Information Risk Management - Group 4

Brandon Ngo, Wally Lu, Ben Wishart, Tony Lee, Qi Mao

Module 1 - Introduction

Risk Management Principle and Definition

- Risk Management
    - Process of identifying risk, evaluating the costs associated with risk, taking steps to reduce risk to an acceptable level, and then maintaining that acceptable level of risk.
- Risk
    - Possibility that some harm may occur and have a negative effect on an asset. In general risk represents a loss that might happen
- Hazards
    - Potential situation with a conceivable threat to persons, assets or environment.
- Threats
    - Anything that can cause harm to people or property

Risk Assessment

- **Risk = (impact) * (likelihood of occurrence)**
- **Impact** can be thought of as the expected loss that comes with the risk
  - Replacement cost of asset (if physical)
  - Customer goodwill, cascading losses to other assets
- **Likelihood** can be thought of as the probability of the risk happening

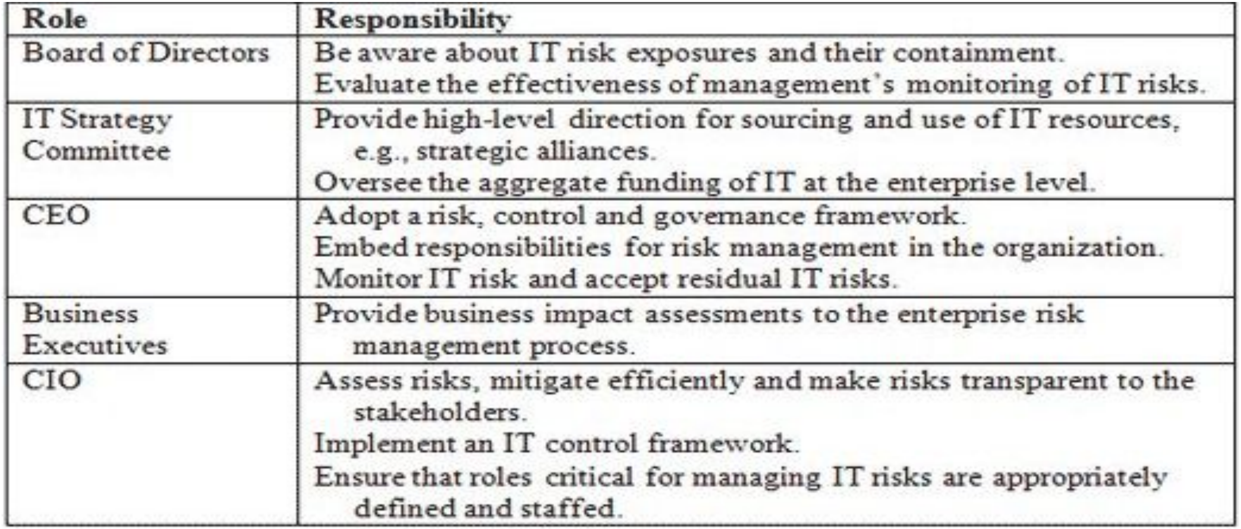
Information Security Risk Management (ISRM)

- Overall goals of ISRM include **computer security**, **information systems security,** and **information assurance**.
- ISRM different from traditional Risk Management
  - “the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing" (GAO, 1999).
- Major activities include
  - Assessment of assets
  - ID and vulnerability to threats
  - Impact, likelihood, loss and protection analysis, & cost-benefit analysis

Information Security Program Objectives

- Managing risks
- Develop Security Program
- Assign responsibilities
- Promote awareness
- Monitor controls
- Implement corrective action

Risk Management Roles & Responsibilities



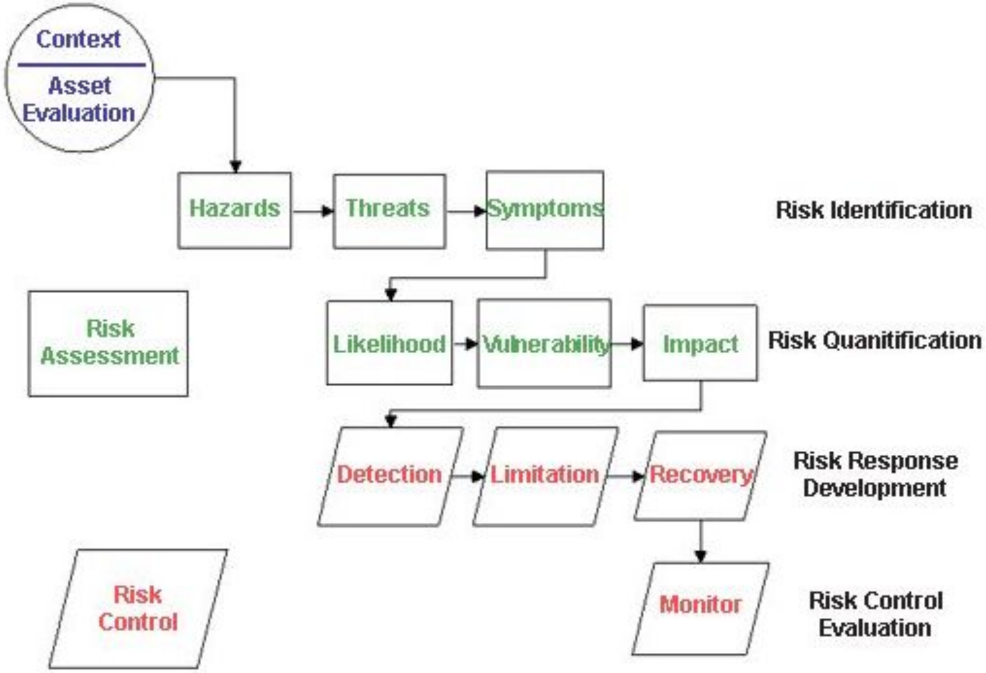
Role	Responsibility
Board of Directors	Be aware about IT risk exposures and their containment. Evaluate the effectiveness of management's monitoring of IT risks.
IT Strategy Committee	Provide high-level direction for sourcing and use of IT resources, e.g., strategic alliances. Oversee the aggregate funding of IT at the enterprise level.
CEO	Adopt a risk, control and governance framework. Embed responsibilities for risk management in the organization. Monitor IT risk and accept residual IT risks.
Business Executives	Provide business impact assessments to the enterprise risk management process.
CIO	Assess risks, mitigate efficiently and make risks transparent to the stakeholders. Implement an IT control framework. Ensure that roles critical for managing IT risks are appropriately defined and staffed.

Risk Management Roles and Responsibilities (ITGI, 2005)

Risk Management Frameworks

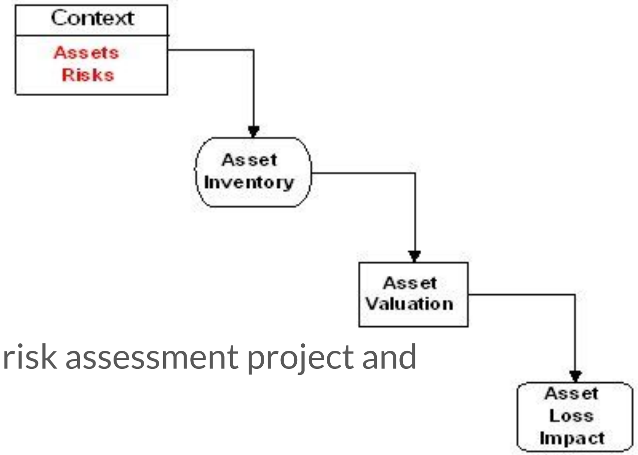
- **Risk management frameworks** describe the business and/or technical processes and the key activities within those processes that are believed to be needed for effective risk management.
- Specification of responsibility/accountability, Risk analysis, & Risk management plan to reduce risks to acceptable level
- OCTAVE Method
- FISMA (combined with NIST) Framework
- ITGI's COBIT Framework
- ISO 27001/27002

IT Risk Management Process



Course Risk Processes

Module 2 - Risk Management Context



Risk Management Context

- **System Characterization:** Process of establishing the scope of the risk assessment project and identifying operational boundaries
- **Asset Evaluation:** Process of determining the value and importance of the organization’s assets
- **Business Impact Analysis:** documenting and analyzing how the various business functions within an organization are affected by the loss or damage to an IT physical asset.

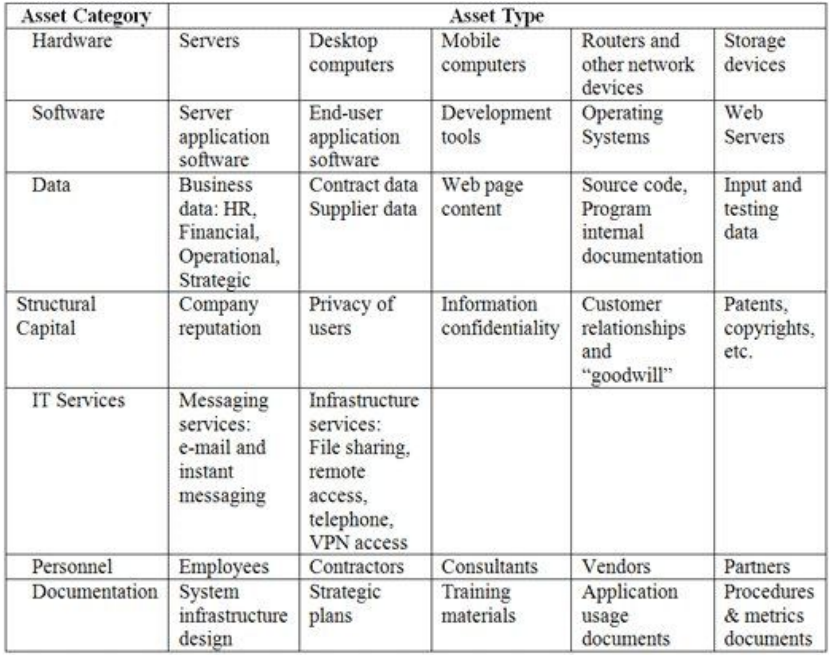
Risk Management: Identifying The Assets

- **IT Components:** Identifying the assets that need to be protected
  - People
  - Physical Items
  - Intangible Items With PHysical Manifestations
  - Pure Intangibles

Information Assets

Methods to collect Asset Inventory Data

- document reviews,
- visual inspection,
- automated tools,
- and personal interviews.
- To ensure accuracy, key asset attributes should be verified.

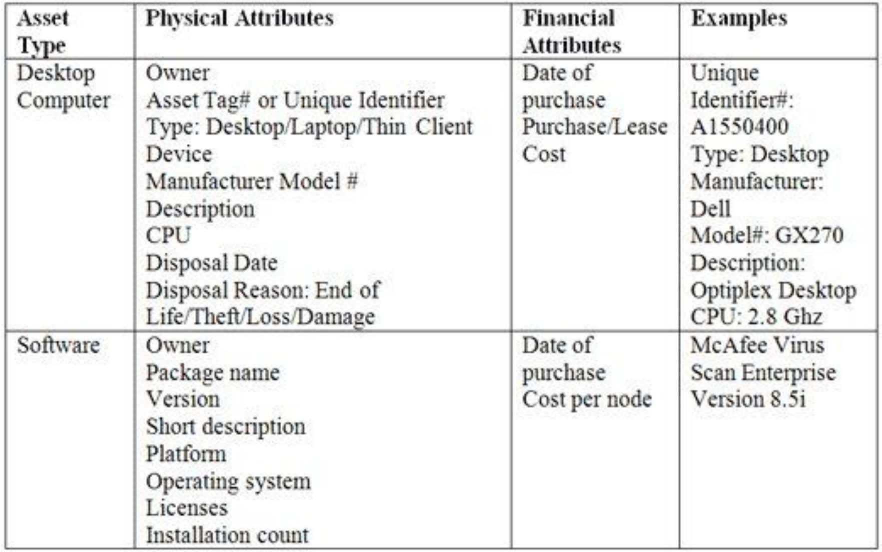


Asset Category	Asset Type				
Hardware	Servers	Desktop computers	Mobile computers	Routers and other network devices	Storage devices
Software	Server application software	End-user application software	Development tools	Operating Systems	Web Servers
Data	Business data: HR, Financial, Operational, Strategic	Contract data Supplier data	Web page content	Source code, Program internal documentation	Input and testing data
Structural Capital	Company reputation	Privacy of users	Information confidentiality	Customer relationships and "goodwill"	Patents, copyrights, etc.
IT Services	Messaging services: e-mail and instant messaging	Infrastructure services: File sharing, remote access, telephone, VPN access			
Personnel	Employees	Contractors	Consultants	Vendors	Partners
Documentation	System infrastructure design	Strategic plans	Training materials	Application usage documents	Procedures & metrics documents

Common Computer System and Information Assets

Information Assets: Hardware and Software Asset Attributes

The table to the right provides examples of hardware and software asset attributes that may be documented during the asset evaluation process. This list may be expanded to include other hardware assets such as printers/plotters, network routers, network switches, network hubs, network bridges, network gateways, mainframes, mainframe controllers, mainframe tape storage devices, mainframe disk storage devices, and servers.

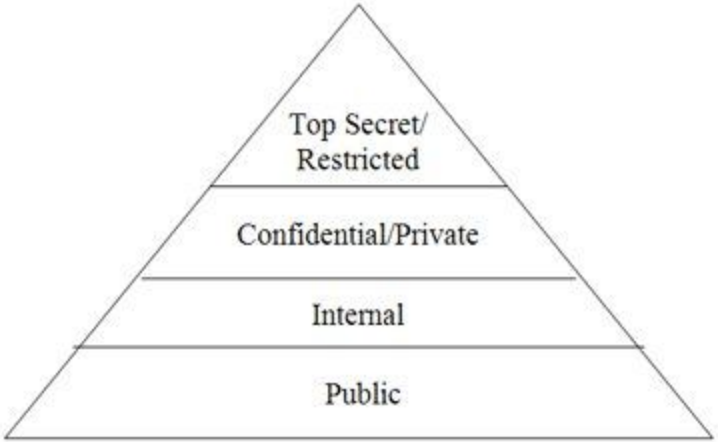


Asset Type	Physical Attributes	Financial Attributes	Examples
Desktop Computer	Owner Asset Tag# or Unique Identifier Type: Desktop/Laptop/Thin Client Device Manufacturer Model # Description CPU Disposal Date Disposal Reason: End of Life/Theft/Loss/Damage	Date of purchase Purchase/Lease Cost	Unique Identifier#: A1550400 Type: Desktop Manufacturer: Dell Model#: GX270 Description: Optiplex Desktop CPU: 2.8 Ghz
Software	Owner Package name Version Short description Platform Operating system Licenses Installation count	Date of purchase Cost per node	McAfee Virus Scan Enterprise Version 8.5i

Examples of Asset Attributes

Types Of Information Assets

- Customer Information
- Production Information
- Business Process information
- Management information
- Human Resource Information
- Supplier information



Information Classification Hierarchy (Gartner, 2005)

NIST IT Security Framework

- **System Identification:** assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.
- **System Criticality**: rating the system's sensitivity based on three security objectives: confidentiality, integrity, and availability.
- **Inter-Connected Systems**: involves identifying interconnected systems and boundary controls. System dependencies are important because a non–critical system may act as an upstream or downstream component to a critical system.

Module 3 - Risk Identification Process

Risk Identification Process

- Risk identification is one of many processes involved in risk management.
- There are three sub processes within the risk identification process
  - Hazard identification
  - Threat identification
  - Symptom itemization
- Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
- Risk – The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
- Hazard - A living person or inanimate object that can pose or act on a threat to assets.

Hazard Itemization

- The first step in the risk identification process, goal is to itemize hazards within the context that has been set for the overall risk management plan.
- Approaches to identify risks can include risk questionnaires, taxonomies, brainstorming, scenario analysis, lessons learned, and prototyping.
- Hazard context is characterized by different dimensions but characterization by cause is the most common.
- “The goal of threat identification is to identify the potential threat-sources [hazards] and prepare a threat statement listing those threat sources that apply to the IT system being evaluated” (NIST 800-30, 2002)

Hazard Itemization cont.

- More classification breakdowns:
    - Business Risks vs Pure Risks
        - External vs Internal - whether the cause of the risk/hazard lie outside or inside the organization.
    - Organizational vs Project Hazards
        - Hazards that pose threats to the organization’s overall health vs a project’s health which does not necessarily affect the company as a whole.

Threat Identification

- Risk identification frameworks have been proposed by a number of groups, both IT and related and not.
- Framework examples:
  - ACM’s risk identification framework
  - The NSTISSI model
- These frameworks are used by organizations to have a guideline to follow for their risk/threat identification process.

Threat Identification cont.

- CIA of information security
  - Confidentiality - information is confidential and known only to those with authority to know.
  - Integrity - information is truthful and hasn’t been tampered with.
  - Availability - information is available to individuals with authority to access and only those individuals.
- Common cyber threats
  - Top 3 according to FBI: insider abuse of internal access, viruses, laptop or mobile device theft

Symptom Itemization

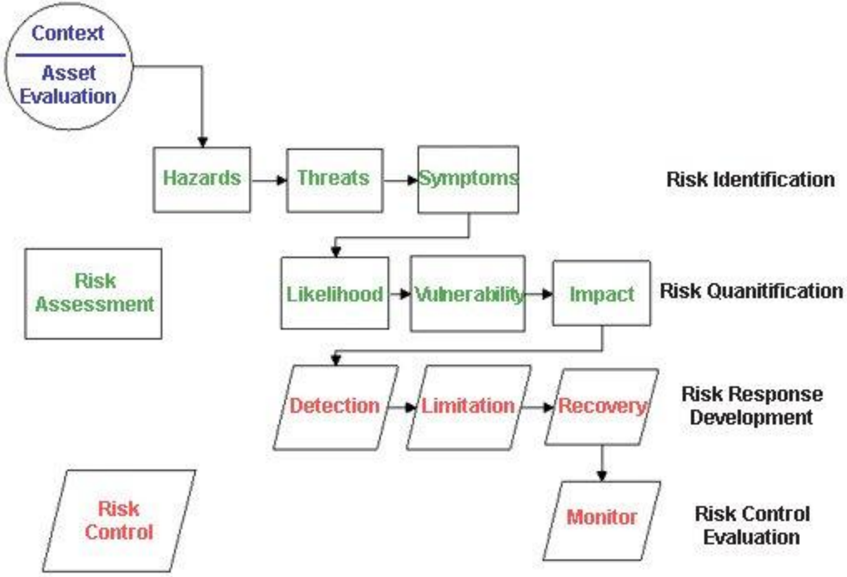
- Risk symptoms are physical or virtual signs that a problem is a about to occur or has occurred.
- Symptoms can be early warning signals that a problem is about to occur.
- Risk symptoms can be at the overall hazard level or the individual threat level where a hazard affects a specific asset or asset type.
- Itemization of symptoms facilitates risk response and control mechanisms as it allows certains controls to be activated at the right time and circumstances.

Symptom Itemization cont.

- Pareto chart - classic engineering diagram that helps to focus attention on the most critical problems of a project by presenting information in order of priority--based on the 80/20 rule (80% of problems come from 20% of the activities)
- Cause-and-effect diagrams - an ishikawa/fishbone diagram that tracks and links various causes and problems and their contribution to the overall problem.
- Symptom Itemization is a key part in the risk identification process as it’s one of the key factors in catching risks.

Module 4

Risk Quantification



Course Risk Processes

Quantification Methods

It is important to be able to distinguish between:

Danger

Damage

Risk EMV = Threat-Probability x Vulnerability x Impact

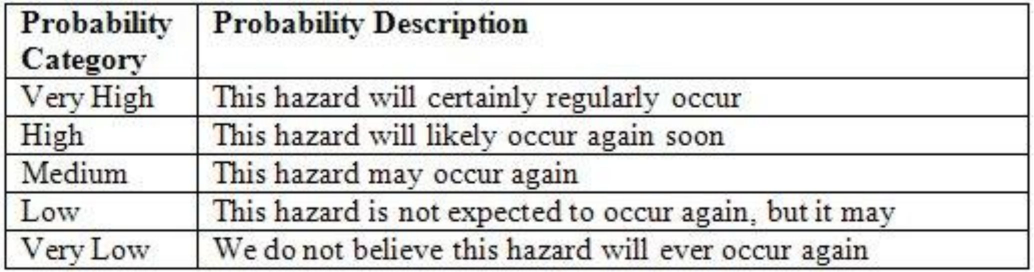
Business Risk vs. Pure Risk

Business - A risk of either a gain or a loss

Pure - a potential loss (Insurable risks)

Qualitative Methods

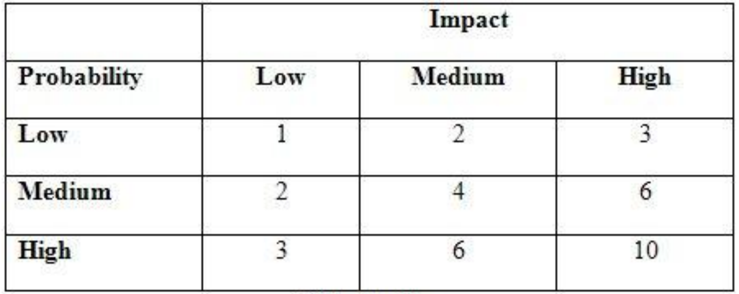
Qualitative methods attempt to rank probability and vulnerability in categories such as high, medium, and low.



Probability Category	Probability Description
Very High	This hazard will certainly regularly occur
High	This hazard will likely occur again soon
Medium	This hazard may occur again
Low	This hazard is not expected to occur again, but it may
Very Low	We do not believe this hazard will ever occur again

Qualitative Methods Cont.

Another similar method is based upon a risk matrix which gives a grade to the intersection of hazard probabilities and impacts.



	Impact		
Probability	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	10

Risk Grading

Human Malicious Hazards

People and groups can be divided into intentional (malicious) and non-malicious (accidental) hazards, and those can be further divided into internal and external people.

- Physical attacks
- Remote access control software
- Sabotage
- Terrorists
- Social engineering

Vulnerability Analysis

Vulnerability analysis is the process of developing a list of system flaws or weaknesses that could be exploited by potential hazards. Vulnerability is typically determined by questionnaires, walkthroughs (inspections), and testing such as penetration testing.

Organizational Risk Tolerance

To determine an acceptable risk level, the organization considers its legal and regulatory requirements as well as its business drivers and objectives. The acceptable risk level is reflected in the organization's information security policies, standards, guidelines and procedures.

Module 5 - Risk Control

Risk Control

- The results from the risk identification step acts as the inputs for the risk control step which seeks to illustrate the methodology for risk control process.
  - Steps in the risk control process:
    - Risk detection
    - Risk limitation
    - Risk recovery
    - Risk plan monitoring
- Based on the results of the risk identification process and stakeholder risk tolerance an organization will then need to determine what risks to accept and which risks to mitigate.

Risk Mitigation

- NIST's suggested risk mitigation methodology includes seven steps (NIST 800-30, 2002):
  - Prioritize actions
  - Evaluate recommended control options
  - Conduct cost-benefit analysis
  - Select controls
  - Assign responsibility
  - Develop safeguard implementation plan
  - Implement selected controls
- Risk response involves four activities: detection, limitation, reaction, and recovery

Risk Detection

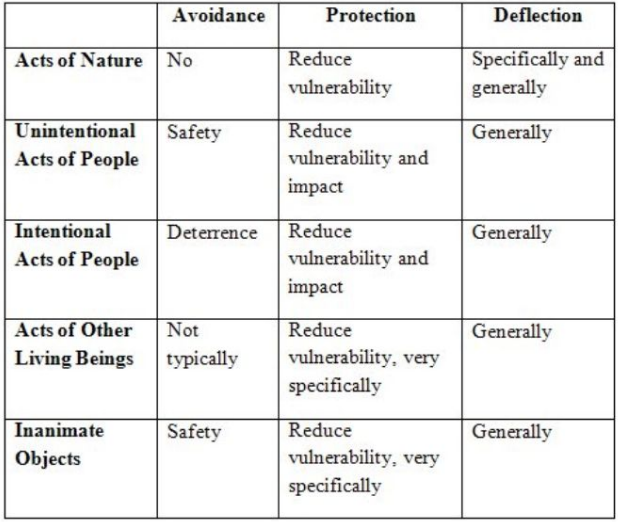
- Risk detection means to observe and look for risks
- There are a few ways that an organization could accomplish this such as audits and detection systems
  - Layered defenses like firewalls can also detect and notify of possible risks

Risk Limitation

- NIST outlines six risk mitigation options to implement risk limitation (NIST 800-30, 2005):
    - Risk assumption/acceptance
    - Risk avoidance
    - Risk limitation
    - Risk planning
    - Research and acknowledgement
    - Risk transference

Risk Limitation cont.

- There are four control methods:
  - Avoidance - reducing risk by reducing the probability of the hazard event occurring
  - Protection - reducing impact of and/or vulnerability to hazards
  - Deflection - transfer risk in part or completely to another party
    - Insurance, outsourcing, procurement/contracts
  - Acceptance - taking on the risk and the damages it can create
- This does not eliminate the risk it just transfers it and reduces it.
- For risk limitation you could use a risk template
  - Details information, parameters, and responses for the associated hazards and threats



	Avoidance	Protection	Deflection
Acts of Nature	No	Reduce vulnerability	Specifically and generally
Unintentional Acts of People	Safety	Reduce vulnerability and impact	Generally
Intentional Acts of People	Deterrence	Reduce vulnerability and impact	Generally
Acts of Other Living Beings	Not typically	Reduce vulnerability, very specifically	Generally
Inanimate Objects	Safety	Reduce vulnerability, very specifically	Generally

Cyber Security Controls

- NIST has recommended security controls for federal information systems that fall into categories:
    - Access Control
    - Awareness and Training
    - Audit and Accountability
    - Certification, Accreditation, and Security Assessments
    - Configuration Management
    - Contingency Planning
    - Identification and Authentication
    - Incident Response
    - Maintenance
    - Media Protection

Risk Safety and Prevention

- Risk Logs
  - Risks need to be monitored at all times, checking for identified symptoms
  - Describes risk, circumstances of occurence, risk response taken, degree of success of response, estimated cost of event
  - Improvements for the future
- Schedule for Evaluating Security Controls
  - Controls need to be evaluated and reevaluated on a regular basis, and also when risk events occur
  - Evaluation process evolves as the company evolves
  - Used to follow up and improve controls

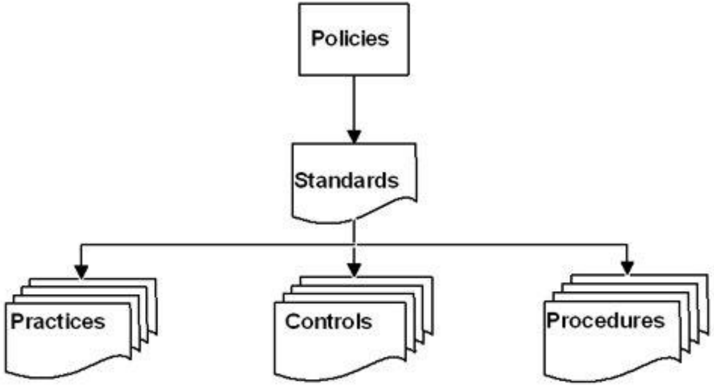
Module 6

Security and Risk Management Policy

Hazards, threats, threat agents, technology, controls, assets, and vulnerabilities will change over time; thus the success of any organization's security program ultimately lies with its overall security policy and program. The goal of an organizational security policy is to provide for the ongoing effectiveness, currency, and relevancy of the organization's security and risk management efforts.

Policy Cont

A policy is a written document containing guidelines and regulations which members of a group or organization must abide by. A policy will guide members toward actions that should be performed for a beneficial outcome, while discouraging undesirable actions that may negatively affect the organization.



System Plans Framework

For both the hazard specific policies and the system specific policies, the information outlined within the risk templates should be included and kept current.

1. **Information System Name/Title**:
   - Unique identifier and name given to the system.
2. **Information System Categorization**:
   - Identify the appropriate FIPS 199 categorization (low, moderate, high).
3. **Information System Owner**:
   - Name, title, agency, address, e-mail address, and phone number of person who owns the system.

FISMA

The **Federal Information Security Management Act of 2002 (FISMA)** is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The Act is designed to improve IT security within the US government and related parties (especially government contractors) by mandating yearly audits. FISMA defines a set of security steps that must be followed, and the processes involved must follow a combination of Federal Information Processing standards (FIPS).

COBIT

- **Control Objectives for Information and related Technology**
  - Not only a standard, also a reference
  - Set of best practices for IT management created by ISACA and ITGI
  - Useful for managers, IT users and auditors
- **MISSION**
  - **Its mission is to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors**
- **Four Domains**
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support

Plan And Organize & Acquire And Implement

- **P & O:** How to best use information technology to achieve company’s goal

- **A & I:** identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes.

Delivery And Support & Monitor And Evaluation

- **D & S:** It covers areas such as the execution of the applications within the IT system and its results, as well as the support processes that enable the effective and efficient execution of these IT systems
- **M & E:** Focuses on the organization's strategy in the needs of that company

Sources

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/
- https://nvd.nist.gov/800-53/Rev4/control/CA-3
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf