Insurance Information Institute

Observations on OMB's Proposed Risk Assessment Bulletin

Reflections on Terrorism Risk and Homeland Security

Dr L James Valverde, Jr
Director, Economics and Risk Management
Insurance Information Institute
110 William Street
New York, NY 10038
Tel: (212) 346-5522
Fax: (212) 732-1916
jamesv@iii.org www.iii.org

24 May 2006

Introduction

- Motivation
  - The need for RA guidance
- Similar set of challenges faced at GAO
- Main criticism of the draft bulletin:
  - RA – at the exclusion of everything else
  - Myopic focus on EHS
    - Homeland Security context as a key omission
  - Need to work towards a generic and modularizable framework

Outline of Remarks

GAO Risk Management Framework

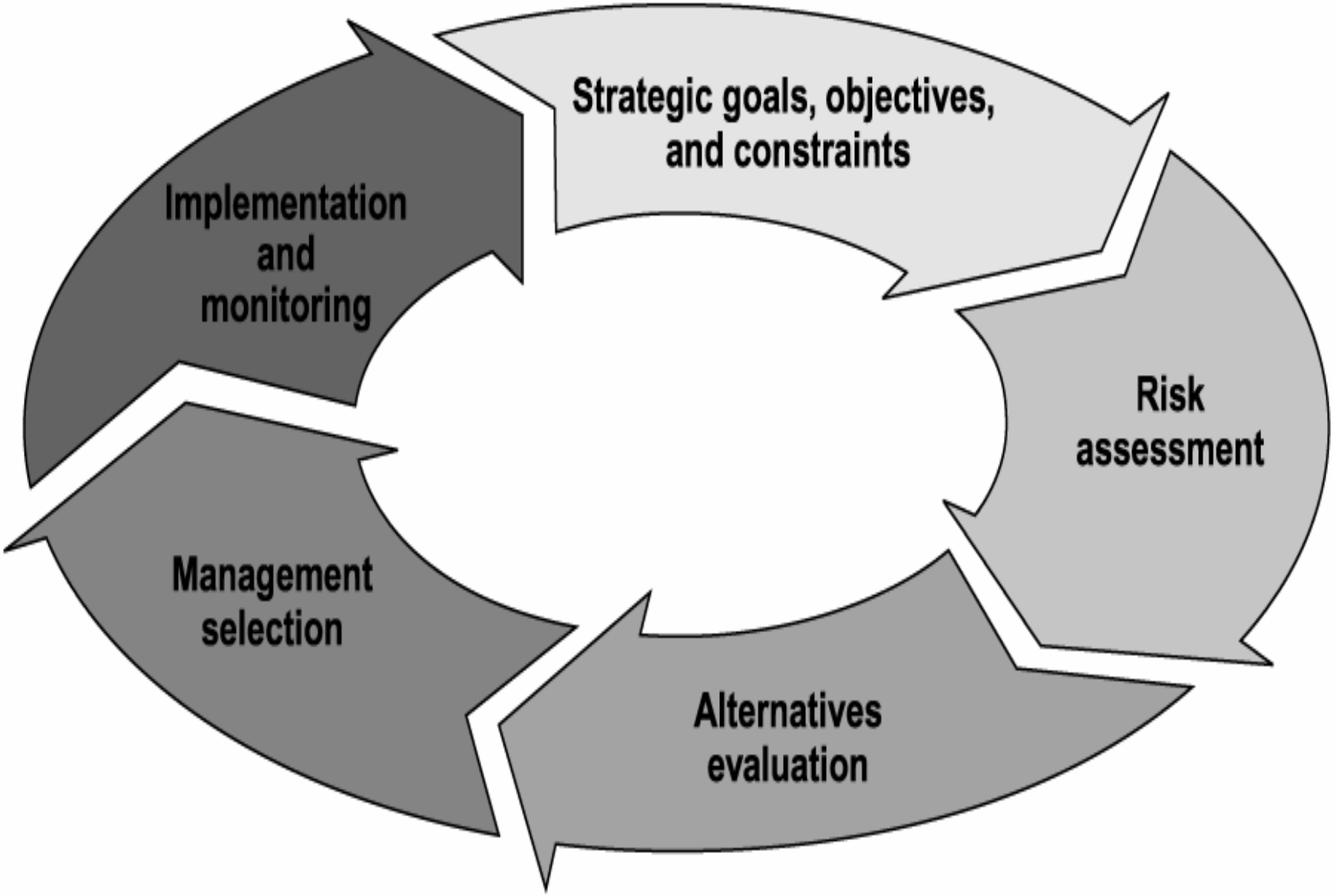
- Individual components
- Integration of components
- A Closer Look at the Risk Assessment Component in Homeland Security contexts

The Emerging T-V-C Paradigm in Homeland Security

- Emerging best-practices

Concluding Remarks and Observations

Top Level: The GAO Risk Management Cycle



Source: GAO.

GAO Risk Management Framework: *Strategic Goals, Objectives, and Constraints*

- Management decisions are made in context of *strategic goals* and the *objectives* that flow from those goals
- Objectives that are linked to goals should be clear, concise, and *measurable*
- Constraints may be imposed by statute, departmental policy, budget, or other factors that may vary with the scale of the application

GAO Risk Management Framework: *Risk Assessment*

- Helps decision-makers identify and evaluate potential risks to an entity's mission so that countermeasures can be designed and implemented to prevent or mitigate the effects of those risks
- Risk is typically defined as the *probability* and *consequence* of an adverse event
- Most sources model risk in the security area only if the following are present:
  - A specific *threat*
  - A *vulnerability* in the asset or system, and
  - An *adverse outcome* associated with consequence.

GAO Risk Management Framework: *Alternatives evaluation*

- Risks can be reduced by *preventing* or *mitigating* their impact
- Countermeasures should be evaluated to determine the extent to which threats can be reduced
- Countermeasures are measured in terms of monetary costs, although other costs may be included
- Benefits are usually measured in terms of the risk reduction they provide, or the decrease in vulnerability

GAO Risk Management Framework: *Management Selection*

- The goal is to select the countermeasure option(s) that reduce risk to an acceptable level, at the lowest cost.

- Evaluation and application of counter-measures will depend on:

  - Preference and judgments of decision makers

  - Risk tolerance of decision-makers – level of comfort with various levels of risk

  - Fiscal and other constraints

GAO Risk Management Framework: *Implementation and Monitoring*

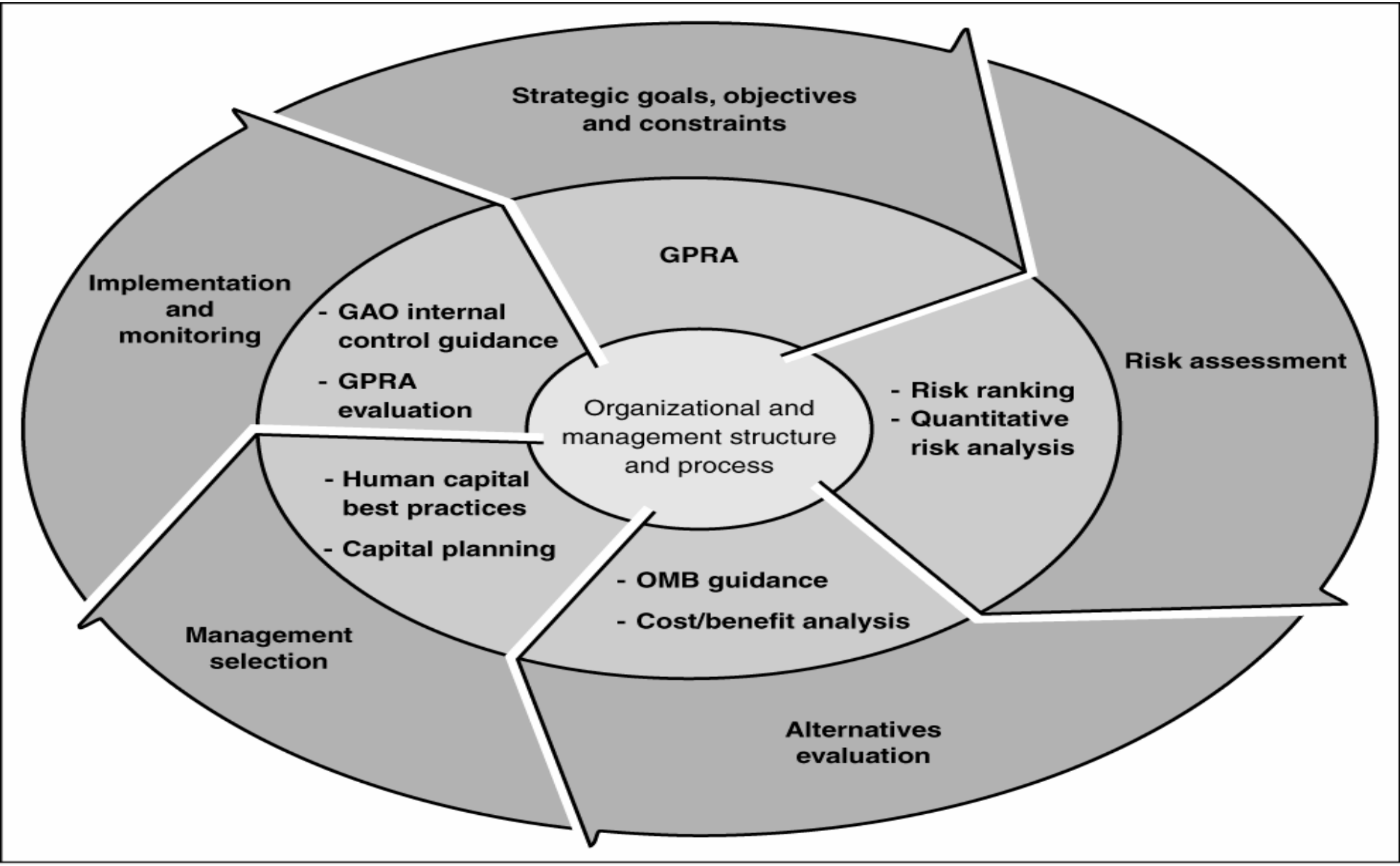
- Criteria for evaluating implementation are frequently contained in planning documents and federal guidance

- GAO's work focuses on internal controls and performance measurement

  - GAO's recommends that internal controls should generally be designed to ensure continual monitoring

  - GAO supports program evaluation for assessing *efficiency* and *effectiveness*.

Cross-cutting Criteria Sources

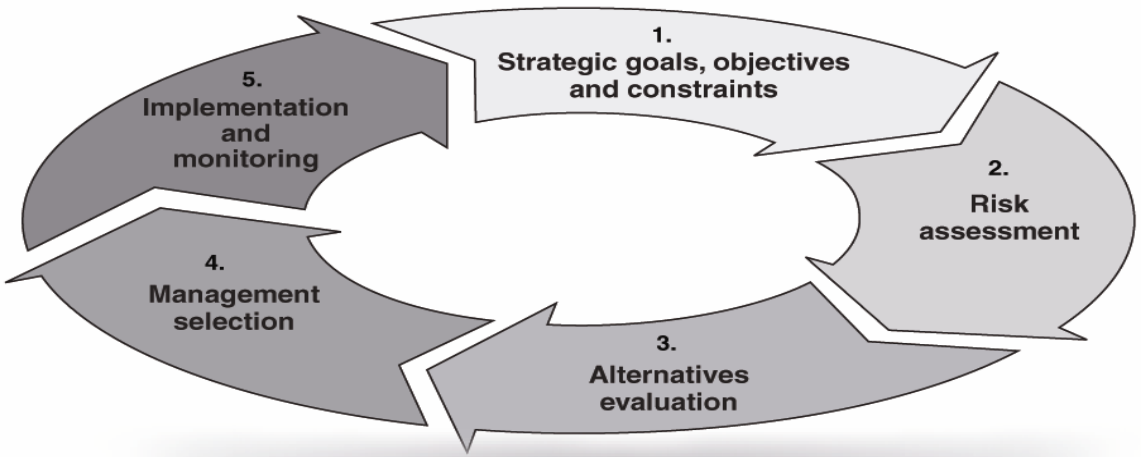


Source: GAO.

Adaptability of the Framework:

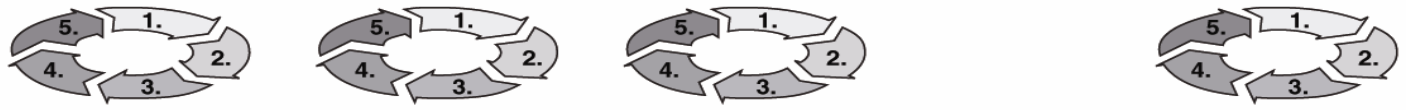
- Tiering effect, with various possible levels of aggregation
  - Framework may be applied at the department level, agency level, program level, down to the project level
  - Facilitates analysis and comparison of information
  - Common set of outcomes that measure risk and risk reduction will increase confidence in results

GAO Risk Management Framework: Macro-to-Micro and Micro-to-Macro Linkages



Sector-specific agencies have the same risk management process, but each agency approach is independent

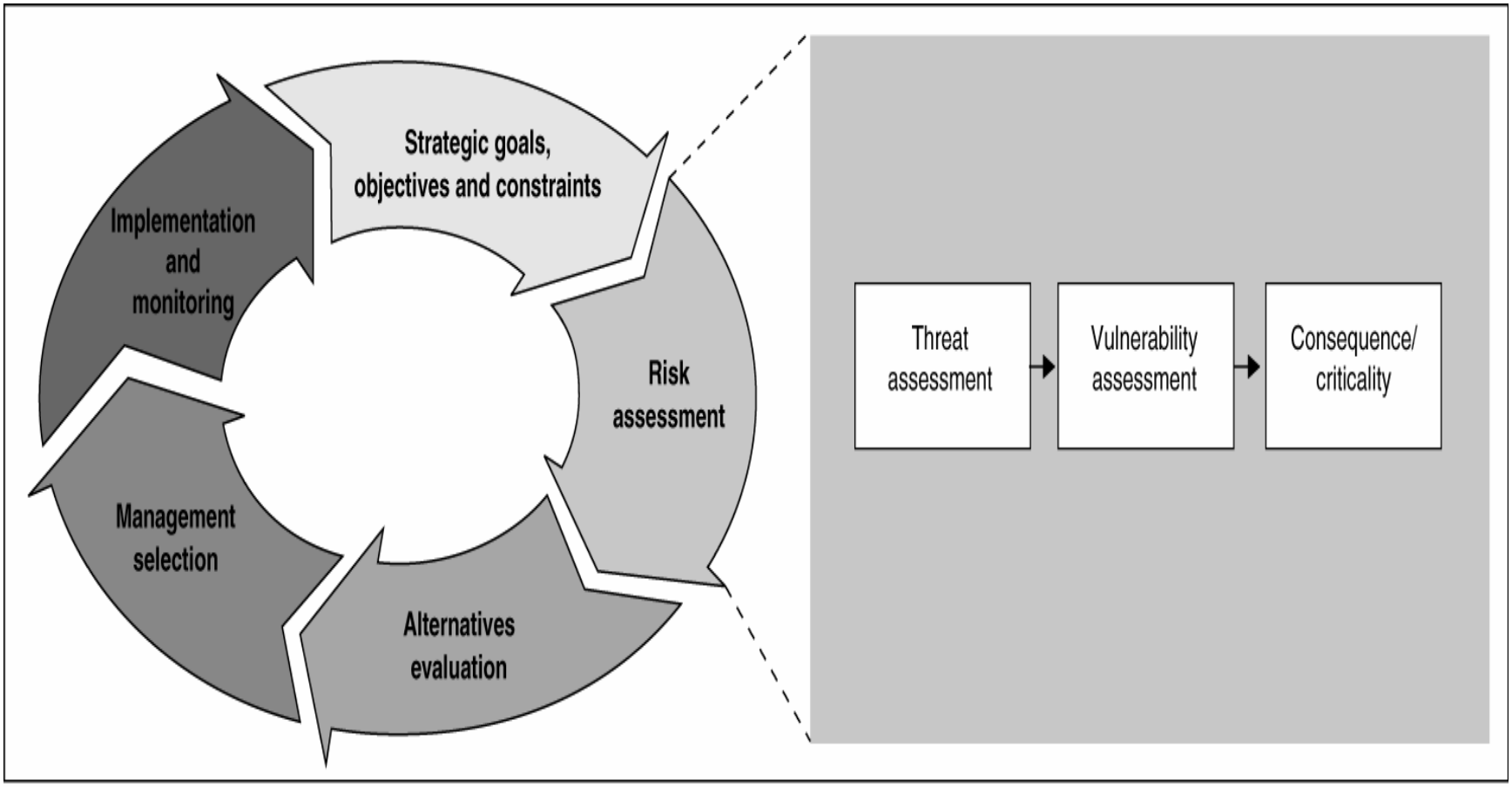
Sector-specific agencies



Risk management process is adopted for each sector-specific agency

Source: GAO.

Risk Assessment: Applications to Homeland Security



Source: GAO.

Risk Assessment and Homeland Security

- In the late 1990s, GAO stated that risk assessments are valuable decision aides in helping combat the threat of transnational terrorism

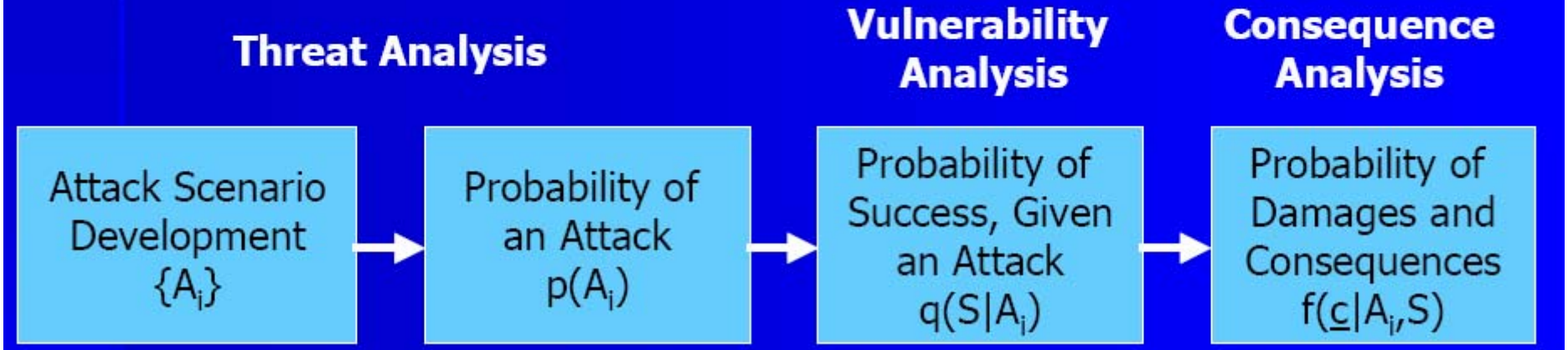
- Following the events of 9-11, GAO's work focused on RM construed as Threat, Vulnerability, and Criticality:

  - *Threat Assessment* – An attempt to identify relevant threats, and to characterize their potential risk

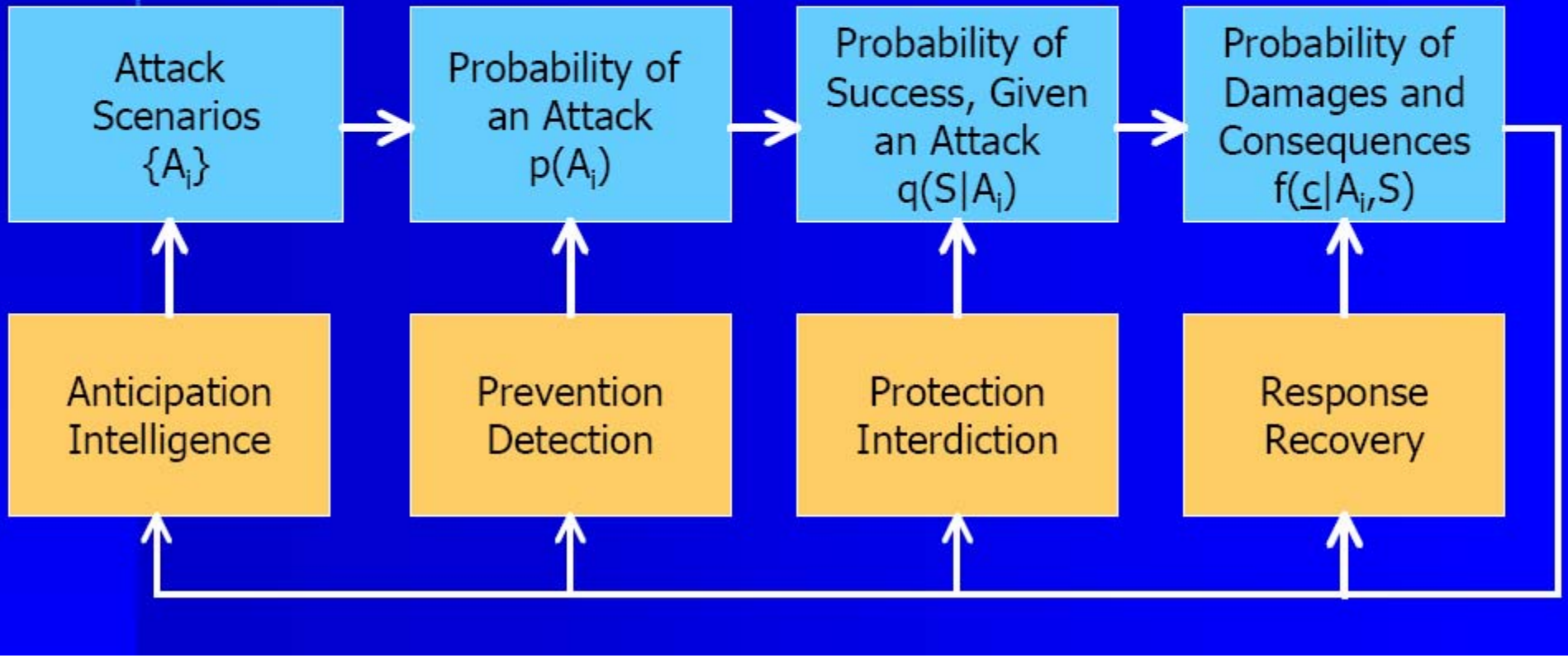
  - *Vulnerability Assessment* – Involves the identification of weaknesses and vulnerabilities in a system

  - *Criticality Assessment* – An attempt to systematically identify and evaluate an organization's assets by the importance of its mission or function, individuals at risk, or the significance of a structure

Terrorism Risk Analysis



Risk Analysis with Interventions



Risk Assessment Models Based on Threat, Vulnerability, and Consequence

- T-V-C is a frequently used decomposition of risk in the security literature
- Agencies working in homeland security have developed a variety of TVC-based models:
  - CARVER-SHOCK
  - N-RAT and PS-RAT
  - TRAVEL
  - TSARM
  - RAMCAP

Multi-Criteria Analysis and the Emerging TVC Paradigm

- Increasing use of MCA-type methods in homeland security settings, largely because costs and benefits are not always easily monetized
- MCA is both an approach and a set of techniques:
  - A way of looking at complex problems that are characterized by a mixture of *monetary* and *non-monetary* objectives
  - A set of analytical techniques for breaking the problem into manageable pieces, allowing data and judgments to be brought to bear on the pieces
  - Reassembling the pieces to present a coherent overall picture to decision-makers
- Vulnerabilities and consequences lend themselves well to MCA-type decompositions

Emerging Best-Practices with Regard to TVC-Based Risk Assessment Models

Criteria for Evaluating MCA Techniques: A Top-Level View

- Internal consistency and logical soundness
- Transparency
- Ease of use
- Data requirements not inconsistent with the importance of the issue being considered
- Realistic time and manpower resource requirements for the analysis process
- Ability to provide and audit trail
- Software Availability, where needed

Relevant Questions To Pose When Evaluating TVC-Based Risk Models

- How is the threat information gathered? Does it come from multiple sources? How is the information combined or summarized?
- Are a broad range of possible threat scenarios utilized as part of the risk assessment process?
- Are the threat scenarios "generic" (e.g., oriented towards a "general threat environment") or are they asset- and/or location-specific?
- Is the utilized set of threat scenarios mutually exclusive and collectively exhaustive?
- If Risk Filtering techniques are utilized to arrive at a "manageable" set of threat scenarios, how is the filtering process implemented? Are "discarded" scenarios re-assessed at some later stage in the risk assessment/management process, perhaps in response to new or improved information?

Relevant Questions (cont.)

- Are likelihoods (expressed qualitatively or quantitatively) assessed for each identified threat scenario, or are all scenarios assumed to be equally likely?
- If qualitative characterizations of likelihood are utilized – such as "logical", "plausible", etc. – are precise operational definitions provided for these characterizations?
- Are cognitive biases managed as part of the threat characterization process?
- In what manner is the threat assessment coupled to the assessments of vulnerability and consequence?
- What attributes are utilized to characterize an asset's vulnerability?
- Is the scaling of the attributes *natural* or *constructed*?

Relevant Questions (cont.)

- Are the weights assigned to each attribute equal in value? If not, how are the swing weights arrived at?
- How are the consequences associated with specific threats characterized? Is more than one attribute used to characterize these outcomes? If so, are the attributes defined in a clear and consistent manner?
- If consequences are dependent upon threat, is the threat *level* clearly specified as part of the consequence valuation process?
- If more than one threat scenario is utilized as part of the consequence assessment, are the results aggregated in some way? If so, how is the aggregation accomplished?
- What are the specific outputs of the T-V-C analysis? If a relative risk ranking is produced, is a "risk score" provided for each asset? If so, how is this value interpreted?

Concluding Remarks and Recommendations

- RA and RM should not be disjointed
- EHS myopia – broaden the perspective
- Work towards a *generic* framework, with *modular specificity*

INSURANCE INFORMATION INSTITUTE ON-LINE

www.iii.org

If you would like a copy of this presentation, please give me your business card with e-mail address

Dr L James Valverde, Jr
Director, Economics and Risk Management
Insurance Information Institute
110 William Street
New York, NY 10038
Tel: (212) 346-5522
Fax: (212) 732-1916
jamesv@iii.org www.iii.org