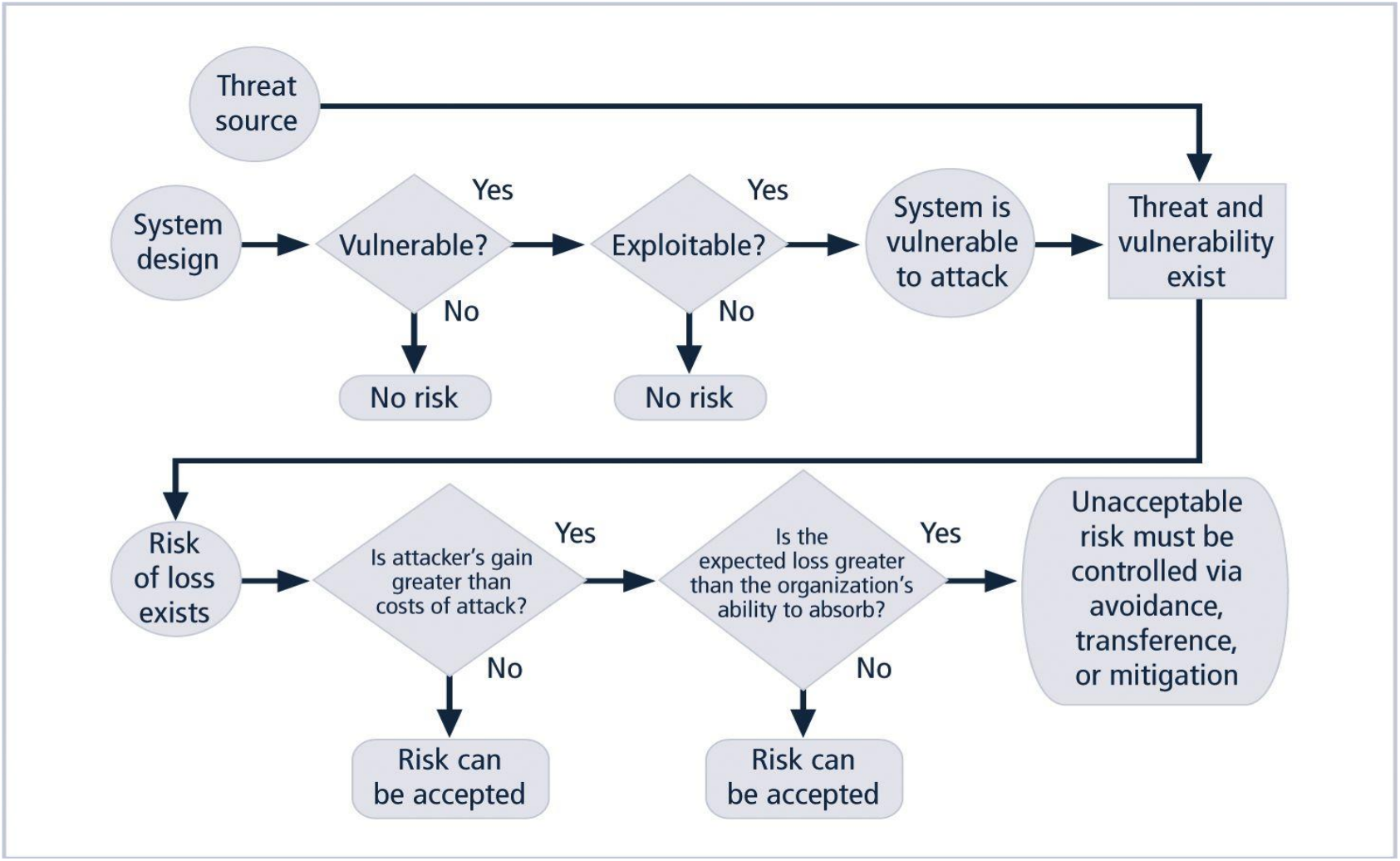
Managing Risk

- **Risk Appetite,** a.k.a **Risk Tolerance**
  - Levels and types of risk that organizations are willing to accept
    - as they evaluate the trade-offs between perfect security and unlimited accessibility
  - Information risks and controls should be in balance
    - the key is to find balance in decision-making process and in feasibility analysis
  - Risk tolerance is based on experience and facts
    - not on ignorance and wishful thinking

Managing Risk

- **Residual Risk**
  - Remaining risk after the organization has implemented
    - Policy
    - Education and training
    - Technical controls and safeguards
- The **goal** of InfoSec in risk management
  - is not to bring residual risk to zero
  - is to bring residual risk in line with the organization's risk tolerance

Risk Handling Process



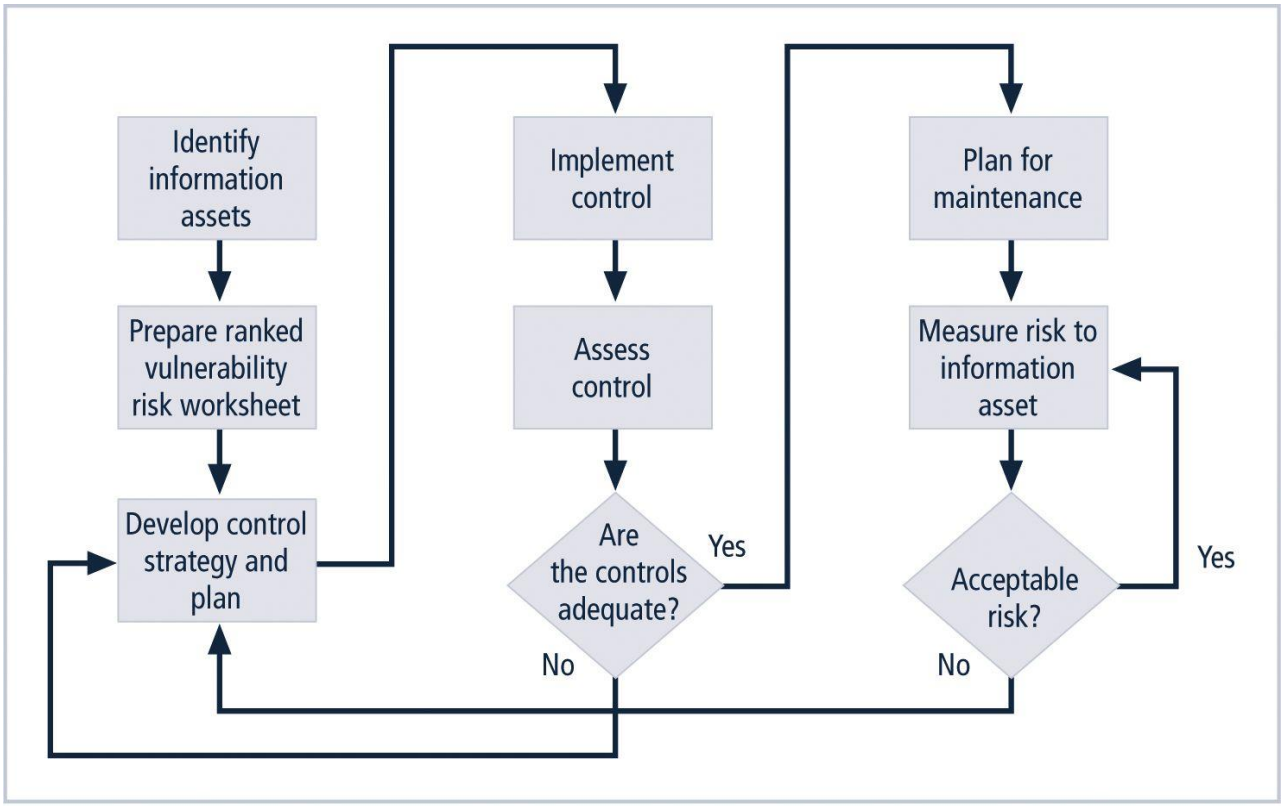
Rules for Strategy Selection

- When a vulnerability exists in an important asset:
  - Implement security controls to reduce the likelihood of a vulnerability being exploited
- When a vulnerability can be exploited:
  - Apply layered protections, architectural designs, and administrative controls to minimize or prevent the attack
- When the attacker's potential gain is greater than the costs of attack
  - Apply protections to increase attacker's cost or reduce attacker's gain
- When the potential loss is substantial
  - Apply technical, design and administrative protections to limit the extent of attack, reducing the potential for loss

Risk Control Strategy Selection

- **Risk control**
  - Involves selecting one of the five risk control strategies for the vulnerabilities presented 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, at least one of the other four control strategies will have to be selected
  - Document selected control strategy for every asset-threat pair
    - strategy, justification, implementation, outcome, residual risk

Risk Control Cycle



- Selected controls should be monitored and measured on an ongoing basis to determine effectiveness

TOPIC 9.3 COST-BENEFIT ANALYSIS

Feasibility Analysis

- An organization must explore the consequences of an exploitation of the vulnerability
  - economic and noneconomic consequences

For example:

Data breach costs

Cost Activity	2010	2009	2008
Lost customer business due to churn	39%	40%	43%
Legal services – defense	14%	14%	9%
Investigations & forensics	11%	8%	9%
Audit and consulting services	10%	12%	11%
Customer acquisition costs	9%	9%	9%
Inbound contact costs	6%	5%	6%
Outbound contact costs	5%	6%	6%
Legal services – compliance	2%	4%	4%
Identity protection services	2%	2%	2%
Free or discounted services	1%	1%	2%
Public relations / communications	1%	1%	1%

Feasibility Analysis

- An organization must explore the consequences of an exploitation of the vulnerability
  - *"What are the actual and perceived advantages and disadvantages of implementing a control?"*
    - Especially, the value of information assets that control is designed to protect
  - **Cost avoidance:** the money saved by using the defense strategy via the implementation of control
    - economic feasibility

Cost-Benefit Analysis (CBA)

- **Economic feasibility analysis**
  - The most common criterion used when evaluating a strategy to implement InfoSec controls and safeguards
  - First valuing the information assets
  - Then, determining the loss in value if those assets become compromised
- **Cost-benefit analysis** is a form of economic feasibility study
  - Compares the life-cycle cost of implementing a control mechanism against the estimated economic benefit that would accrue from the implementation of the control

Cost vs. Benefit

- 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

- It is difficult to determine the *cost of safeguarding information assets*
  - Cost of development or acquisition of hardware, software, and services
  - Service costs (vendor fees for maintenance & upgrades)
  - Training fees
  - Cost of implementation (installing, configuring, and testing hardware, software, and services)
  - Cost of maintenance (labor expense to verify and continually test, maintain, train, and update)
- **Annual cost of the safeguard (ACS)**

Cybersecurity Cost

- Capital Investment
  - Expenditure that will benefit for several periods
    - e.g., purchase of an IDS system (+ personnel cost)
  - Expect to work at least next few years
    - Capital investments lose their economic values
    - Portion of the investment that has been lost during a particular period is charged to that period
- 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

Benefit

- **Benefit**
  - The value to the organization of using controls to prevent losses associated with a specific vulnerability
- Usually determined by
  - Valuing the information asset or assets exposed by the vulnerability
  - Determining how much of that value is at risk and how much risk exists for the asset
- The result is expressed as the annualized loss expectancy (ALE)

Asset Valuation

- Organization must be able to place a dollar value on each information assets it owns, based on:
  - How much did it cost to create or acquire?
  - How much would it cost to recreate or recover?
  - How much does it cost to maintain?
  - How much is it worth to the organization?
  - How much is it worth to the competitor?

Asset Valuation

- **Asset valuation**
  - The process of assigning financial value or worth to each information asset
  - Can use the info assets assessment introduced before
  - Can involve the estimation of real or perceived costs
- Costs can be associated with
  - Design, development, installation, maintenance, protection, recovery, and defense against loss or litigation
  - Some costs are easily determined while others not
    - cost of replacing a network switch
    - dollar value loss in market share

Asset Valuation Components

- Asset valuation is a complex process
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Asset Valuation

- After estimating the worth of an asset, calculate the **potential loss** from the exploitation of vulnerability or a threat occurrence
  - What loss could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the financial impact of damage?
  - What is the single loss expectancy for each risk?

Asset Valuation Techniques

- **Single loss expectancy (SLE)**
  - Value associated with the most likely loss from a single occurrence of a specific attack

SLE = asset value (AV) x exposure factor (EF)

- Value of the asset
- EF = percentage of loss that would occur from a given vulnerability being exploited
- For example:
  - A Web site with an estimate value of $1,000,000
  - 10% of Web site would be damaged by a vandalism hacking

Asset Valuation Techniques

- **Annualized rate of occurrence (ARO)**
  - How often you expect a specific type of attack to occur?
    - For example: if a successful act of vandalism occurs once every two years
    - ARO = 0.5
- **Annualized loss expectancy (ALE)**
  - A comparative estimate of the losses from successful attacks on an asset over one year
  - **ALE = SLE x ARO**

Asset Valuation Techniques

- CBA determines whether or not the benefit from a control alternative is worth the associated cost of the control
- **CBA formula**:
  - **CBA = ALE (precontrol) – ALE (postcontrol) – ACS**

  where:
    - ALE (precontrol) = ALE of the risk before implementation of the control
    - ALE (postcontrol) = ALE after the control has been in place for a while
    - ACS = annual cost of the safeguard

Example

Scenario:

- You are the CISO at XYZ Corp with 50 employees.
- You want to implement a company-wide, 2-day-per-year security training program for all employees for the next 3 years.
- Justify the investment to the CEO.

Estimation

- Assume the chance of a breach due to password cracking was 90% per year before the training program. The cost of such a breach averaged $150,000. Therefore, the **precontrol ALE** was:

  (.90) * ($150,000) = $135,000

- Assume the training program is expected to reduce the chance of a breach due to password cracking to 30% per year. The cost of such a breach remains the same, so the **postcontrol ALE** is:

  (.30) * ($150,000) = $45,000

Estimation

	Year 0	Year 1	Year 2	Year 3
Reduced Password Cracking	-	**$90,000**	**$90,000**	**$90,000**

Estimation

	Year 0	Year 1	Year 2	Year 3
Reduced Password Cracking	-	**$90,000**	**$90,000**	**$90,000**
Reduced Insider Threat	-	$30,000	$30,000	$30,000
Reduced Social Engineering	-	$45,000	$45,000	$45,000

Estimation

	Year 0	Year 1	Year 2	Year 3
Reduced Password Cracking	-	**$90,000**	**$90,000**	**$90,000**
Reduced Insider Threat	-	$30,000	$30,000	$30,000
Reduced Social Engineering	-	$45,000	$45,000	$45,000
Staffing	$10,000	$60,000	$62,400	$64,896
Opportunity Cost	-	$16,016	$16,656	$17,322
CBA per year	$10,000	$88,984	$85,944	$82,782
Total CBA	**$247,710**			

Other Feasibility Analysis

- Feasibility analysis measures how ready an organization is for the introduction of controls
  - Economic feasibility is to justify investment for InfoSec controls
  - Also need to consider:
    - Organizational feasibility
    - Operational feasibility
    - Technical feasibility
    - Political feasibility

Organizational Feasibility

- **Organizational feasibility**
  - Define corporate and legal structure of the business, internal and external principles and practices
  - How well the proposed InfoSec alternatives will contribute to the organization's strategic objectives?
    - Efficiency, effectiveness, and overall operation of an organization
    - Begins with program security policy, ends with organization management's decision to empower InfoSec to control the risk
  - The organization should not invest in technology that changes its fundamental ability to explore certain avenues and opportunities

Operational Feasibility

- **Operational feasibility**
  - Also known as **behavioral feasibility**
  - Management acceptance and support
  - User acceptance and support
    - How do the end-users feel about their roles in new system?
    - What end-users or managers may resist or not use the system? Can this problem be overcome? If so, how?
    - **User engagement:** communication, education, and involvement can reduce resistance to change
  - System's compatibility with the requirements of the organization's stakeholders
  - Usability analysis
    - Ease of use, Ease of learning, User satisfaction

Technical Feasibility

- **Technical feasibility**
  - Determine whether an organization already has or can acquire the technology necessary to implement and support them
    - Hardware, software, platform
    - Personnel: examine whether an organization has the technological expertise to manage the new technology

Political Feasibility

- **Political feasibility**
  - What can and cannot occur based on the consensus and relationships among the communities of interest
- Identify policy environment: key players, motivation, belief systems, resources, site of action
- Limits imposed by InfoSec controls must fit within the realm of the possible before they can be effectively implemented
  - Budget allocation, staff resources, …

Alternatives to Feasibility Analysis

- Besides CBA and other feasibility analysis, can adopt:
  1. **Benchmarking:** Seeking out and studying the practices used in other organizations that produce desired results
  2. **Due care and due diligence:** Adopting a certain minimum level of security
  3. **Best business practices:** Considering those thought to be among the best in the industry
  4. **The gold standard:** For those ambitious organizations in which the best business practices are not sufficient
  5. **Government recommendations and best practices**
  6. **Baseline:** Comparing measured actual performance against established standards for the measured category

TOPIC 9.4 RECOMMENDED PRACTICE

Recommended Risk Control Practices

- InfoSec professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities
  - If you put in one safeguard, you decrease the risk associated with all subsequent control evaluations
- Between the difficult task of valuing information assets and the dynamic nature of the ALE calculations
  - Organizations may look for a more straightforward method of implementing controls

Qualitative and Hybrid Measures

- Risk assessment steps can be executed using estimates based on a qualitative assessment, e.g.,
  - Listing all possible attacks on a particular set of information
  - Rating each in terms of its probability of occurrence – high, medium, or low
  - Hybrid assessment uses scales rather than specific estimates
    - instead of a specific value for ARO
    - a scale ranges from 0 (representing no chance of occurrence) to 10 (representing almost certain occurrence)

Delphi Technique

- Delphi technique
  - A group rates or ranks a set of information
    - Can be applied to the development of scales, asset valuation, asset or threat ranking, or any scenario that can benefit from the input of more than one decision maker
  - Individual responses are compiled and then returned to the group for another iteration
    - A facilitator distribute questionnaire to experts
    - Summarize responses and recirculate
  - Process continues until the group is satisfied with the result
    - Achieve consensus of experts

Recommended Approaches

- NIST Risk Management Model
- OCTAVE
- Microsoft Security Risk Management Guide
- FAIR
- ISO 27005

NIST SP

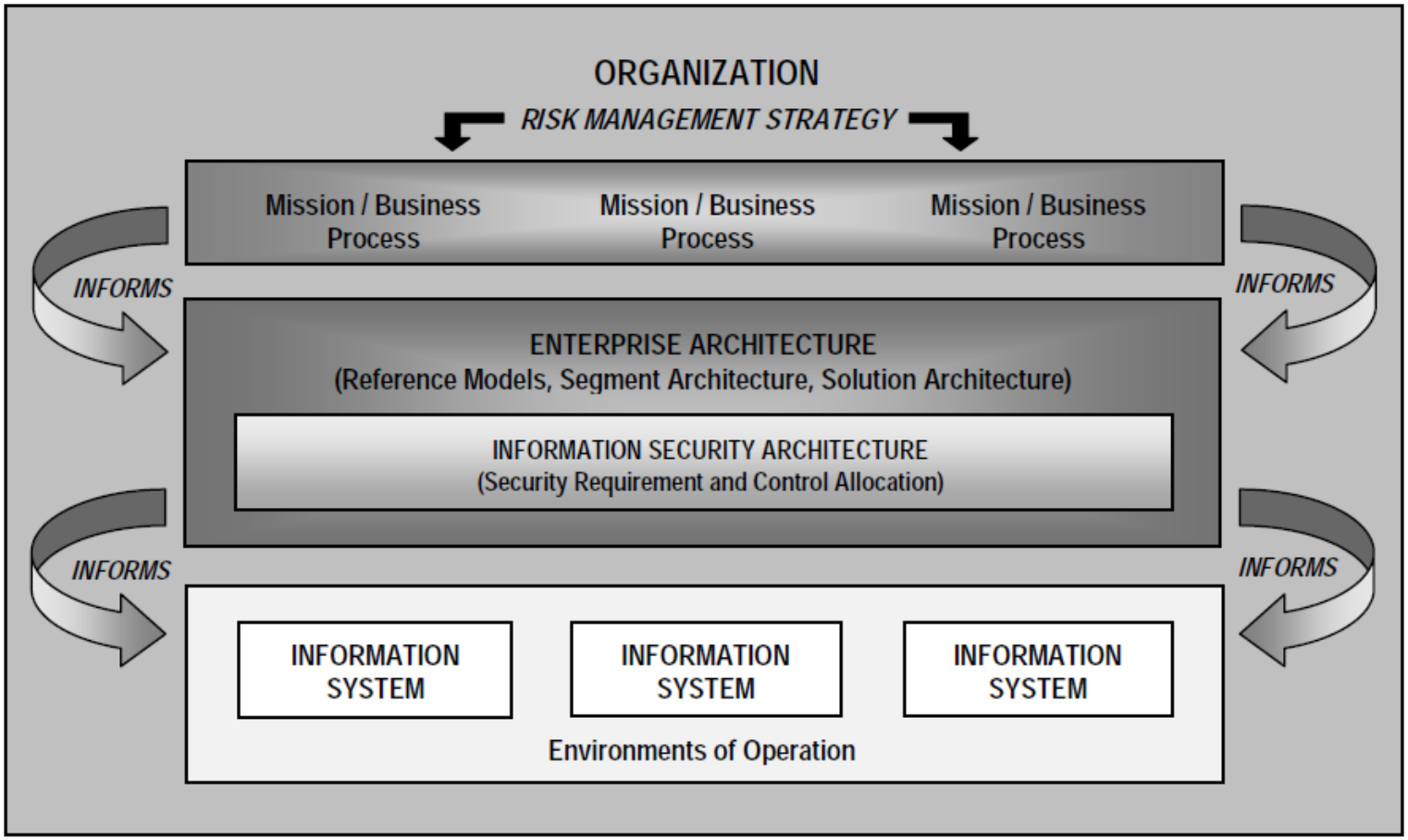
- NIST has a portfolio of guidance on risk management:
  - **SP 800-30** – Guide for Conducting Risk Assessments
  - **SP 800-37** — Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - **SP 800-39** — Managing Information Security Risk: Organization, Mission and Information System View
  - **SP 800-53** — Recommended Security Controls for Federal Information Systems and Organizations
  - **SP 800-53A** — Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans

NIST Risk Management Model

- NIST SP 800-39: Managing Information Security Risk: Organization, Mission and Information System View
  - A general overview of the risk management process
  - How organizations establish the context for risk-based decisions
  - How organizations assess risk considering threats, vulnerabilities, likelihood, and consequences or impact
  - How organizations respond to risk once determined
  - How organizations monitor risk over time with changing mission/business needs, operating environments, and supporting information systems

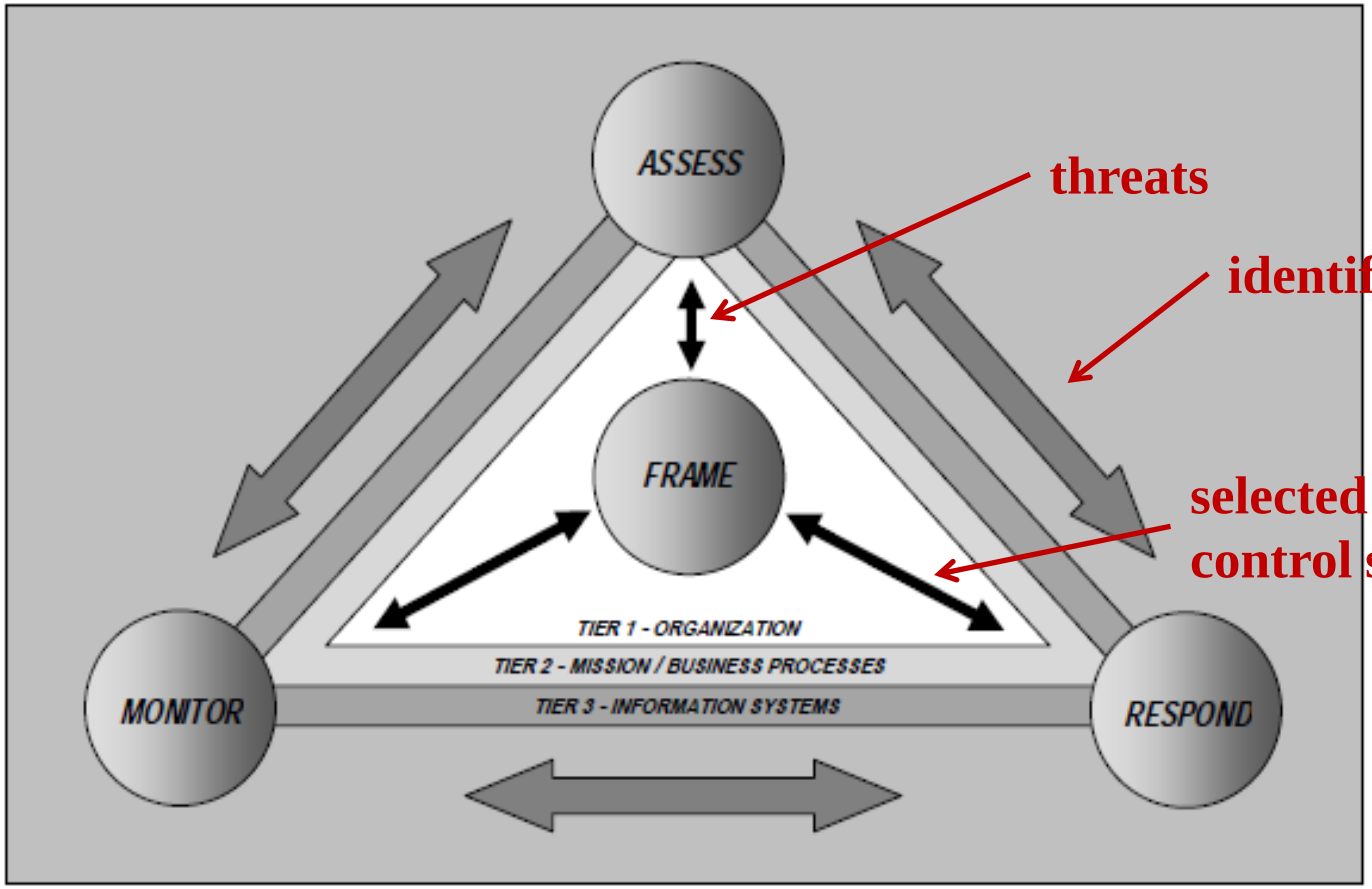
NIST Risk Management Model

- Information Security Architecture



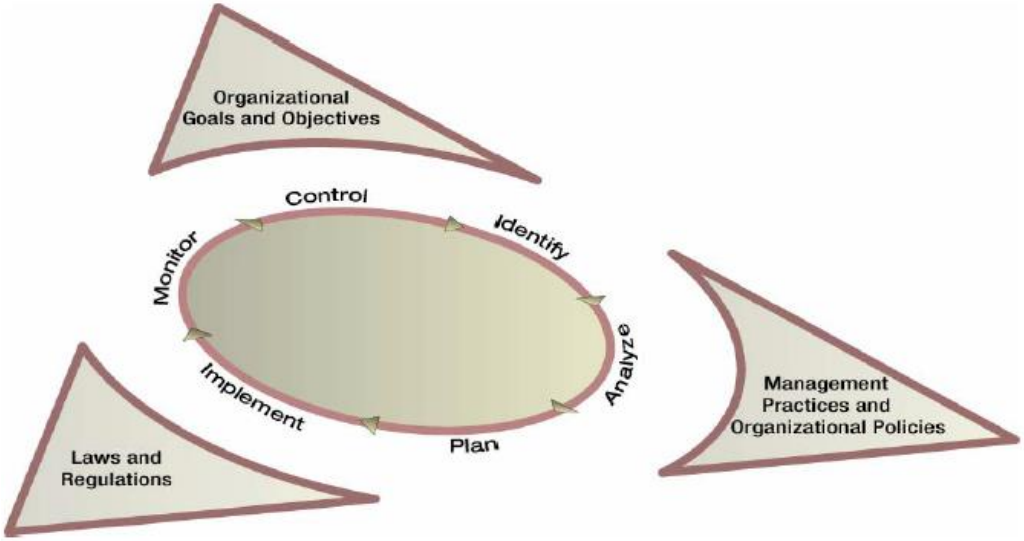
NIST Risk Management Model

Multi-tiered organization-wide risk management process:



OCTAVE

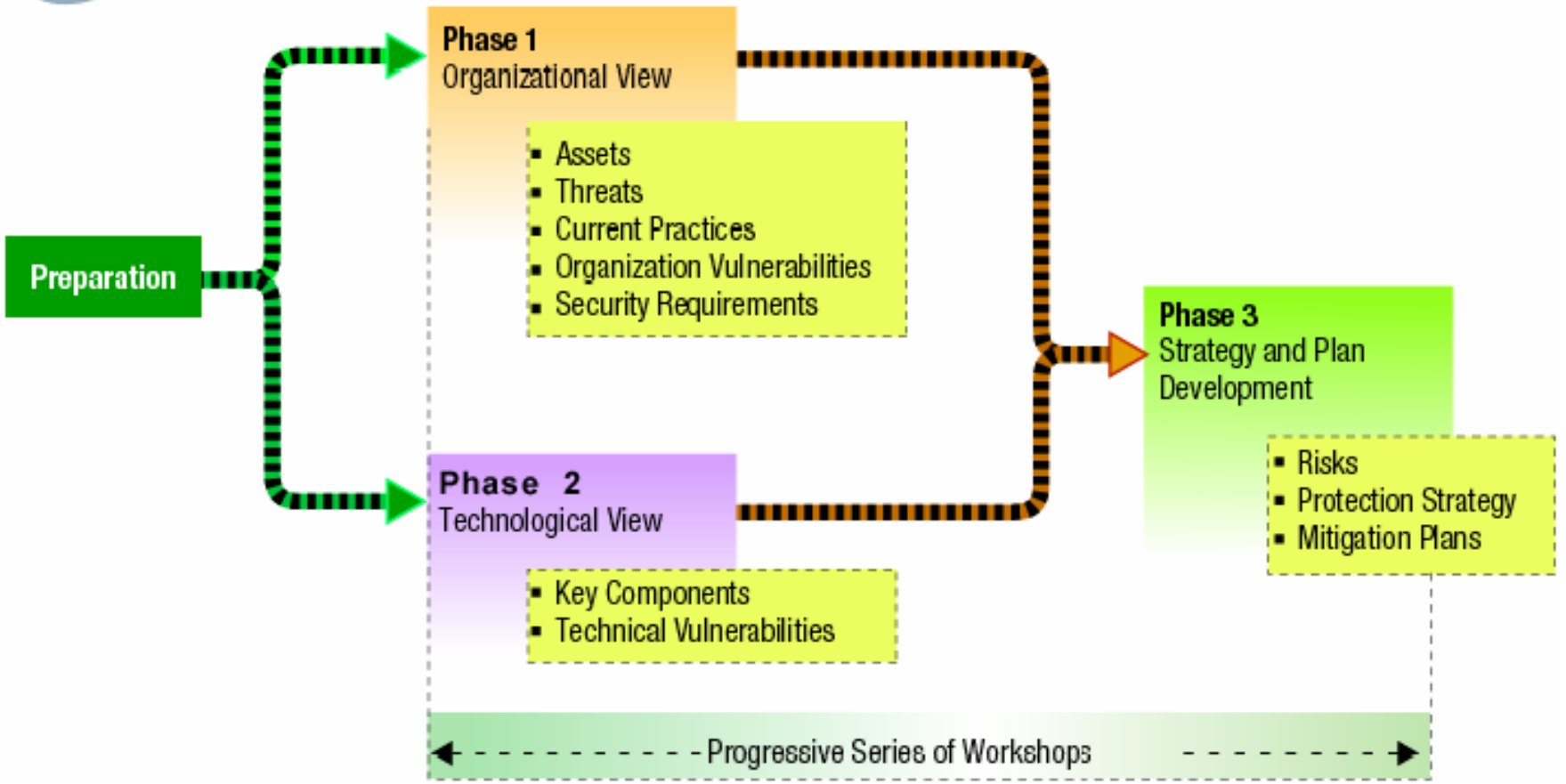
- **OCTAVE: the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation method**
  - An approach to manage information security risk
  - Allows organizations to balance the protection of critical information assets against the costs of providing protective and detection controls



OCTAVE

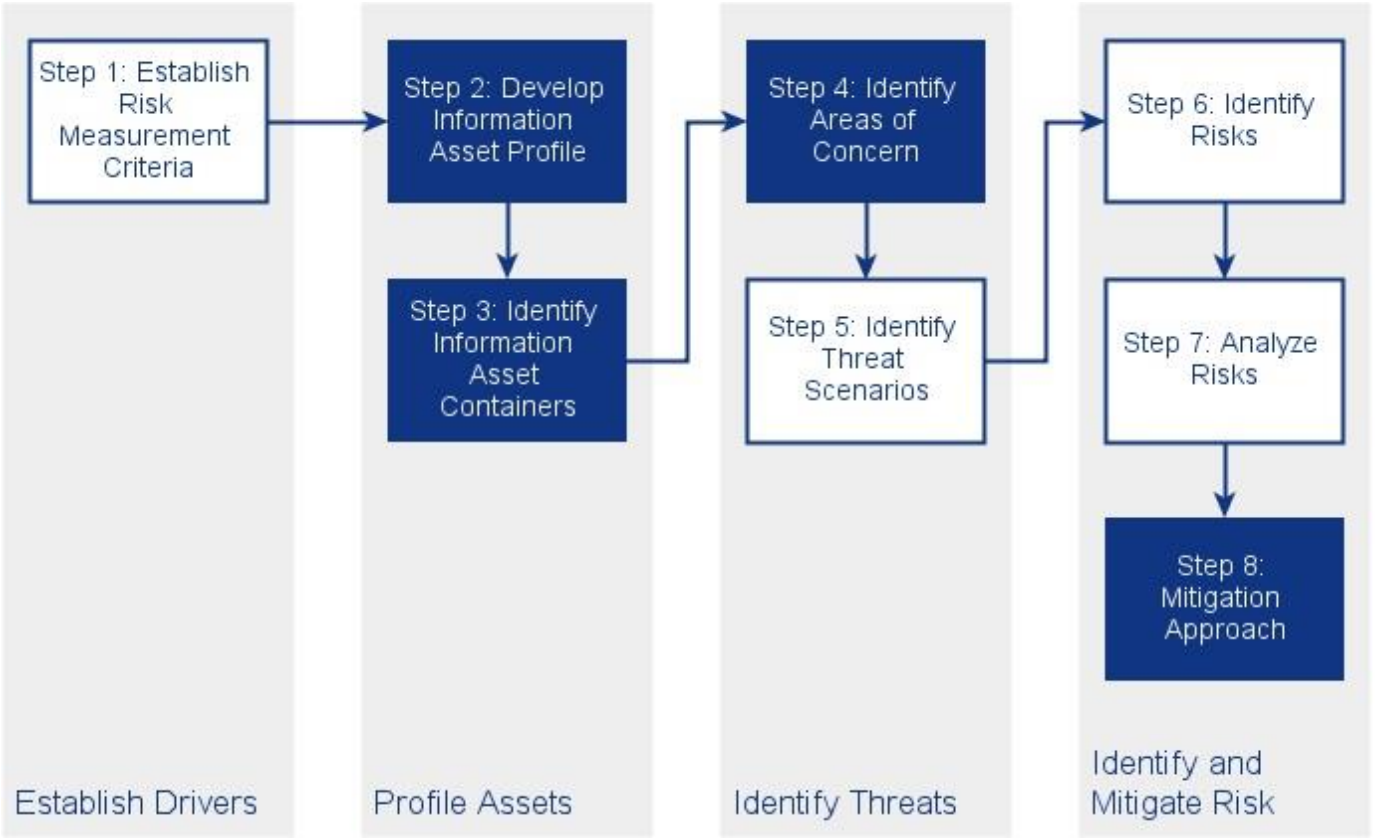
- Asset-based risk assessment
  - What assets require protection?
  - What level of protection is needed?
  - How might an asset be compromised?
  - What is the impact if protection fails?
- Three variations:
  - The original OCTAVE Method, 1999
  - OCTAVE-S, for smaller organizations, 2003
  - OCTAVE-Allegro, a streamlined approach for InfoSec assessment and assurance, 2007

octave® Process



OCTAVE Allegro Phases

- 8 steps in 5 phases:



OCTAVE Phases

- Preparation
  - 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

OCTAVE Phases

- Phase 1: Build Asset-Based Threat Profiles
  - Organizational evaluation
  - Key areas of expertise within organization are examined
    - Information assets, threats to those assets, security requirements of assets
    - What organization is currently doing to protect its information assets
    - Weaknesses in organizational policies and practice
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Management Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles

OCTAVE Phases

- Phase 2: Identify Infrastructure Vulnerabilities
  - Information infrastructure evaluation
  - Key operational components of information technology infrastructure are examined for weaknesses (technology vulnerabilities)
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components

OCTAVE Phases

- Phase 3: Develop Security Strategy and Plans
  - Identify risks to organization
  - Evaluate risks based on their impact to the organization's mission
  - Organization protection strategy and risk mitigation plans for the highest priority risks are developed
  - Process 7: Conduct Risk Analysis
  - Process 8: Develop Protection Strategy

Problem-Based Learning

Read the case study in OCTAVE practitioners report

- HIPAA-mandated Risk Assessments
  - The Defense Health Information Assurance Program standardize risk assessment in DoD medical treatment facilities
- The National Center for Manufacturing Sciences Case
  - To explore and broaden vulnerability types in manufacturing domains
  - Develop a process model to identify critical processes/assets through process maps
- The Telescopes in Education (TIE) project
  - A three-server private network connecting to a telescope using the Sky software
  - Identified Business Process Risks and Security Risks

NIST SP 800-30/OCTAVE Correlation

- NIST SP 800-30 is a *standard*
  - provides guidance on the range of risk management activities for information assets across a system life cycle
- OCTAVE is a *methodology*
  - focuses specifically on information risk assessment activities

NIST SP 800-30 Steps	OCTAVE Phase/Process
Step 1: System Characterization	OCTAVE Phase 1/Processes 1 - 3
Step 2: Threat Identification	OCTAVE Phase 1/Process 4
Step 3: Vulnerability Identification	OCTAVE Phase 2/Process 5 - 6
Step 4: Control Analysis	OCTAVE Phase 3/Processes 7 - 8
Step 5: Likelihood Determination	OCTAVE Phase 3/Process 7
Step 6: Impact Analysis	OCTAVE Phases 1/2/3/Processes 1 - 7
Step 7: Risk Determination	OCTAVE Phase 3/Process 7
Step 8: Control Solutions	OCTAVE Phase 3/Process 8
Step 9: Results Documentation	OCTAVE Phases 1/2/3/Processes 1 - 8

Microsoft Risk Management Approach

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

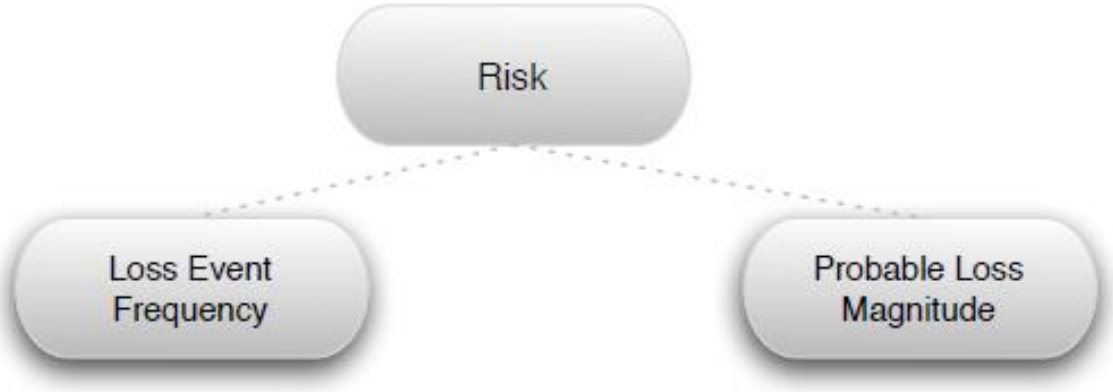
FAIR

- **Factor Analysis of Information Risk (FAIR)**
  - a risk management framework developed by Jack Jones at Risk Management Insight, LLC
- 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

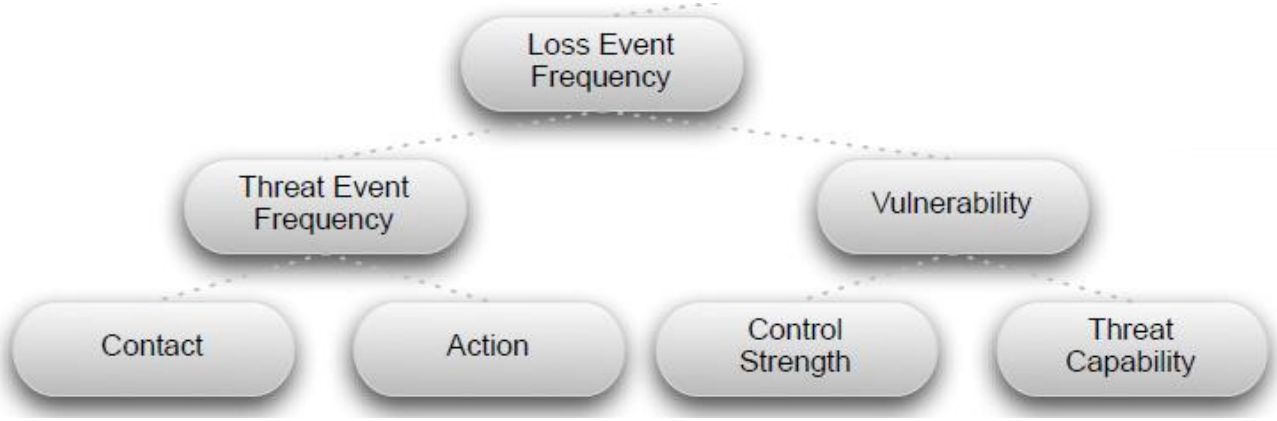
- 10 steps in 4 stages:
  - Stage 1-Identify Scenario Components
    - Identify the asset at risk
    - Identify the threat community under consideration

The probable frequency and probable magnitude of future loss



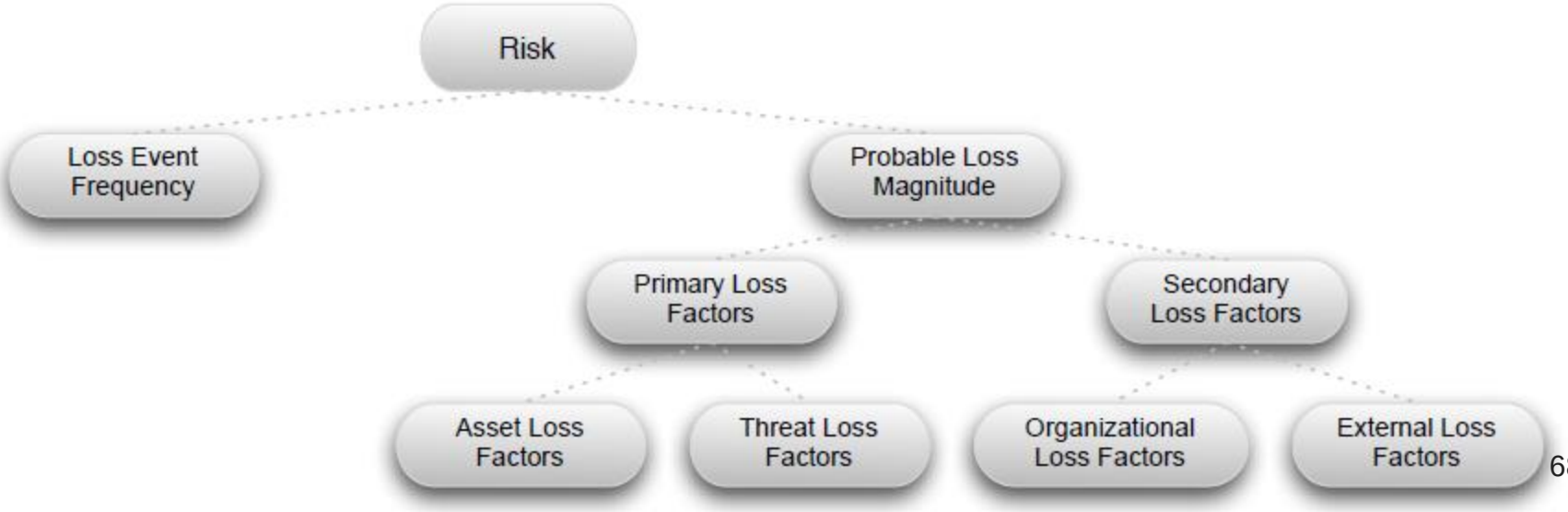
FAIR

- 10 steps in 4 stages:
  - 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

- 10 steps in 4 stages:
  - 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



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