# University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

**PSIT302 & PSIT3P2 – Information Security Management (ISM)**

---

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

# Outline of the Syllabus

- Unit I : Security Risk Assessment and Management
- Unit II : Security Management of IT Systems
- Unit III : Key Management in Organizations
- Unit IV : Auditing and Business Continuity Planning
- Unit V : Computer Forensics

# Unit I : Risk Assessment and Management

- What are Risk and Risk Assessment?
- Risk Management Process
- Components of Risk Management
- Risk Based Decisions and Activities
- Relationship among Risk Framing Components
- Risk Models
- Threat and Threat Shifting
- Vulnerabilities and Predisposing Conditions
- Likelihood
- Impact
- Generic Risk Model with Risk Factors
- Aggregation
- Uncertainty
- Risk Assessment Process

# What are Risk and Risk Assessment?

- *Risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event

---

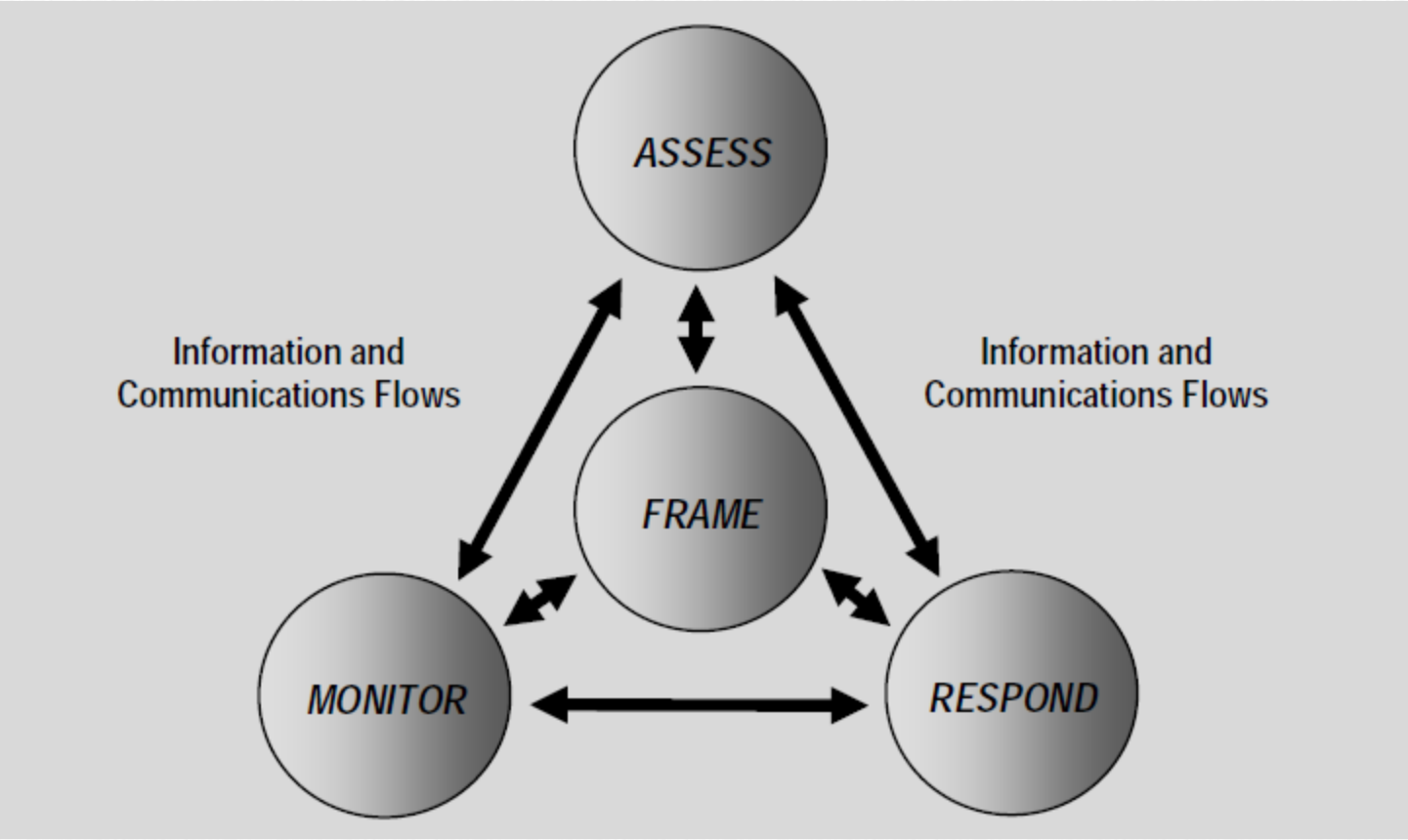
- It is a function of:
  - the adverse impacts that would arise if the circurustance or event occurs
  - the likelihood of occurrence
- Information Security Risk – Arises from the loss of confidentiality, integrity, availability
- Risk Assessment - the process of identifying, estimating, and prioritizing information security risks

# Risk Management Process

- Risk Assessment is a key component of a holistic organizational risk management process

- Risk Management process consists of
  - Framing risks
  - Assessing risks
  - Responding to risk
  - Monitoring risk

# Risk Assessment within Risk Management Process



# First Component - Frame

- How a risk is established
- Describing the environment in which risk based decisions are made
- Purpose is to produce risk management strategy
  - Addresses how risk assessed, responds and monitored

# Second Component –Assess

- How risk assessed within the frame
- Purpose
  - To identify threats
  - Vulnerabilities
  - The harm
  - Likelihood of the harm

# Third Component –Respond

- Response to the risk determined through the risk assessment
- Provides consistent, organizational wide respond to risk in accordance with the frame
  - Developing alternative courses of action
  - Evaluating the alternative courses of action
  - Determining the appropriate courses of action consistent with organizational risk tolerance
  - Implementing risk responses based on selected courses of action

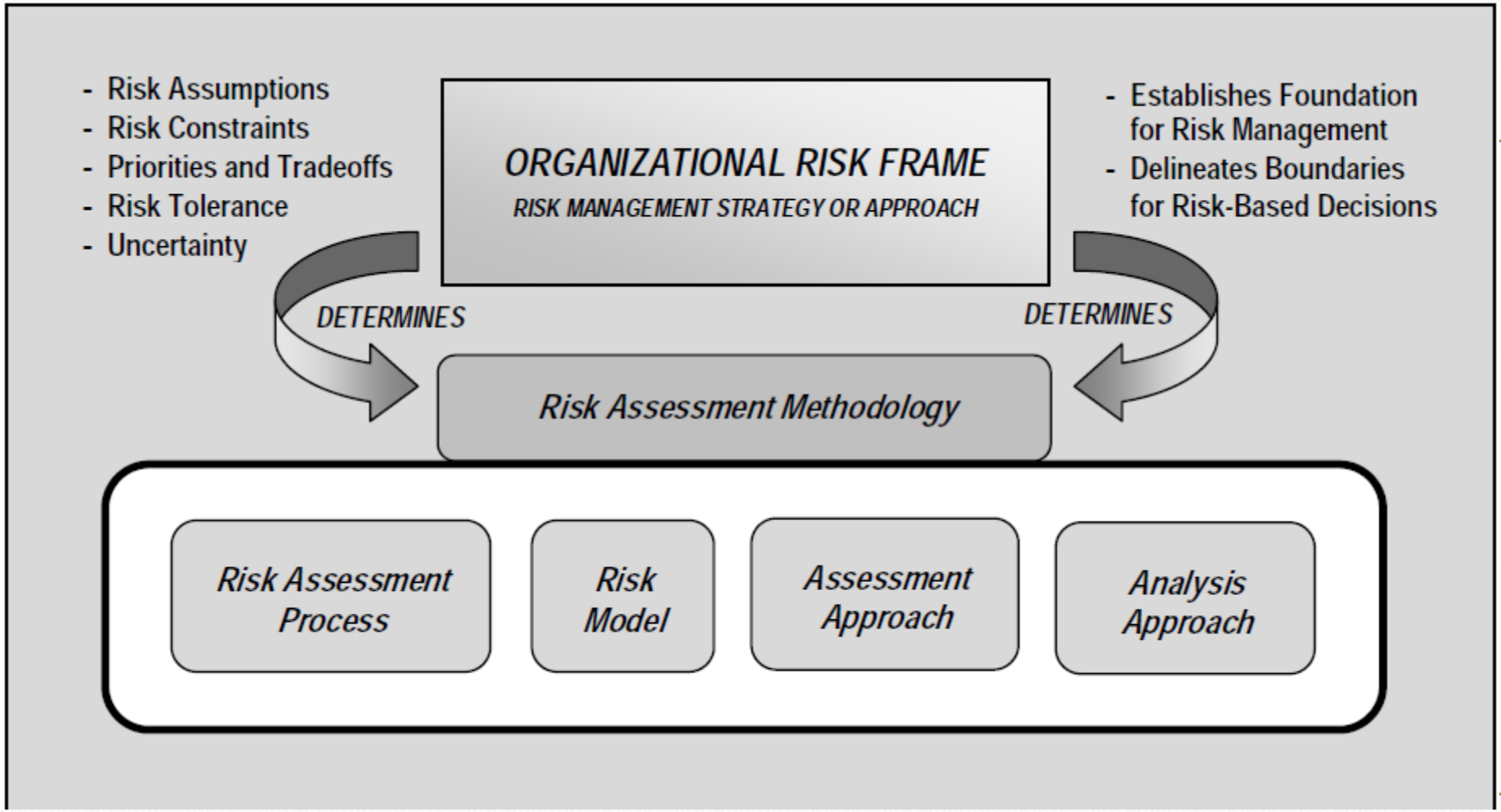
# Fourth Component – Monitor

- How risk assessment and response are monitored
- Purpose is to
  - Determine the ongoing effectiveness of risk responses
  - Identify the risk impacting changes to organizational information systems and the environments in which the systems operate
  - Verify that planned risk responses are implemented
  - Information security requirements derived from and traceable to organizational business functions, federal legislations, directives, regulations, policies, standards and guidelines are satisfied

# Risk based Decisions and Activities

- Development of an information security architecture;
- Definition of interconnection requirements for information systems (including systems supporting mission/business processes and common infrastructure/support services);
- Design of security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers/supply chain, and contractors;
- Authorization (or denial of authorization) to operate information systems or to use security controls inherited by those systems (i.e., common controls);
- Modification of missions/business functions and/or mission/business processes permanently, or for a specific time frame (e.g., until a newly discovered threat or vulnerability is addressed, until a compensating control is replaced);
- Implementation of security solutions (e.g., whether specific information technology products or configurations for those products meet established requirements); and
- Operation and maintenance of security solutions (e.g., continuous monitoring strategies and programs, ongoing authorizations).

# Relationship among risk framing networks



# Risk Models and Risk Factors

- Risk Models define the risk factors to be assessed and their relationship
- Risk Factors are inputs of risk models in determining the levels of risk and the assessment
  - Threat, vulnerability, impact, likelihood, predisposing condition
  - Can be decomposed further as threat sources and threat events

# Threats

- A *threat* is any circumstance or event with the potential to adversely irnpact organizational operations and assets, individuals, other organizations, or the Nation through an information system1via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
- A *threat source* is characterized as:
  - the intent and method targeted at the exploitation of a vulnerability ;
  - a situation and method that play accidentally exploit a vulnerability.
- In general, types of threat sources include:
  - hostile cyber or physical attacks
  - human errors of omission or commission
  - Structural failures of organization-controlled resources (e.g., hardware, software, environmental controls)
  - Natural and man-made disasters, accidents, and failures beyond the control of the organization.

# Threat Shifting

- Response of adversaries to perceived safeguards and/or counter measures (i.e., security controls), in which adversaries change some characteristic of their intent/targeting in order to avoid and/or overcome those safeguards/ counter measures
- Threat shifting can occur in one or more domains including
  - the time domain (e.g., a delay in an attack or illegal entity to conduct additional surveillance)
  - the target domain (e.g., selecting a different target that is not as well protected)
  - the resource domain (e.g., adding resources to the attack in order to reduce uncertainty or overcome safeguards and/or counter measures)
  - the attack planning/attack method domain (e.g., changing the attack weapon or attack path).

# Vulnerabilities and Predisposing Conditions

- Is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

---

- Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness.
- However, it is also important to allow for the possibility of emergent vulnerabilities that can arise naturally over time as organizational missions/business functions evolve, environments of operation change

# Likelihood

- The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).

- The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).
- For adversarial threats, an assessment of likelihood of occurrence is typically based on:
  - adversary *intent;*
  - adversary *capability*
  - adversary *targeting*.

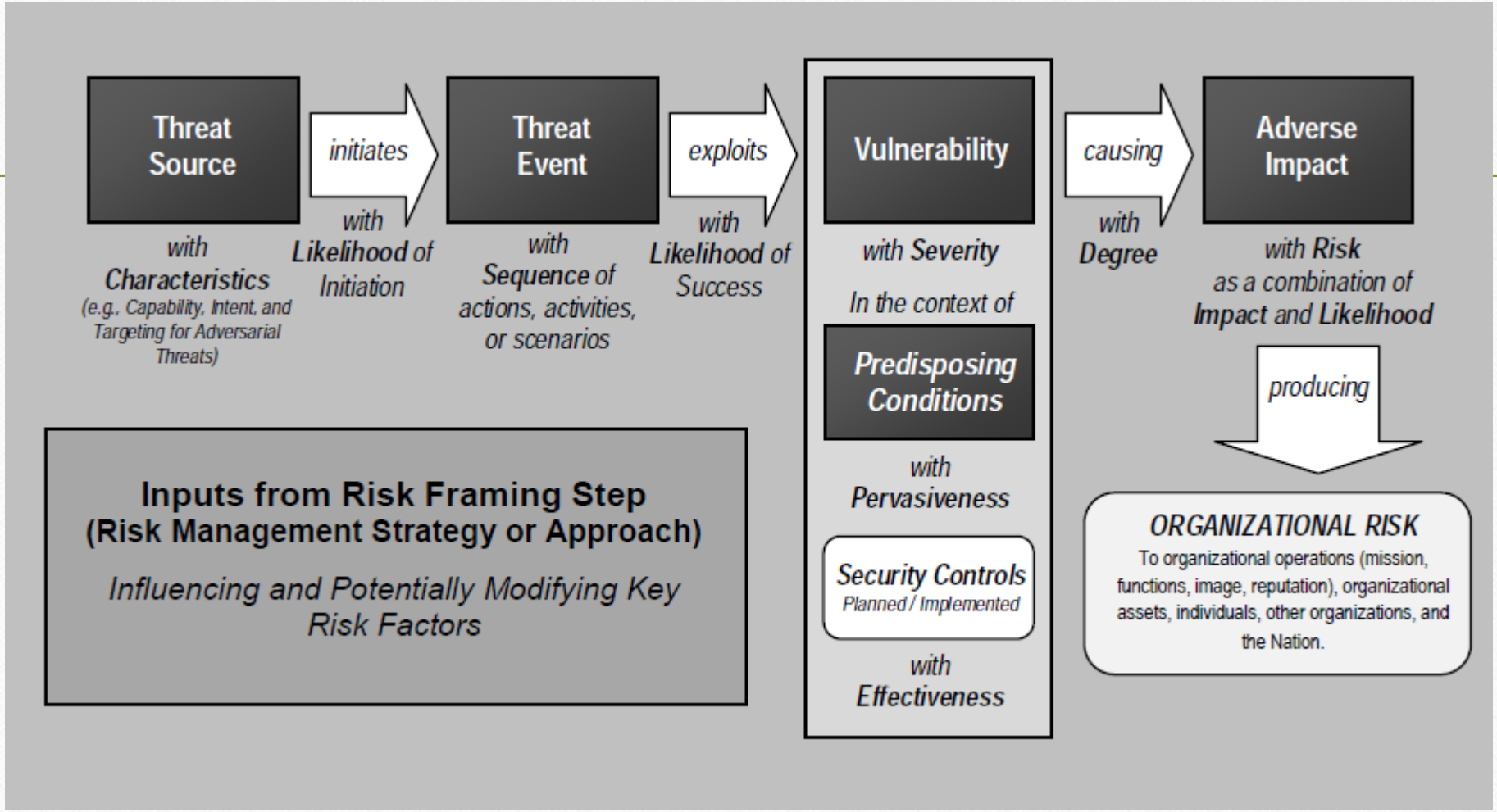
# Impact

- The level of *impact* from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

---

- Such harm can be experienced by a variety of organizational and non organizational stakeholders
- For example, heads of agencies, mission and business owners, information owners/stewards, mission/business process, individuals/groups in the public or private sectors relying on the organization-in essence, anyone with a vested interest in the organization's operations, assets, or individuals, including other organizations in partnership with the organization, or the nation.
- Organizations take explicit: (i) the process used to conduct impact determinations; (ii) assumptions related to impact determinations; (iii) sources and methods for obtaining impact information; and (iv) the rationale for conclusions reached

# Generic Risk Model with key Risk Factors

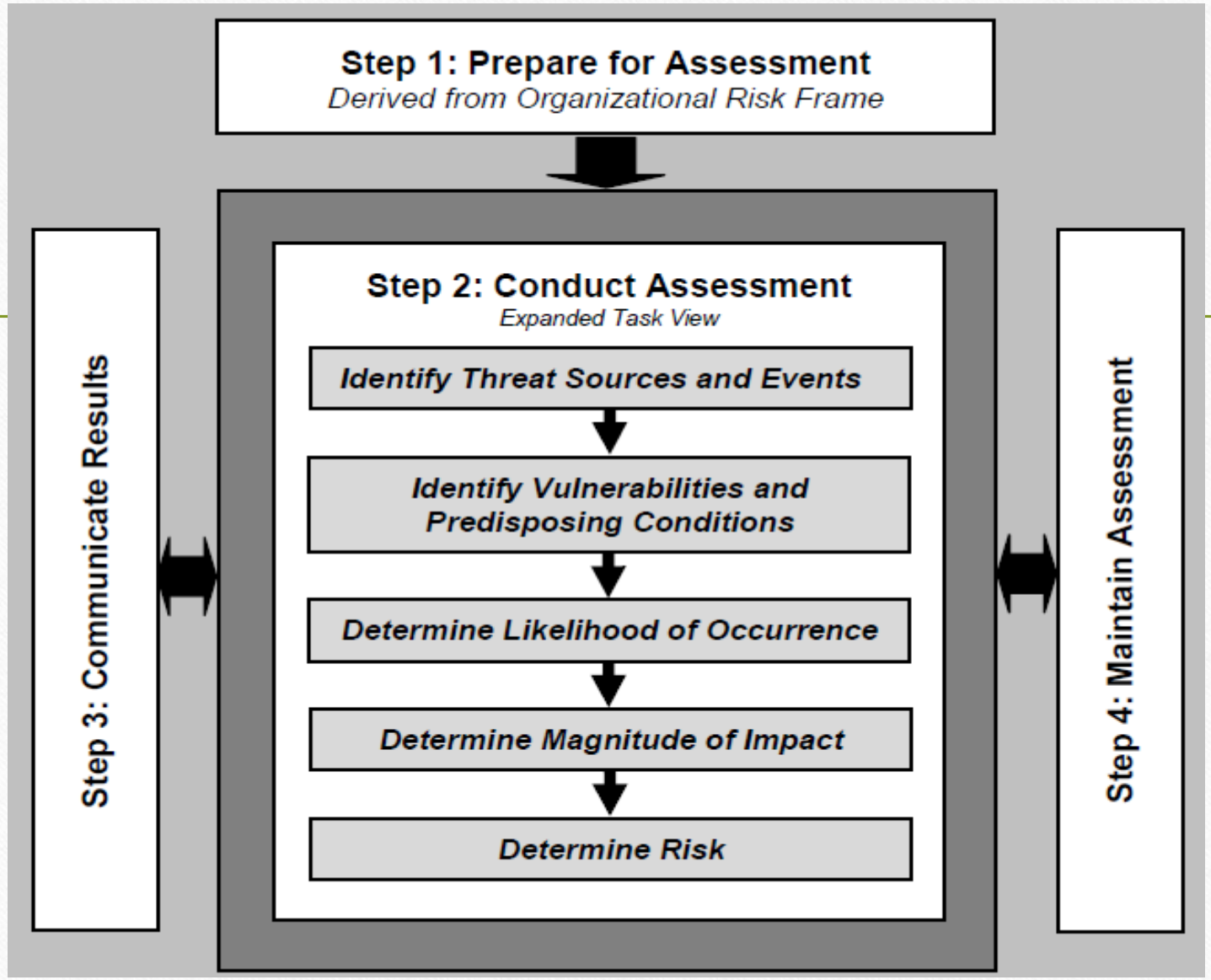


# Aggregation

- Use risk *aggregation* to roll up several discrete or lower-level risks into a more general or higher-level risk.
- Organizations may also use risk aggregation to efficiently manage the scope and scale of risk assessments involving multiple information systems and multiple mission/business processes with specified relationships and dependencies among those systems and processes.
- Risk aggregation , conducted primarily at Tiers 1 and 2 and occasionally at Tier 3, assesses the overall risk to organizational operations, assets, and individuals given the set of discrete risks.
- One issue for risk aggregation is that this upper bound for risk may fail to apply.
  - For exa1nple, it may be advantageous for organizations to assess risk at the organization level when multiple risks materialize concurrently or when the same risk materializes repeatedly over a period of time.
  - In such situations, there is the possibility that the amount of overall risk incurred is beyond the risk capacity of the organization, and therefore the overall impact to organizational operations and assets (i.e., mission/business in1pact) goes beyond that which was originally assessed for each specific risk.

# Uncertainty

- *Uncertainty* is inherent in the evaluation of risk, due to such considerations as:
  - limitations on the extent to which the future will resemble the past
  - imperfect or incomplete knowledge of the threat (e.g., characteristics of adversaries including tactics, techniques , and procedures)
  - undiscovered vulnerabilities in technologies or products
  - unrecognized dependencies
- Uncertainty about the value of specific risk factors can also be due to the step in the RMF or phase in the system development life cycle at which a risk assessment is perforn1ed.
  - For example, at early phases in the system development life cycle, the presence and effectiveness of security controls may be unknown, while at later phases in the life cycle, the cost of evaluating control effectiveness may outweigh the benefits in terms of n1ore fully inforn1ed decision making.
  - Finally, uncertainty can be due to incomplete knowledge of the risks associated with other information systems, mission/ business processes , services, common infrastructures, and/or organizations.
  - The degree of uncertainty in risk assessn1ent results, due to these different reasons, can be communicated in the form of the results (e.g., by expressing results qualitatively, by providing ranges of values rather than single values for identified risks, or by using a visual representations of fuzzy regions rather than points).


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment