C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

CS 668: Risk Identification and Assessment for Information Security

This lecture is about information security risk – from which we will move to ICS/OT security risk and risk assessment in subsequent lectures

Acknowledgement

- **Dr Loai Tawalbeh and Muna Ahmed, Jordan University of Science and Technology**

Main topics

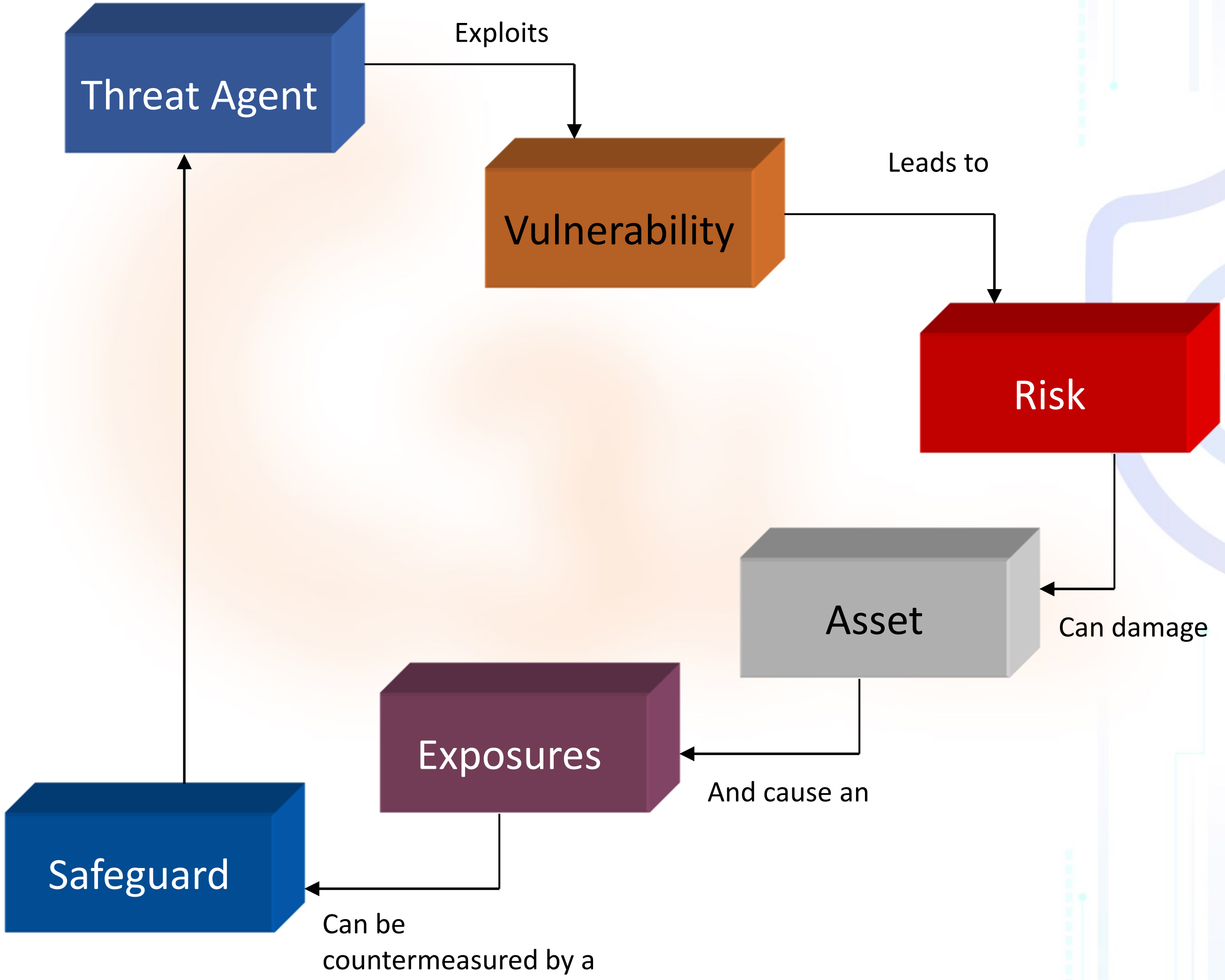
- What is Risk & Risk management?
- Risk Management Cycle
- Risk Identification
- Primary sources of Risk Items
- What is Risk Assessment ?
- How to assess the risks ?
- Risk Assessment methodologies
- Methods of Risk Assessment
- Who is responsible in risk assessment?

What is Information Security Risk & Risk Management?

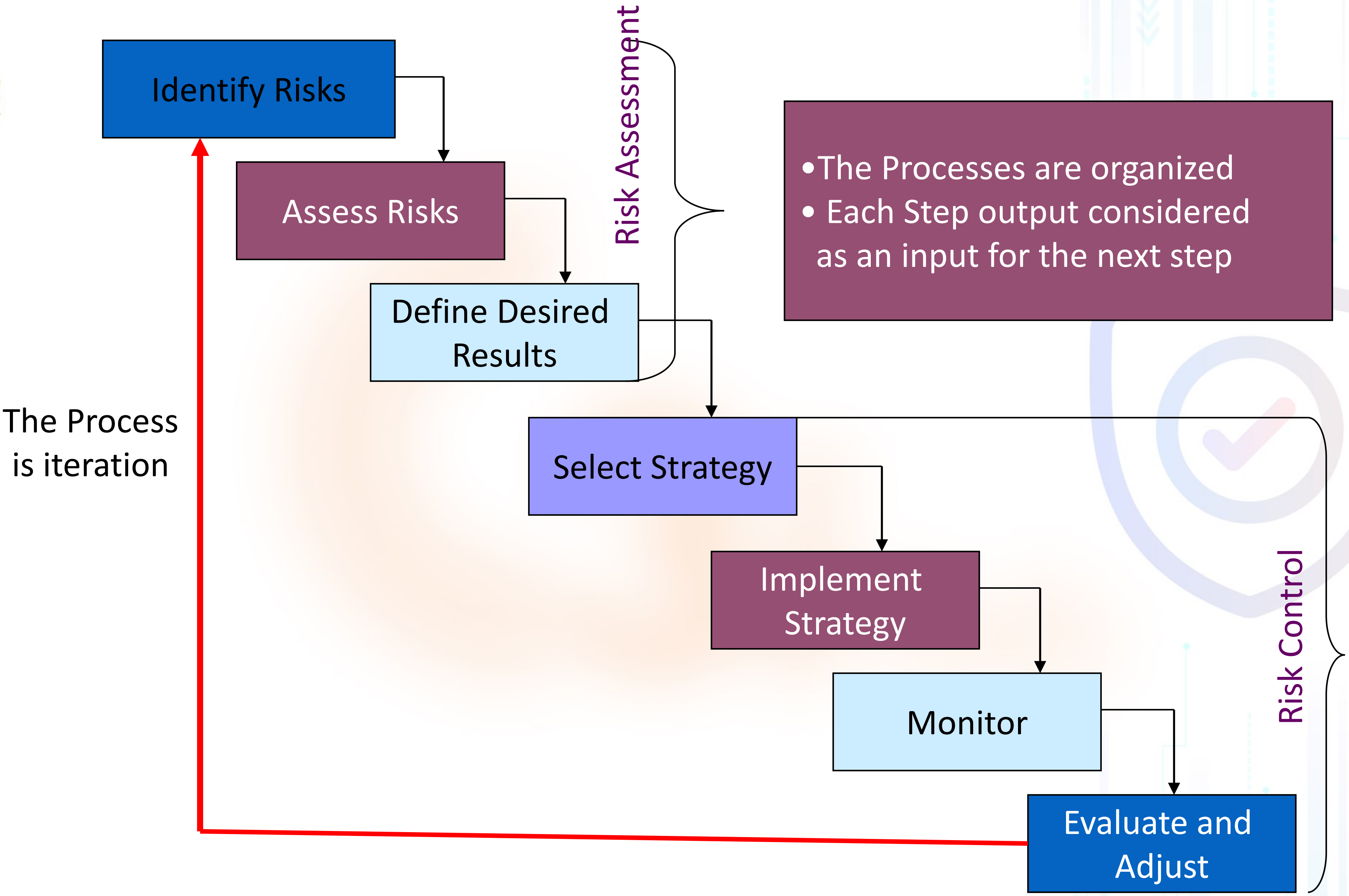
- *Risk : The is an object, person or other entity that represent a danger, harm or loss to an asset*
  - *May have to be qualified with a scoring method*

- *Risk Management : Is the process of Identifying , assessing and evaluating the level of risk facing the organization*
  - *specifically the threats to the information stored and used by organizations for achieving business objectives*
  - *deciding what countermeasures, if any, to take in reducing risk to an acceptable level,*
    - *based on the value of the information resource to the organization*

Risk Life Cycle



Risk Management Cycle



- The Processes are organized
- Each Step output considered as an input for the next step

Risk Management

- “If you know the enemy and know yourself, you need not fear the results of a hundred battles
- If you know yourself and not the enemy, for every victory gained, you will also suffer a defeat
- If you know neither the enemy nor yourself, you will succumb in every battle”

Sun Tzu

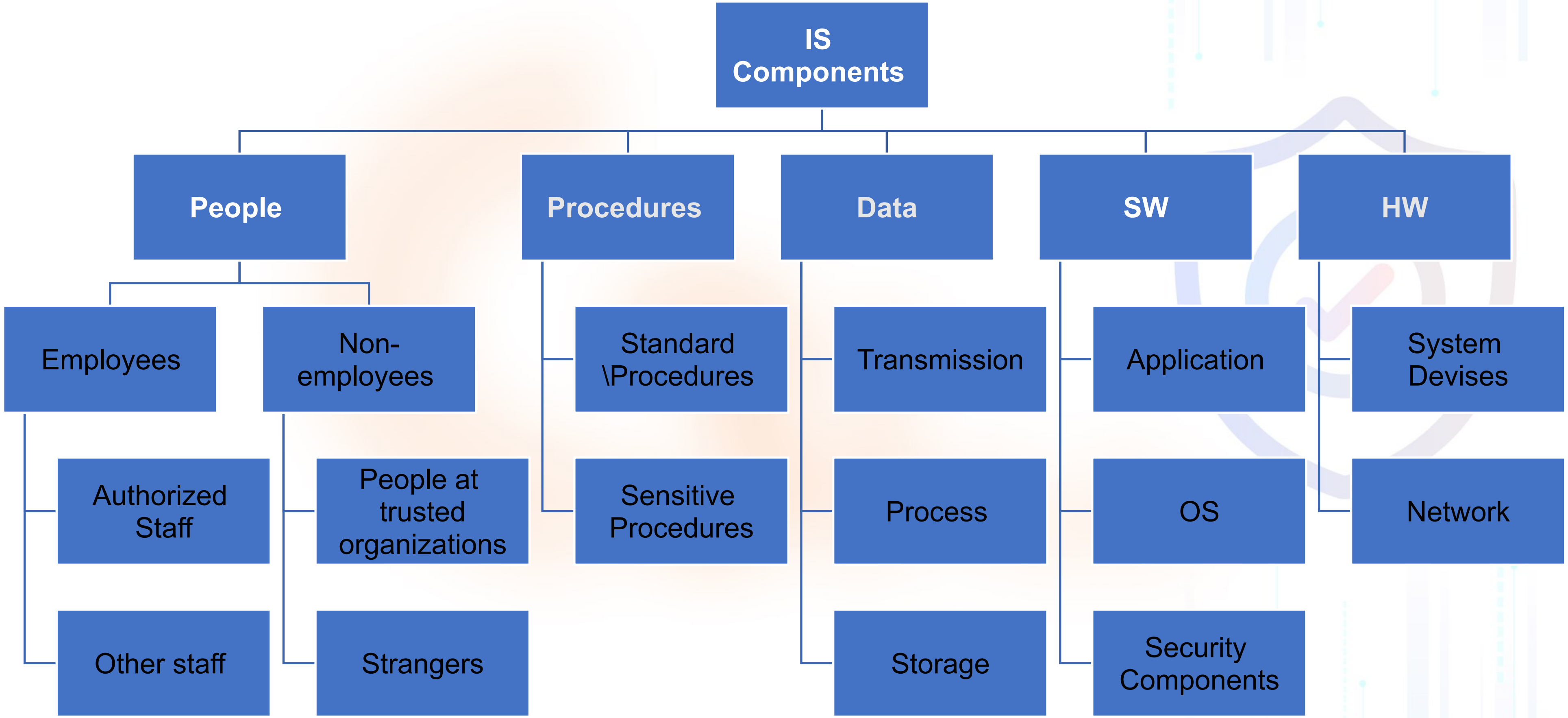
The Art of War

Risk Identification

What is the purpose of this phase ?

- The aims of this phase is to identify , classify and prioritizing the organization’s information assets (Know ourselves)
- identify all important types and sources of risk and uncertainty (know our enemy), associated with each of the investment objectives.
- This is a crucial phase.
  - *If a risk is not identified it cannot be evaluated and managed*

Information Assets



IS Components

People

- Employees
  - Authorized Staff
  - Other staff
- Non-employees
  - People at trusted organizations
  - Strangers

Procedures

- Standard \Procedures
- Sensitive Procedures

Data

- Transmission
- Process
- Storage

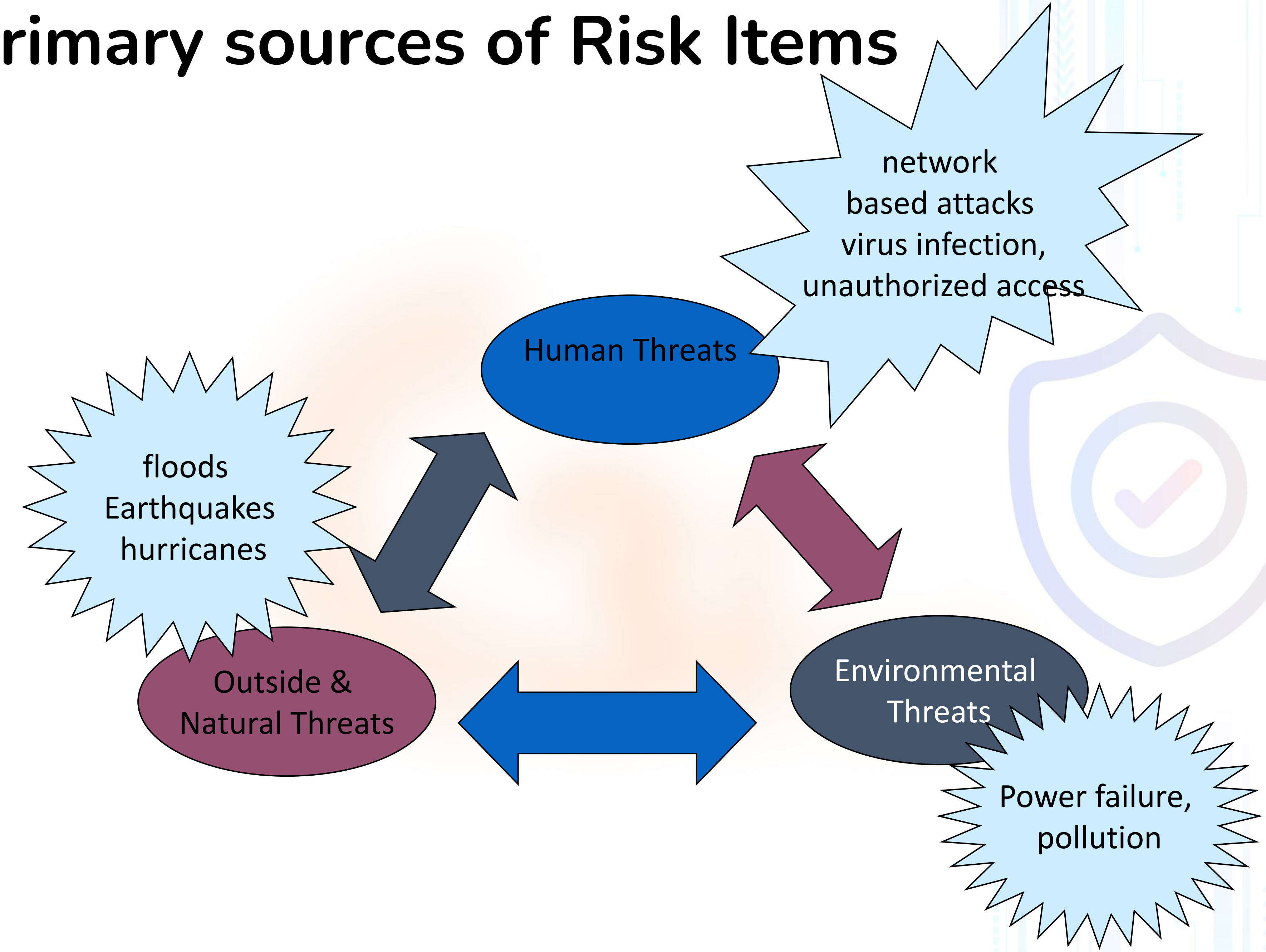
SW

- Application
- OS
- Security Components

HW

- System Devises
- Network

Primary sources of Risk Items



Human Threats

network based attacks virus infection, unauthorized access

Outside & Natural Threats

floods Earthquakes hurricanes

Environmental Threats

Power failure, pollution

Risk Assessment

- For each identified component & risk, which has a 'clearly significant' or 'possibly significant' position, each should be *assessed* to *establish qualitatively and estimate the value in terms of loss*

What is Risk Assessment ?

- Assessing risk is *the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise* , *i.e* determine the relative risk for each of the vulnerabilities

- Risk assessment assigns a risk rating or score to *each specific information asset*, useful in *evaluating the relative risk* and making comparative ratings later in the risk control process

- Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle.

- In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies

Methods of Risk Assessment

There are various methods assessing risk,

First : Quantitative risk assessment :

generally, estimates values of Information Systems components as ; information, systems, business processes, recovery costs, etc.,

risk can be measured in terms of direct and indirect costs , based on

(1) the likelihood that a damaging event will occur

(2) the costs of potential losses

(3) the costs of mitigating actions that could be taken.

Risk = Likelihood X consequences

Second : Qualitative Risk Assessment

This approach can be taken by defining

- **Risk in more subjective and general terms such as high, medium, and low.**
- **qualitative assessments depend more on the *expertise, experience, and judgment of those conducting the assessment*.**

- Qualitative risk assessments typically give risk results of "High", "Moderate" and "Low". However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization's management.

Third :Quantitative and Qualitative

- It is also possible to use a combination of quantitative and qualitative method

Difference in Risk Assessment for Insurance vs Information Systems

- Quantitative risk measurement is the standard way of measuring risk in many fields, such as insurance,
    - but it is not commonly used to measure risk in information systems.
- Two of the reasons claimed for this are
    - 1) the difficulties in identifying and assigning a value of all components
    - 2) Moral Effects couldn’t be measured by quantitative measurements
    - 2) the lack of statistical information that would make it possible to determine frequency.

- *Thus, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk.*

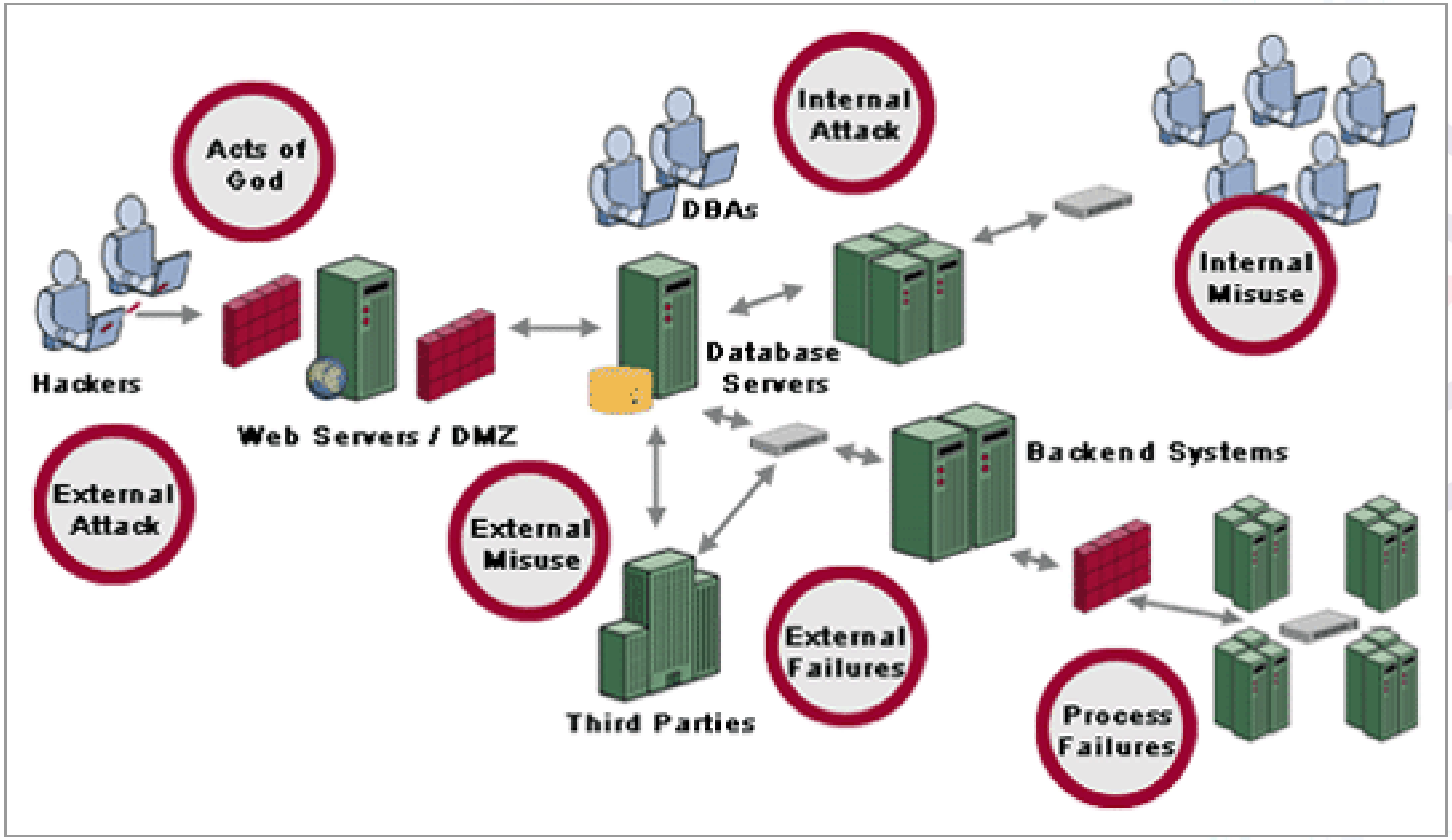
How to assess the risks

Risk is assessed by following the following steps :

- Identifying threats
- Identifying vulnerabilities
- Relating Threats to Vulnerabilities
- determining the likelihood
- Evaluate impact for each risk

Evaluate impact for each risk
determining the likelihood
Relating Threats to Vulnerabilities
Identifying vulnerabilities
Identifying threats

Identifying Risk



Identifying Vulnerabilities

- **Identifying Vulnerabilities** : how each of the threats that are possible or likely could perpetrate , and list the organization’s assets and their vulnerabilities
- Vulnerabilities can be identified by numerous means.
- **Different methodologies for identifying vulnerabilities**.
  - start with commonly available vulnerability lists.
  - working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system.
  - Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org) or the National Vulnerability Database (NVD - http://nvd.nist.gov).

Relating Threats to Vulnerabilities

- Not every threat-action/threat can be exercised against every vulnerability.

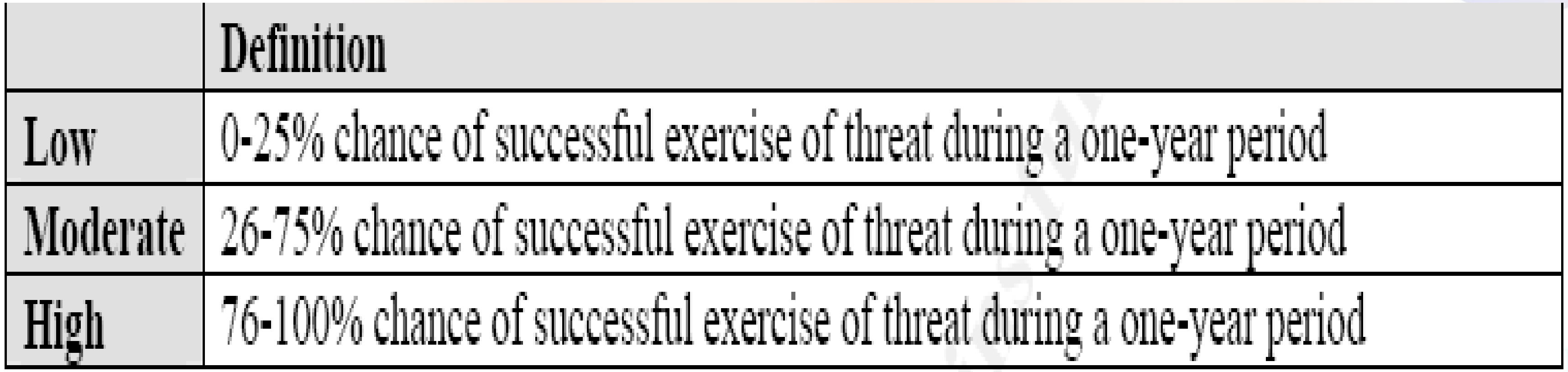
- For example, a threat of “flood” obviously applies to a vulnerability of “lack of contingency planning”, but not to a vulnerability of “failure to change default authenticators.”

Defining Likelihood

Likelihood is :

- the estimation of the probability that a threat will succeed in achieving an undesirable event
- is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited

- **Sample Likelihood Definitions**

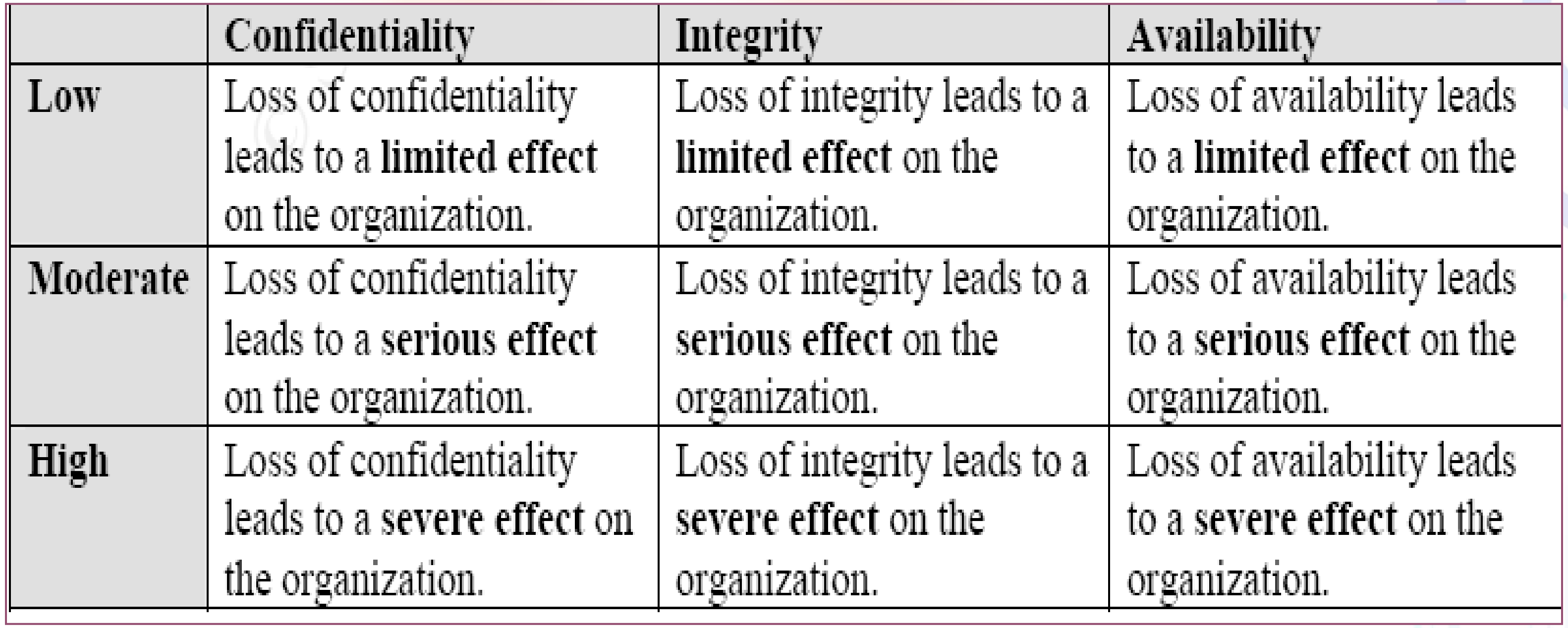


	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

Defining Impact

- impact (Value)
  - Using the information documented during the risk identification process, assign weighted scores based on the value of each information asset, i.e.1-100, low-med-high, etc.

Sample Impact Definitions

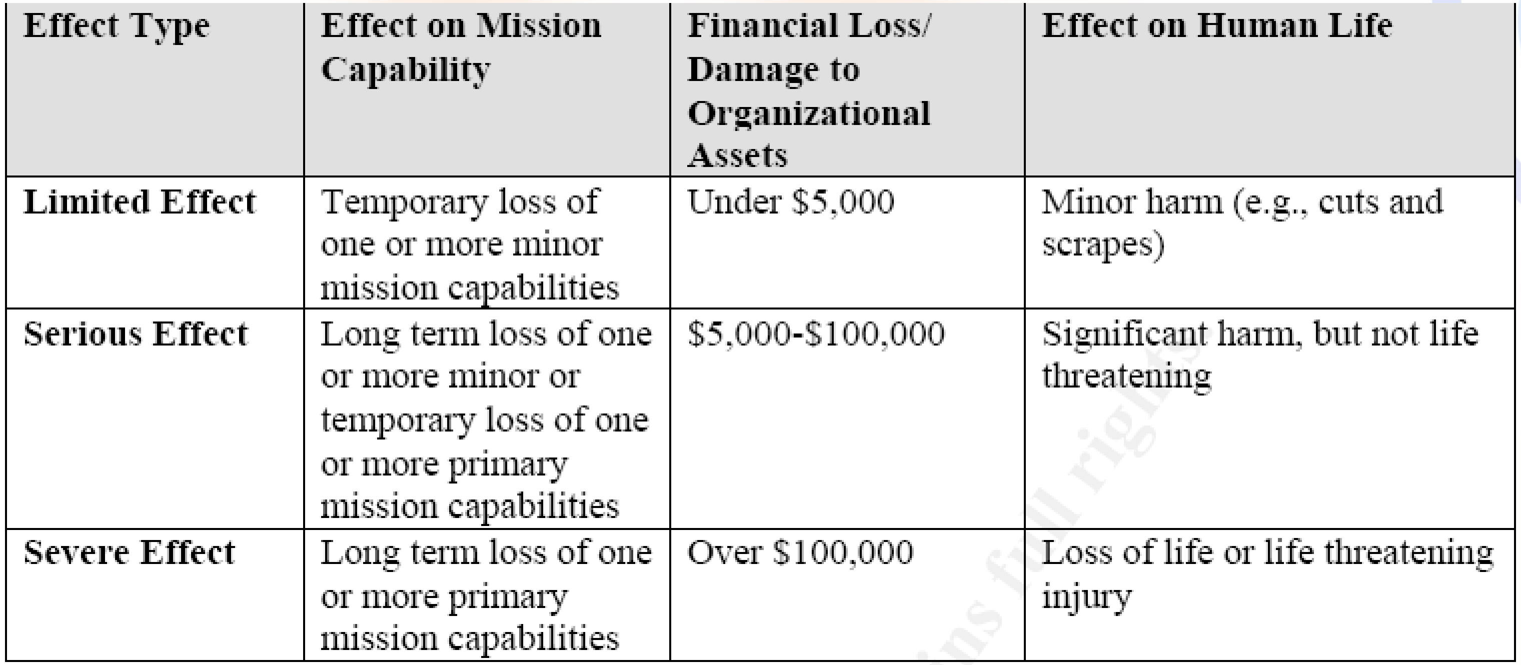


	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

Defining Impact

- However, in order the risk assessment to be meaningful, reusable and easily communicated, specific ratings should be produced for the entire organization as below example .

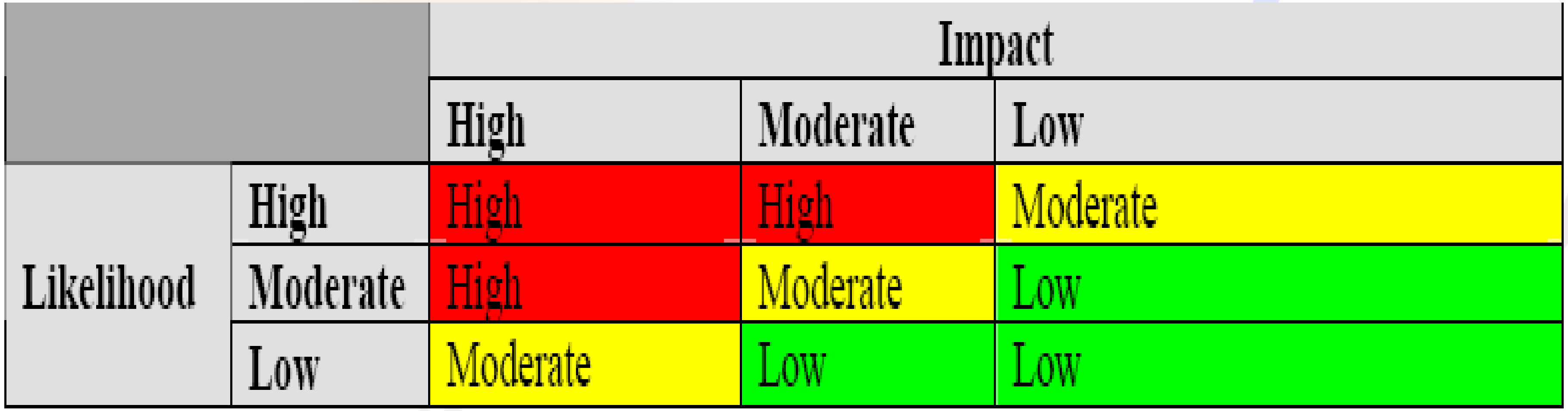
Examples of Organizational Effect



Effect Type	Effect on Mission Capability	Financial Loss/ Damage to Organizational Assets	Effect on Human Life
Limited Effect	Temporary loss of one or more minor mission capabilities	Under $5,000	Minor harm (e.g., cuts and scrapes)
Serious Effect	Long term loss of one or more minor or temporary loss of one or more primary mission capabilities	$5,000-$100,000	Significant harm, but not life threatening
Severe Effect	Long term loss of one or more primary mission capabilities	Over $100,000	Loss of life or life threatening injury

Risk Matrix

- **Sample Risk Determination Matrix**



		Impact		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Some Common Risk Assessment methodologies

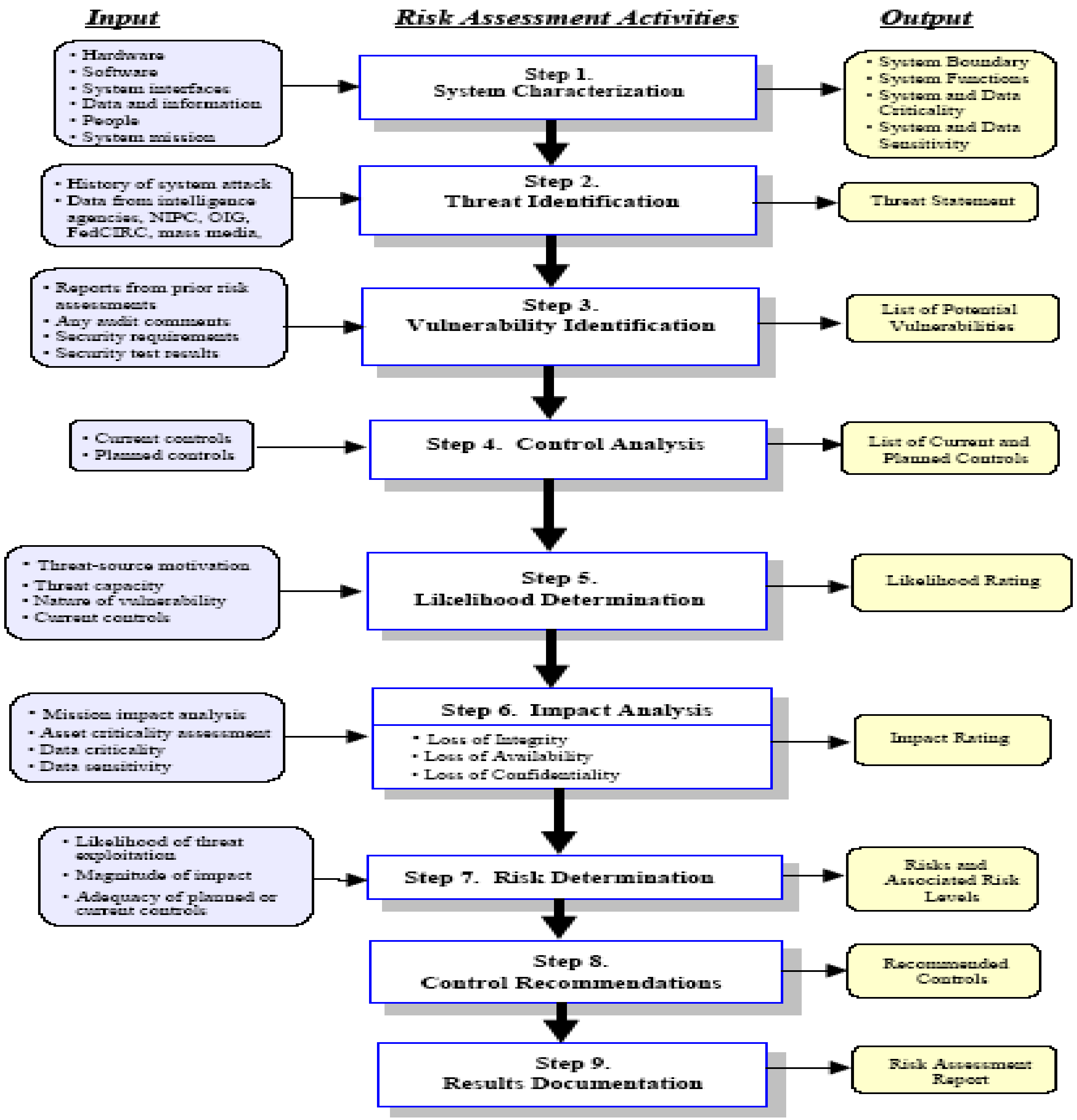
- The following methodologies and tools were developed for managing risks in information systems:
  - National Institute of Standards & Technology (NIST) Methodology
  - OCTAVE®
  - FRAP
  - COBRA
  - Risk Watch

National Institute of Standards & Technology (NIST)

- **(NIST) Methodology**
- NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* is the US Federal Government’s standard.
- This methodology is primarily designed to be qualitative and is based upon skilled security analysts working with system owners and technical experts to thoroughly identify, evaluate and manage risk in IT systems.

NIST Risk Assessment Methodology

- The NIST methodology consists of 9 steps each has inputs and out puts:
- • Step 1: System Characterization
- • Step 2: Threat Identification
- • Step 3: Vulnerability Identification
- • Step 4: Control Analysis
- • Step 5: Likelihood Determination
- • Step 6: Impact Analysis
- • Step 7: Risk Determination
- • Step 8: Control Recommendations
- • Step 9: Results Documentation



Input | ***Risk Assessment Activities*** | ***Output***

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1. System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2. Threat Identification

Threat Statement

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3. Vulnerability Identification

List of Potential Vulnerabilities

- Current controls
- Planned controls

Step 4. Control Analysis

List of Current and Planned Controls

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5. Likelihood Determination

Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

Step 8. Control Recommendations

Recommended Controls

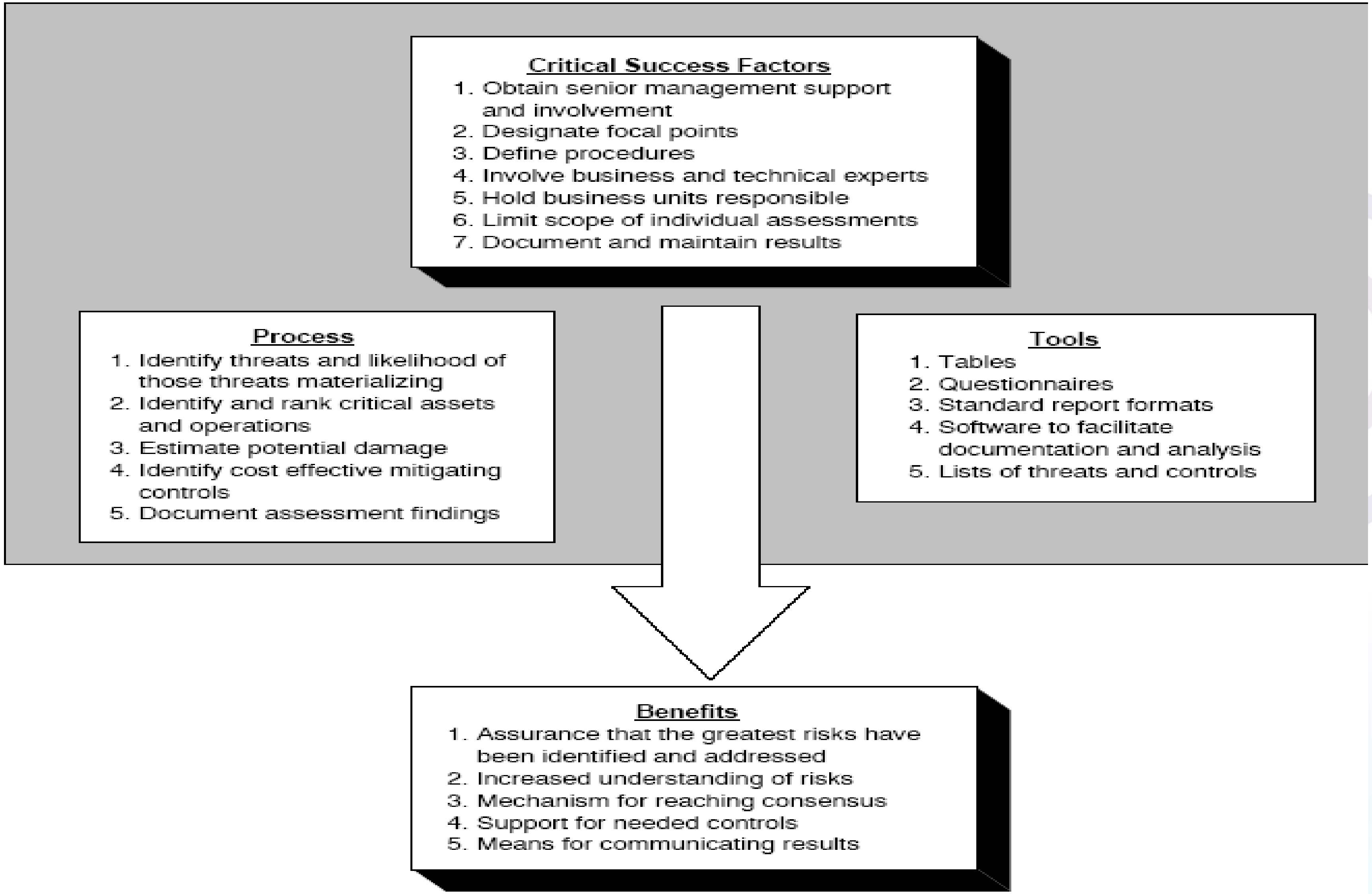
Step 9. Results Documentation

Risk Assessment Report

Who does the Assessment ?

- A risk assessment is carried out by a team of people who have knowledge of specific areas of the business.
- It is the responsibility of each community of interest to manage risks
- Each community has a role to play:
  - Information Security - best understands the threats and attacks that introduce risk into the organization
  - Management and Users – play a part in the early detection and response process - they also ensure sufficient resources are allocated
  - Information Technology – must assist in building secure systems and operating them safely

Summary of Risk Assessment Practices and Related Benefits



Critical Success Factors

1. Obtain senior management support and involvement
2. Designate focal points
3. Define procedures
4. Involve business and technical experts
5. Hold business units responsible
6. Limit scope of individual assessments
7. Document and maintain results

Process

1. Identify threats and likelihood of those threats materializing
2. Identify and rank critical assets and operations
3. Estimate potential damage
4. Identify cost effective mitigating controls
5. Document assessment findings

Tools

1. Tables
2. Questionnaires
3. Standard report formats
4. Software to facilitate documentation and analysis
5. Lists of threats and controls

Benefits

1. Assurance that the greatest risks have been identified and addressed
2. Increased understanding of risks
3. Mechanism for reaching consensus
4. Support for needed controls
5. Means for communicating results

A Case Study

Risk Assessment

"Regulatory Organization"

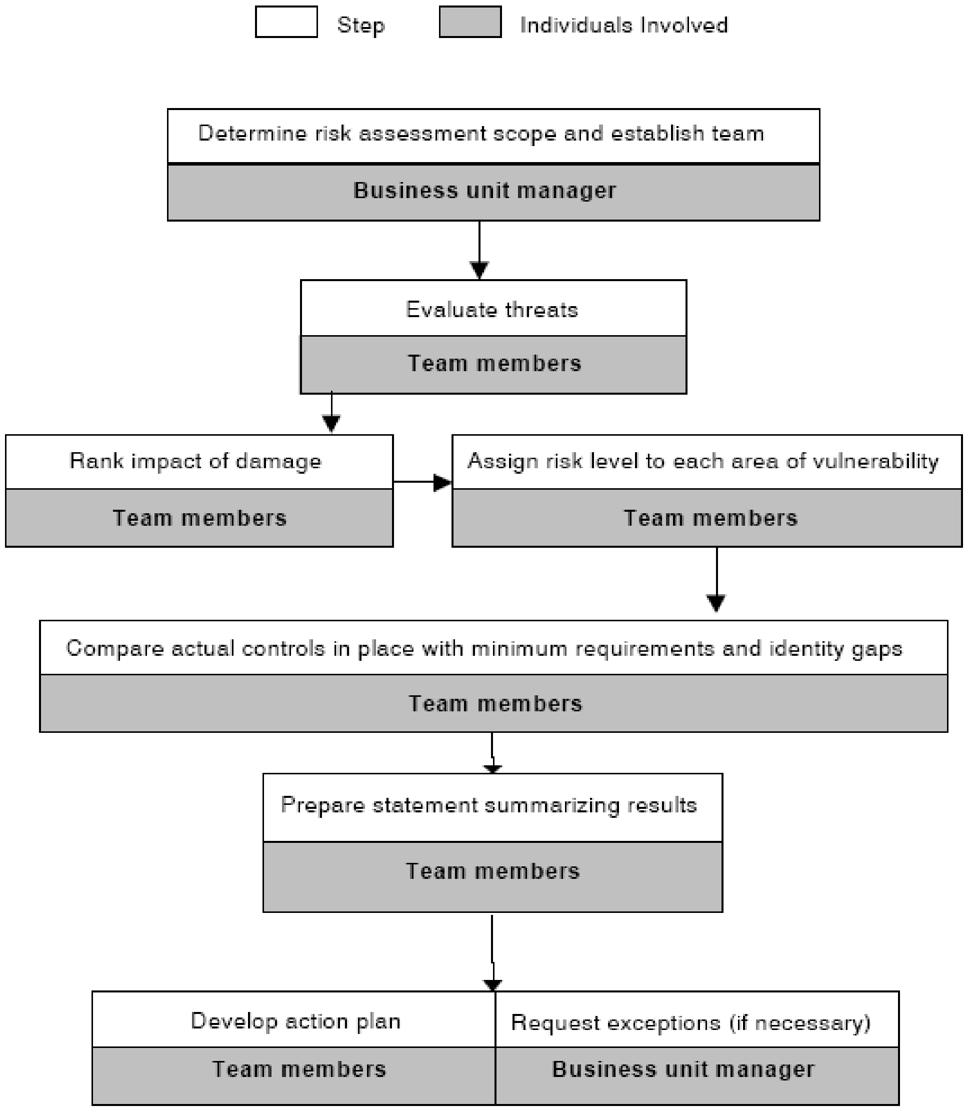
Regulatory Organization

The organization's objectives in its' risk management plan are : :

- To face any risk
- concerned with loss of customer confidence, as well as monetary and productivity losses.

- Risk assessments have always been a part of doing business that leads to determine the level of risk associated with a business function or process in order to determine the applicable security controls.
- The organization consists of a
  - **central office** who *issues organization wide information security risk assessment guidelines* and *establishes minimum control requirements*
  - **regional offices** *throughout the country* who facilitates the process in its geographic area; and individual business units are responsible for conducting the assessments.
- The organization's policy guidelines require
  - business units to conduct risk assessment at least once a year.
  - when a new business operation is established or when significant operational changes occur.

Risk Assessment Process



□ Step ▨ Individuals Involved

Determine risk assessment scope and establish team

Business unit manager

Evaluate threats

Team members

Rank impact of damage

Team members

Assign risk level to each area of vulnerability

Team members

Compare actual controls in place with minimum requirements and identity gaps

Team members

Prepare statement summarizing results

Team members

Develop action plan

Team members

Request exceptions (if necessary)

Business unit manager

Conducting and Documenting the Assessment

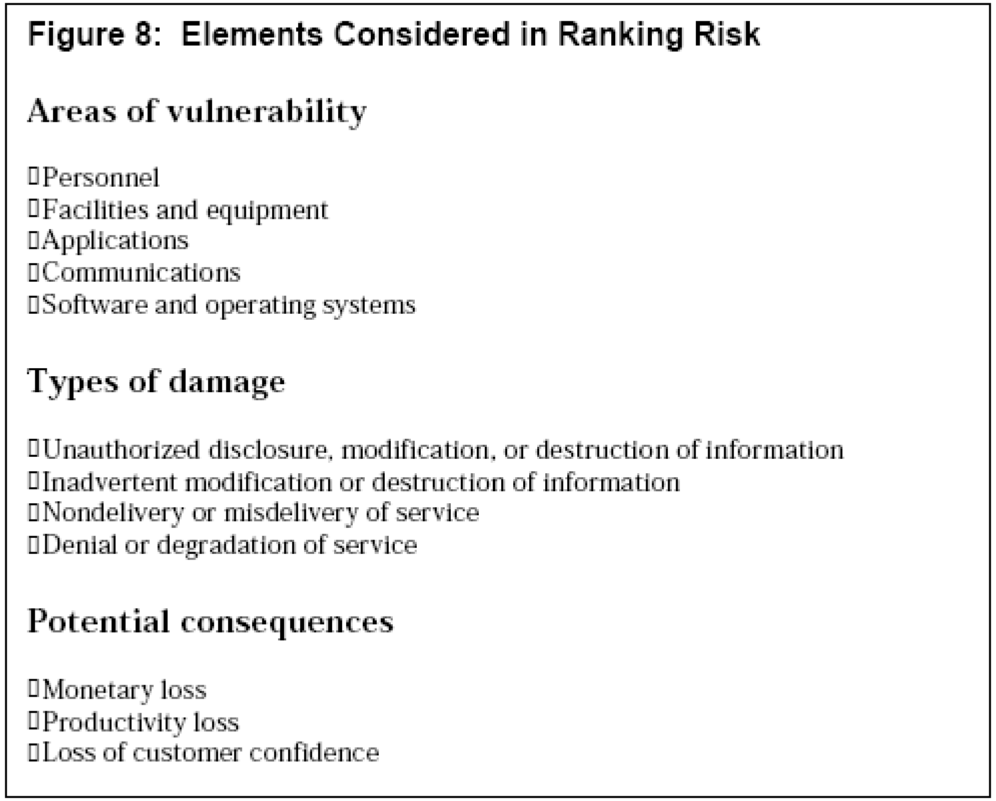


Figure 8: Elements Considered in Ranking Risk

Areas of vulnerability

□Personnel
□Facilities and equipment
□Applications
□Communications
□Software and operating systems

Types of damage

□Unauthorized disclosure, modification, or destruction of information
□Inadvertent modification or destruction of information
□Nondelivery or misdelivery of service
□Denial or degradation of service

Potential consequences

□Monetary loss
□Productivity loss
□Loss of customer confidence

The central office has incorporated these elements into a set of detailed guidelines for *conducting information security risk assessments complementary training manual elaborating on the guidelines* and *providing more detailed step-by-step procedures*.

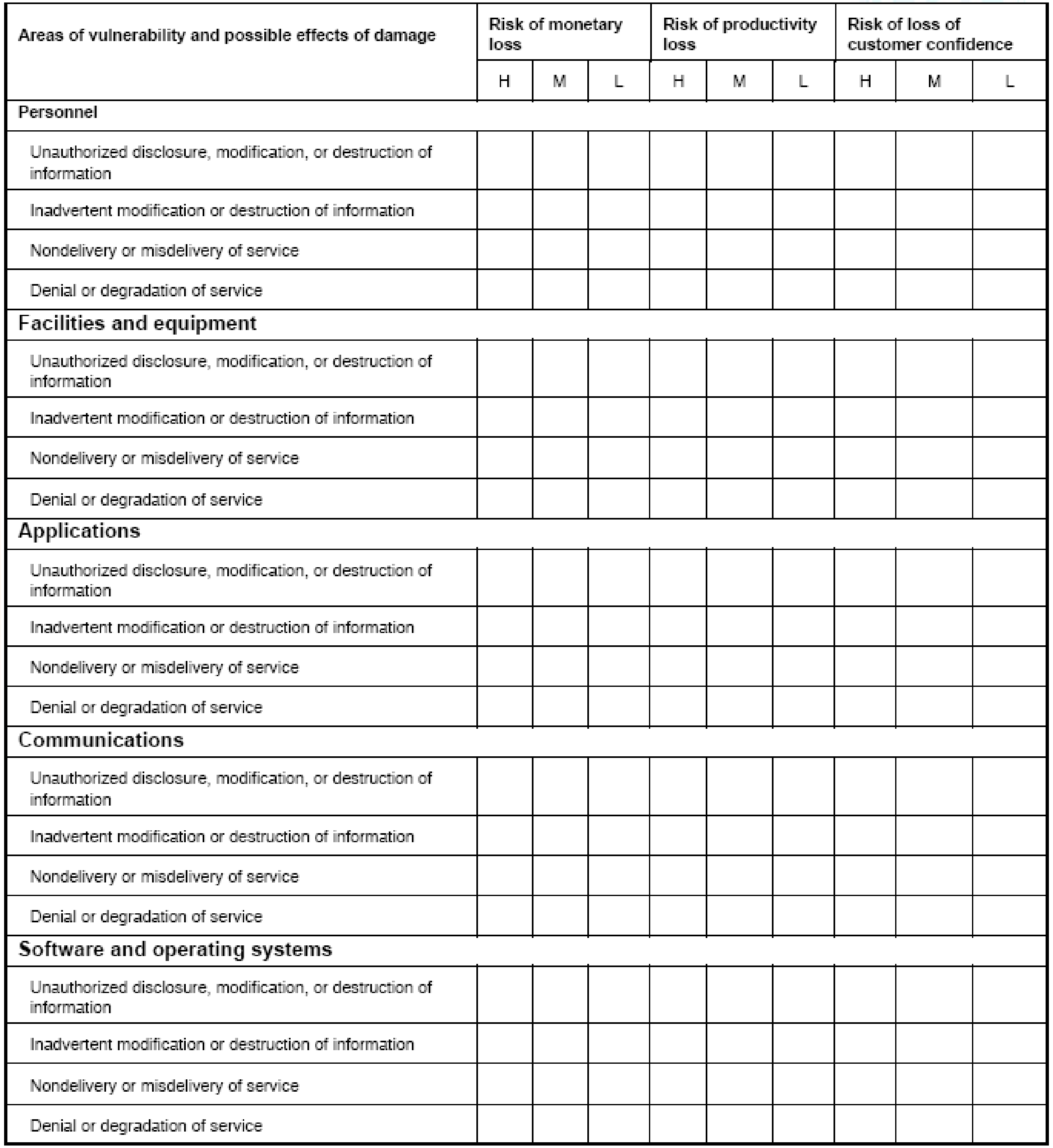
Determining Risk Level

- The team's first step is to evaluate possible threats to information security that may affect the unit's operations.

- The team assigns a risk level of high, moderate, or low for each area of vulnerability to show the possible effect of damage if the threat were to occur.

- The team uses a matrix to assist in its analysis of risk (risk matrix)

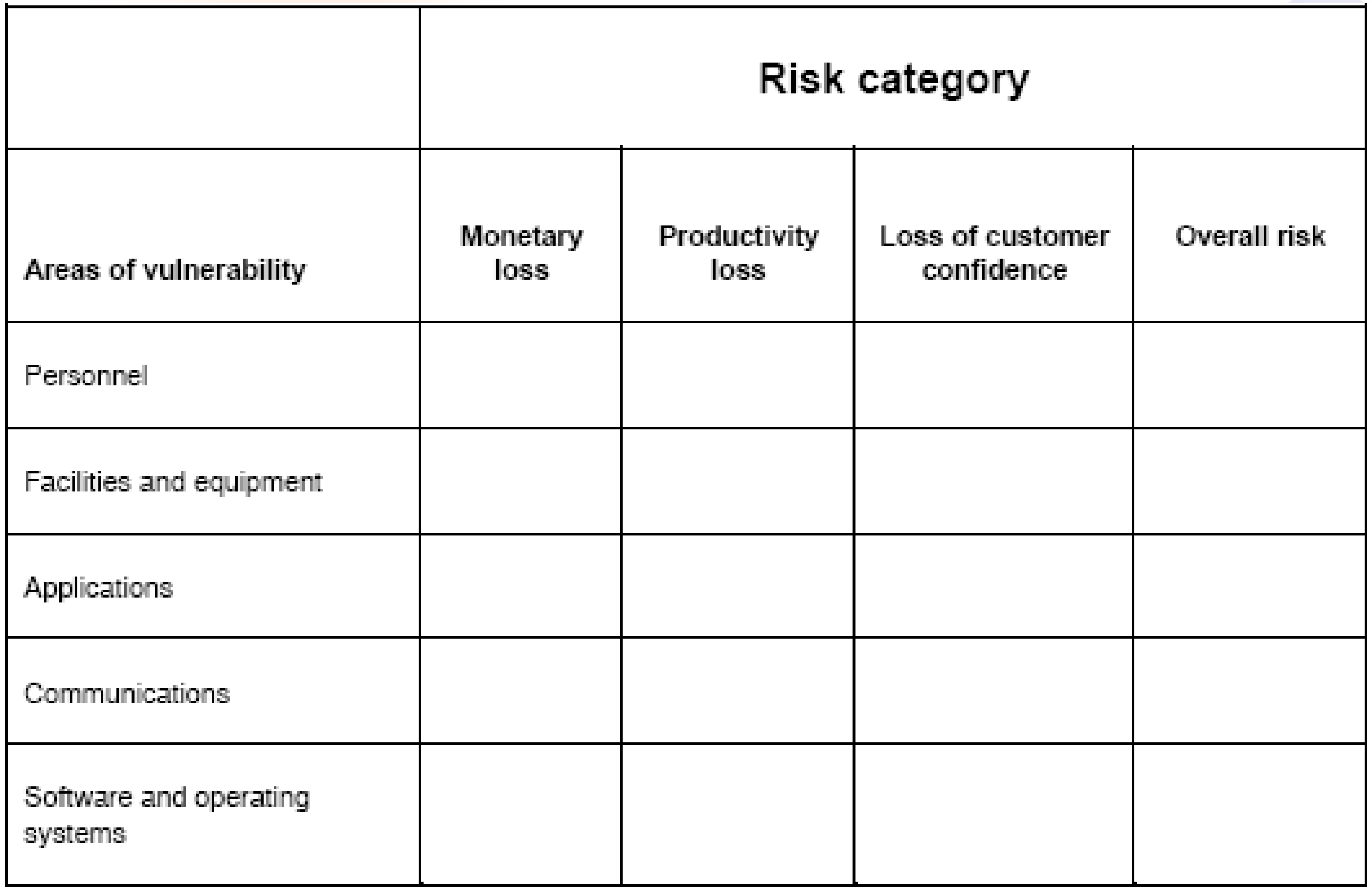
Risk Assessment Matrix



Areas of vulnerability and possible effects of damage	Risk of monetary loss			Risk of productivity loss			Risk of loss of customer confidence		
	H	M	L	H	M	L	H	M	L
Personnel									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Facilities and equipment									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Applications									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Communications									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Software and operating systems									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									

Risk Assessment Table

- After completing the matrix, the team summarizes its findings by assigning a composite risk level to each of the five areas of vulnerability on the matrix.



	Risk category			
Areas of vulnerability	Monetary loss	Productivity loss	Loss of customer confidence	Overall risk
Personnel				
Facilities and equipment				
Applications				
Communications				
Software and operating systems				

Identifying Needed Controls Based on Predetermined Requirements

- After determining the overall risk level for each area of vulnerability, the team identifies the minimum applicable controls that are prescribed in its organizational guidelines.

Reporting and Ensuring That Agreed Actions Are Taken

- After determining the minimum set of controls, the team compares those required controls with controls already in place and identifies any gaps.

- The team prepares a short statement summarizing the outcome and documenting its decisions and decision making process. It then provides the regional office a copy of the risk assessment table.

Case Study

Information Security Plan (“Plan”)
“Arizona State University’s safeguards”

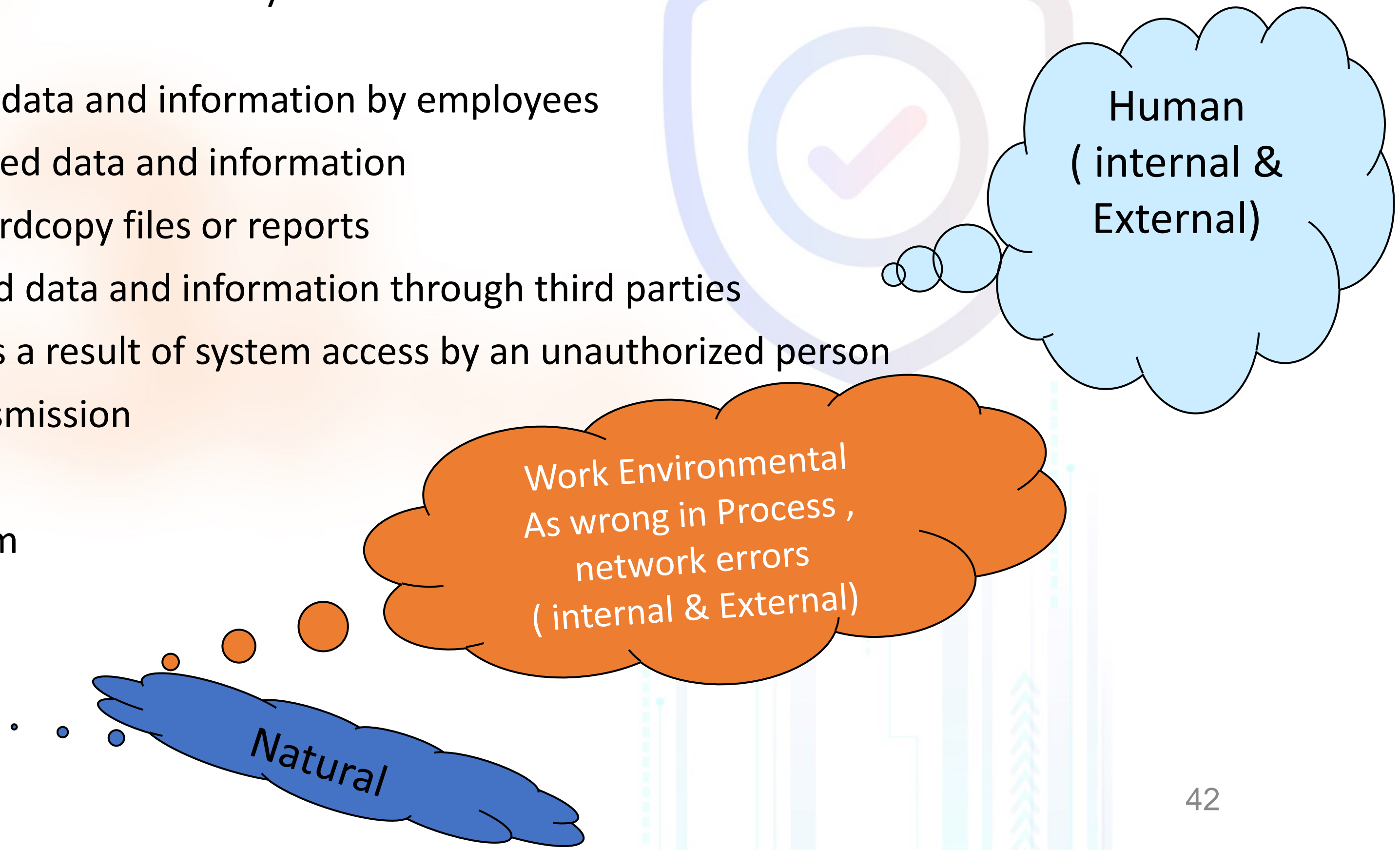
Goals of Security Plan

- ***Main Goal*** :*Protect information and data*

- **Details Goals** :
  - Protect the security and confidentiality of Protected Information;
  - Protect against anticipated threats or hazards to the security or integrity of such information
  - Protect against unauthorized access to or use of Protected Information
  - Provides for mechanisms to: Identify and assess the risks that may threaten Protected Information maintained by Arizona State University;
  - Designate employees responsible for coordinating the program;
  - Design and implement a safeguards program
  - Manage the selection of appropriate service providers
  - Adjust the plan to reflect changes in technology, the sensitivity of Protected Information, and internal or external threats to information security; and reference related policies, standards, and guidelines.

Identification and Assessment of Risks to Customer Information

- Arizona State University recognizes that it has both internal and external risks. These risks include, but are not limited to:
  - Unauthorized access of protected Information by someone other than the owner of the covered data and information
  - Unauthorized access of covered data and information by employees
  - Unauthorized requests for covered data and information
  - Unauthorized access through hardcopy files or reports
  - Unauthorized transfer of covered data and information through third parties
  - Compromised system security as a result of system access by an unauthorized person
  - Interception of data during transmission
  - Loss of data integrity
  - Errors introduced into the system
  - Corruption of data or systems
  - Physical loss of data in a disaster



Human
(internal &
External)

Work Environmental
As wrong in Process ,
network errors
(internal & External)

Natural

Risk Assessment Report at ASU

- Arizona State University recognizes that this may not be a **complete list** of the risks associated with the protection of Protected Information.

- Since technology growth is not static, new risks are created regularly. Accordingly, the University Technology Office and the Office of Student Affairs will actively participate with and seek advice from an advisory committee made up of university representatives for identification of new risks.

- Arizona State University believes current safeguards used by the University Technology Office are reasonable and, in light of current risk assessments are sufficient to provide security and confidentiality to Protected Information maintained by the University.

Who has the responsibility of assessing the risk

- The **University Technology Officer**, in consultation with an advisory committee, is responsible for the maintenance of information security and privacy.

- The advisory committee will include representatives from the departments primarily responsible for safeguarding Protected Information.

- Each department responsible for safeguarding Protected Information will provide an annual update report indicating the status of its safeguarding procedures.

- The Coordinators, in conjunction with the advisory committee, are responsible for assessing the risks associated with unauthorized transfers of Protected Information and implementing procedures to minimize those

Design and Implementation of Safeguards Program

- Minimizing risk and safeguarding covered data and information security can be achieved by *Employee Management and Training*
- *Physical Security can be achieved by* limiting access to only those employees who have a business reason to know such information and requiring signed acknowledgement of the requirement to keep Protected Information private
- Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Arizona State University has policies, standards, and guidelines governing the use of electronic resources and firewall and wireless policies
- The University maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. *Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies …*

Conclusion

Summary

The knowledge of the following are important to do the useful risk assessment

- who was responsible for initiating and conducting risk assessments
- who was to participate
- what steps were to be followed
- how disagreements were to be resolved
- what approvals were needed
- how assessments were to be documented
- how documentation was to be maintained
- to whom reports were to be provided.