Risk Identification
&
Assessment
Chapter_ 2

أ.م.د.عباس عبد العزيز عبد الحميد

كليـة العلـوم / قسم الحاسـوب

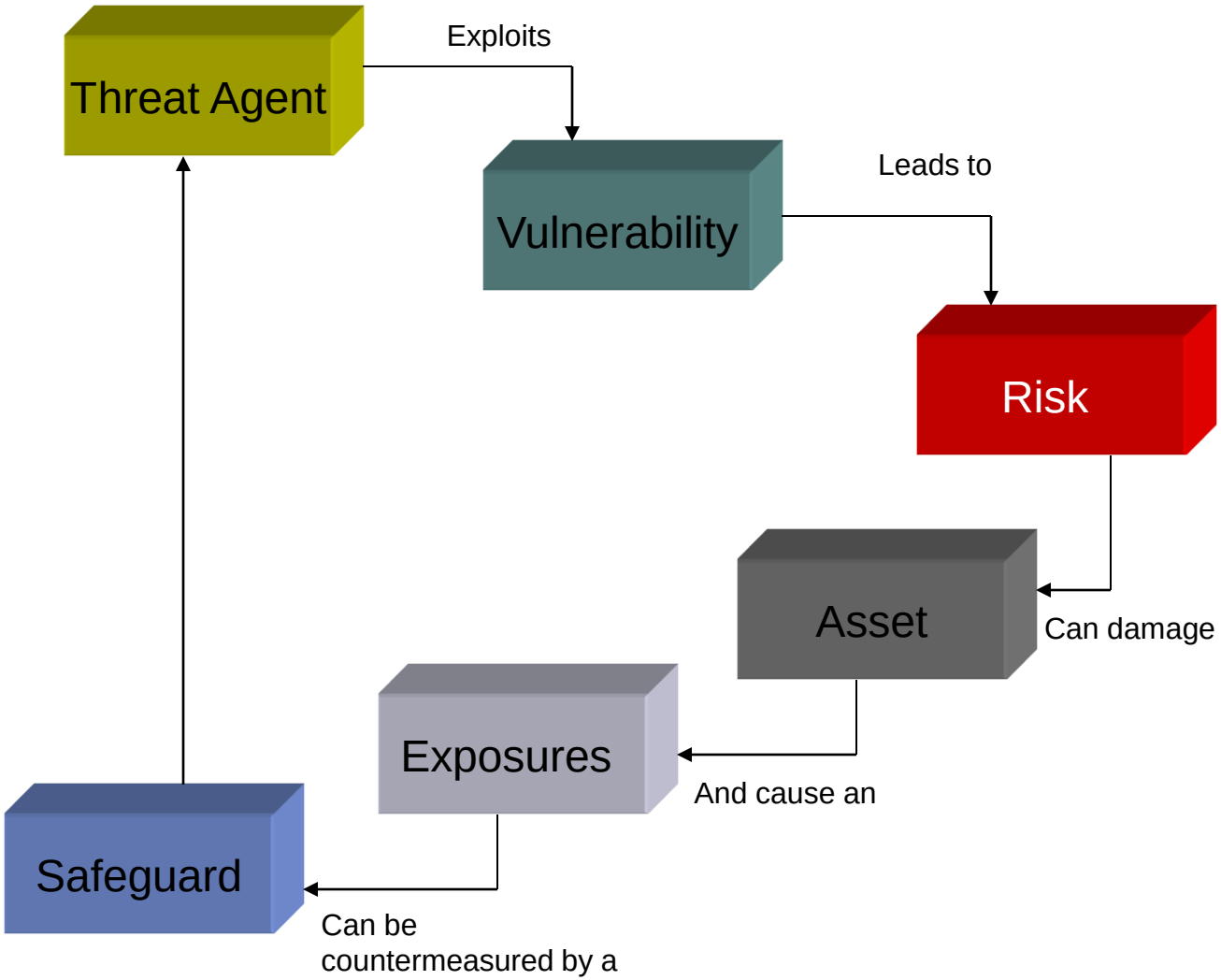
abbasabdulazeez@uomustansiriyah.edu.iq

What is Risk & Risk Management?

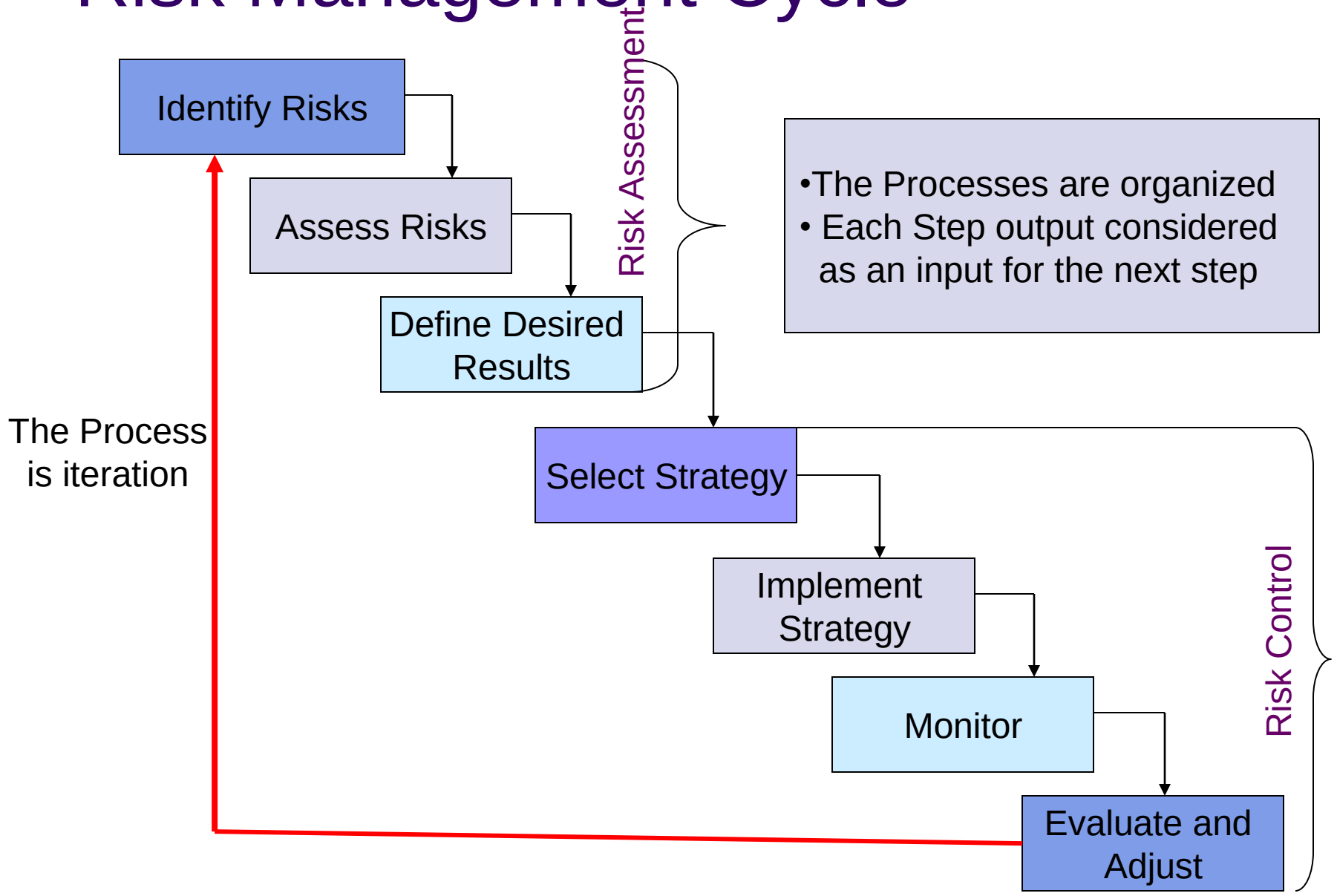
- *Risk : The is an object, person or other entity that represent a danger, harm or loss to an asset*

- *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 using by organization for achieving business objectives, and then 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



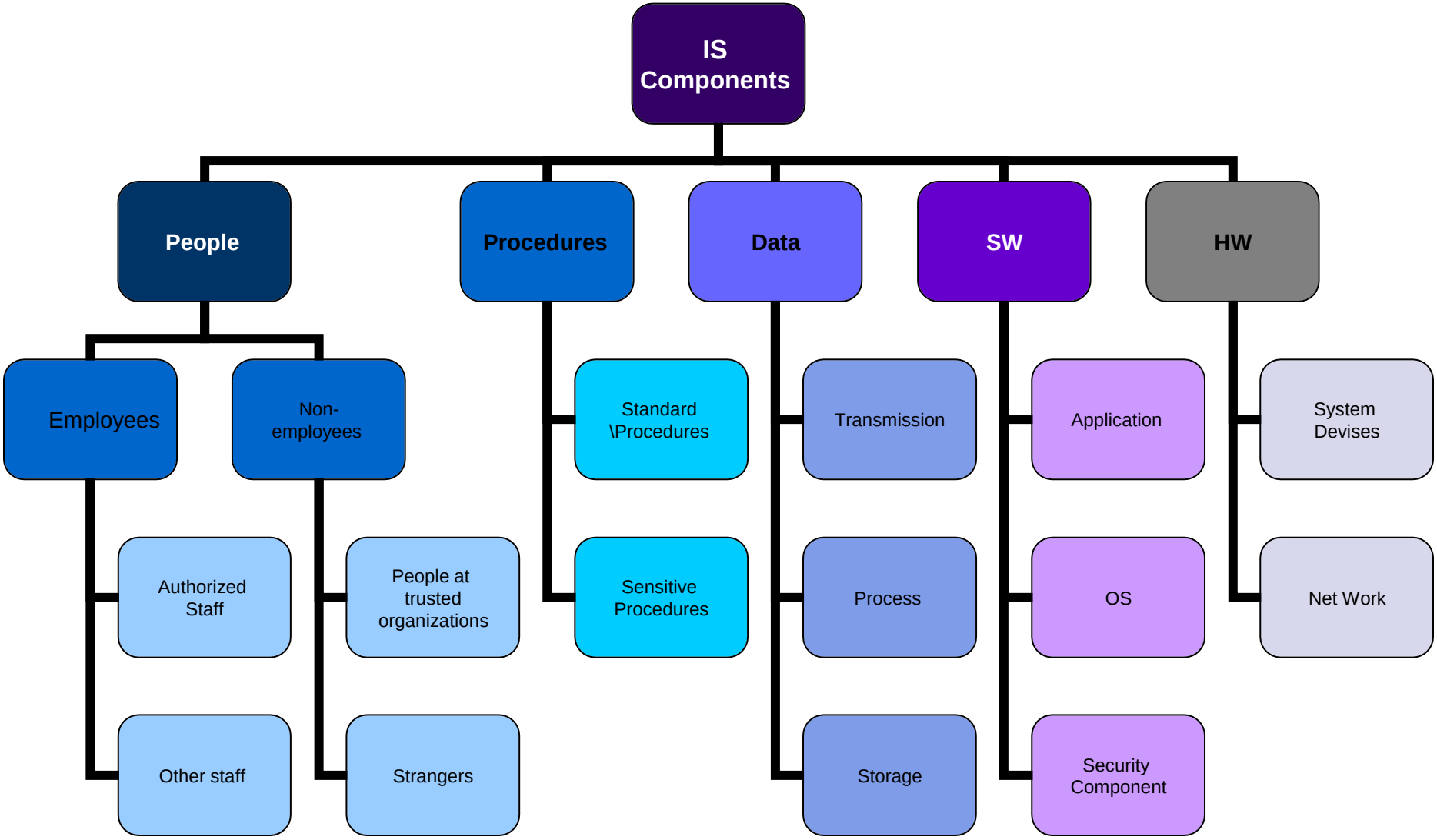
Risk Identification

What is the purpose of this phase ?

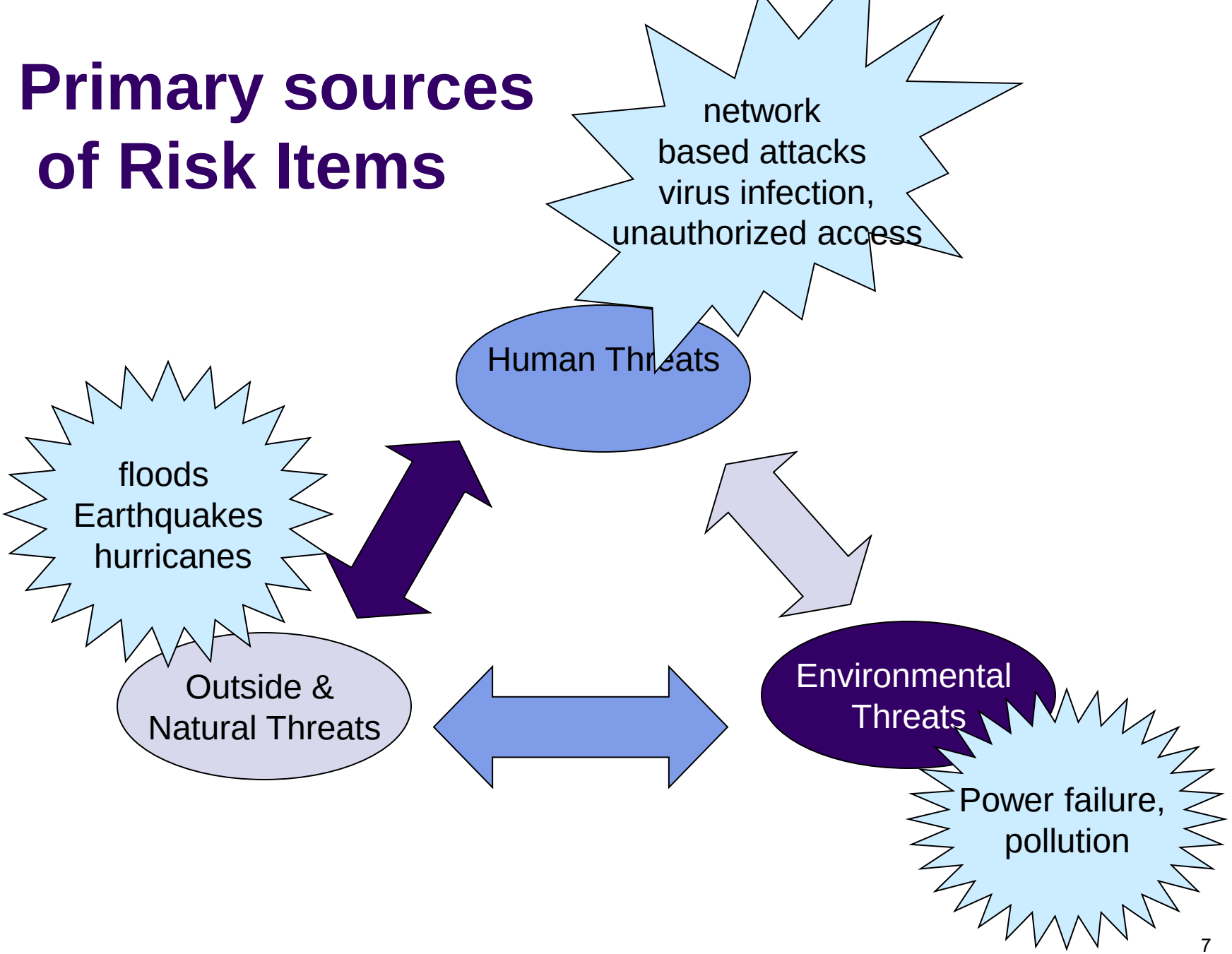
- **The aims of this phase is to identify , classify and prioritizing the organization's information assets (Know ourselves) and identify all important types and sources of risk and uncertainty (know our enemy), associated with each of the investment objectives.**

- **This is a crucial phase.** ***If a risk is not identified it cannot be evaluated and managed***

Information Assets



Primary sources of Risk Items



Risk Assessment

- For each identified component & risk, which has a 'clearly significant' or 'possibly significant' position, each should be *assess* to *establish qualitatively and Estimate the value*

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.

,

Second : Qualitative Risk Assessment

This approach can be taken by defining

- **Risk in more subjective and general terms such as high, medium, and low.**
- **In this regard, 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

- 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.

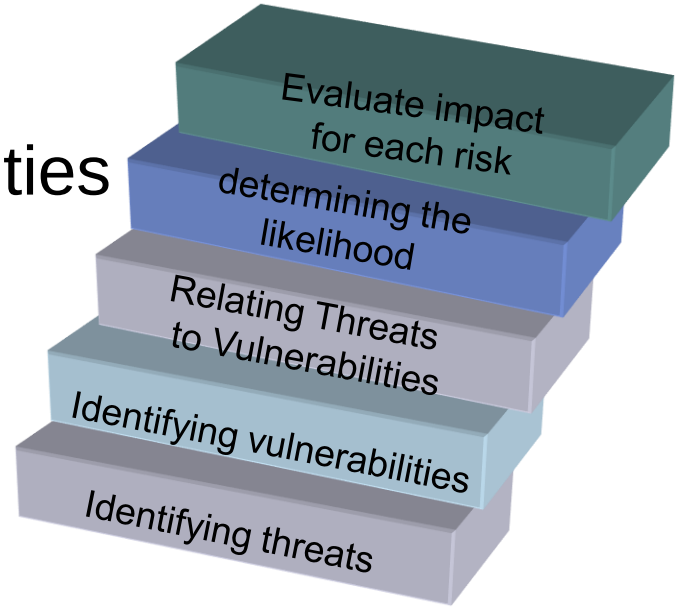
- Two of the reasons claimed for this are
  - 1) the difficulties in identifying and assigning a value of all components
  - 2) Moral Effects couldn't measured by quantitative measurements
  - 2) the lack of statistical information that would make it possible to determine frequency.

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

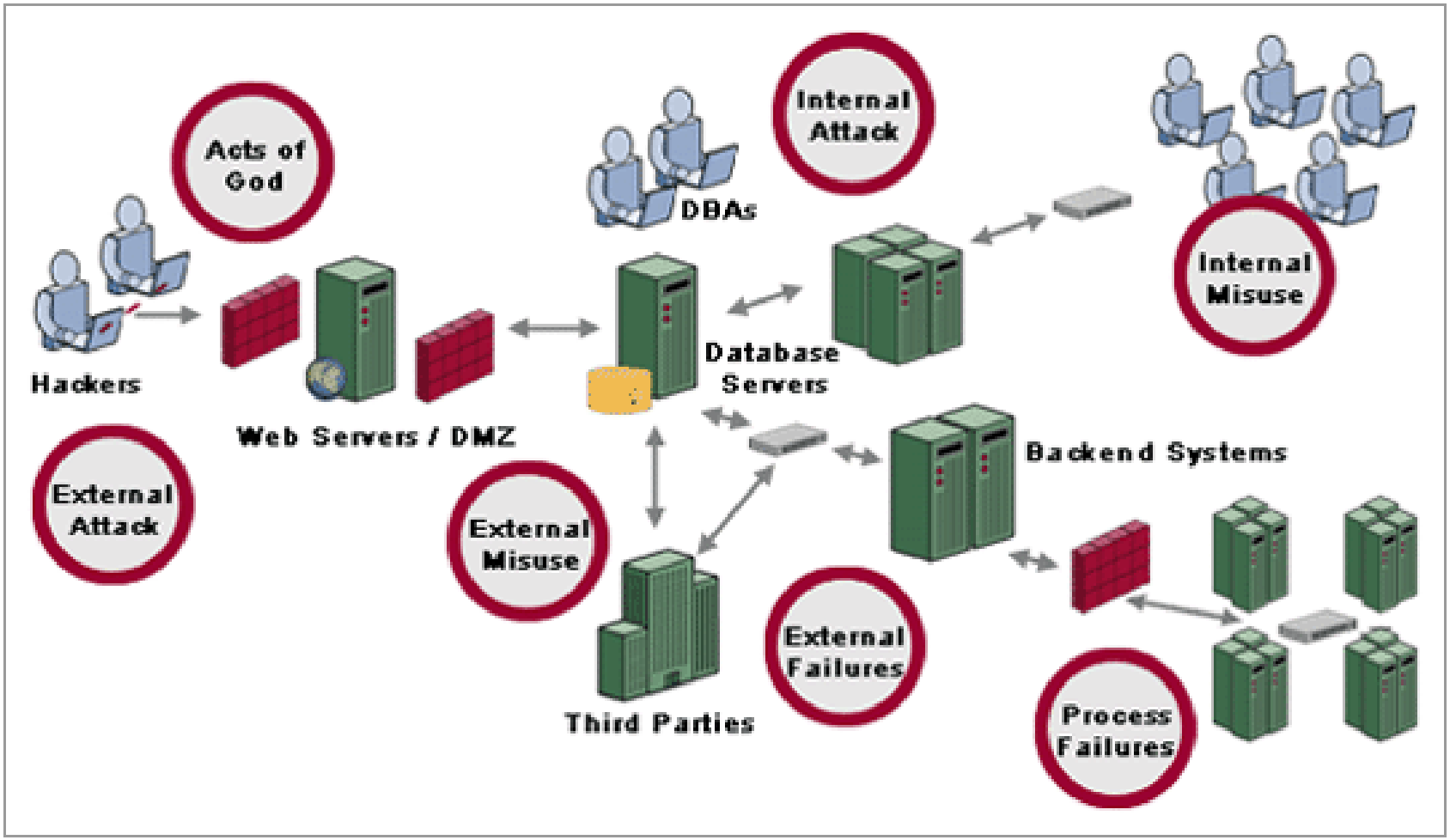
How to assess the risks

Risk is assessed by following the following steps :

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



Identifying Risk



Identifying Vulnerabilities

- **Identifying Vulnerabilities**：how each of the threats that are possible or likely could be perpetrated , 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.
  - Then, 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.

- 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

- **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
- ***The First one will be explained***

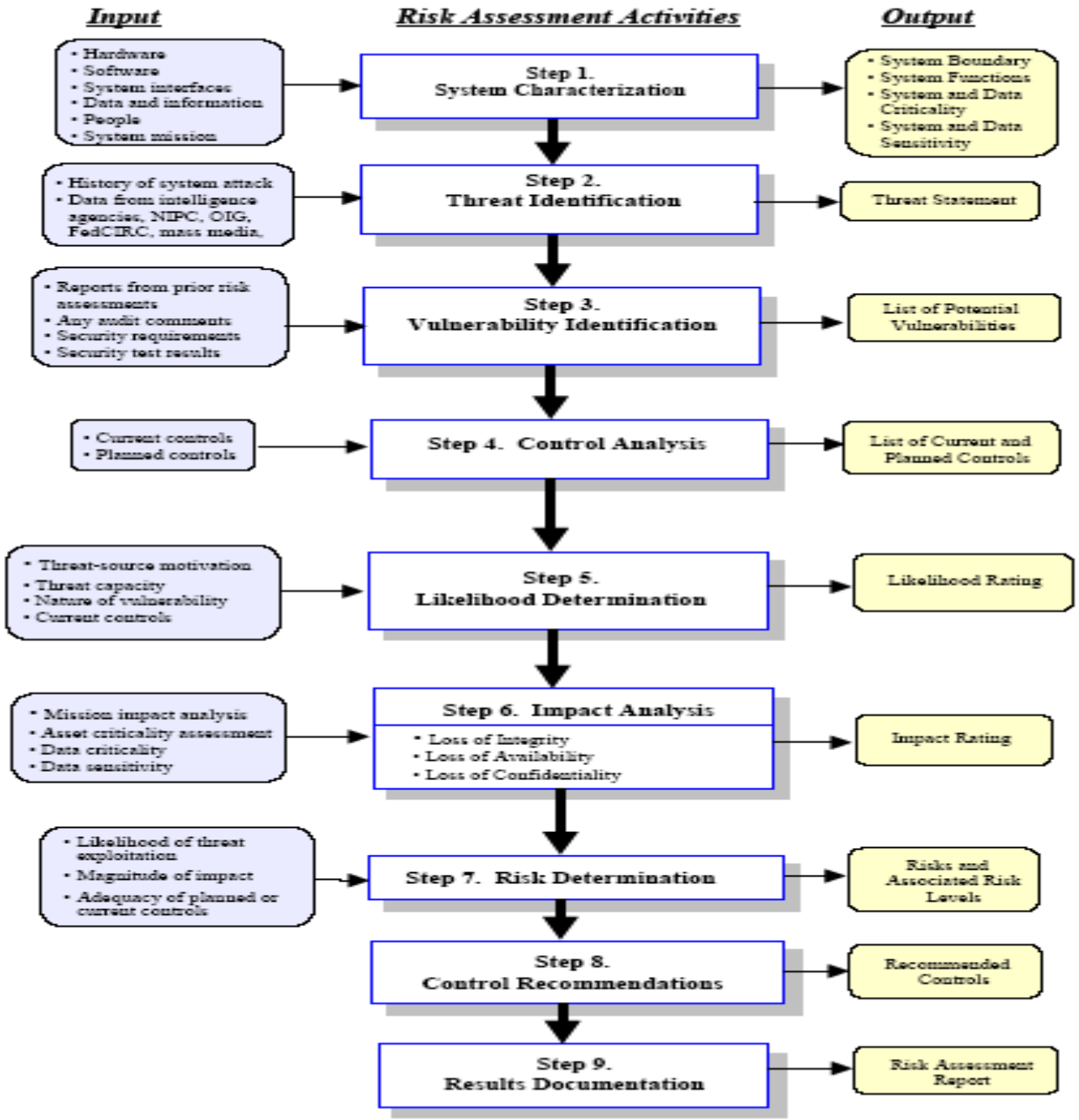
National Institute of Standards & Technology

- **(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.

The NIST methodology consists :

- 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 do 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 insure sufficient resources are allocated
  - Information Technology – must assist in building secure systems and operating them safely

Summary of Risk Assessment Practices and Related Benefits