

# Multi-Criteria Analysis and the Emerging TVC Paradigm

NATO Advanced Research Workshop on Risk Management  
Tools for Port Security, Critical Infrastructure, and Sustainability

**Dr L James Valverde, Jr**

Director, Economics and Risk Management

Insurance Information Institute

110 William Street

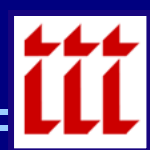
New York, NY 10038

Tel: (212) 346-5522

Fax: (212) 732-1916

[jamesv@iii.org](mailto:jamesv@iii.org) [www.iii.org](http://www.iii.org)

16 March 2006



## Risk Management and the U.S. GAO

- Motivation for the development of a RM framework
- Conceptual evolution of a RM framework
- The need for guidance to analysts

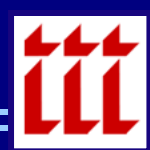
## GAO Risk Management Framework

- Individual components
- Integration of components
- A Closer Look at the Risk Assessment Component

## The Emerging T-V-C Paradigm in Homeland Security

- The role of MCA
- Applications to Port Security

## Discussion and Questions



### *British Medical Association*

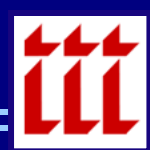
- The probability that something unpleasant will happen

### *Nuclear Industry*

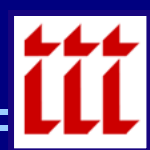
- The probability of an individual dying from radiation, integrated over the number of doses received and the number of people *receiving them*

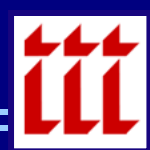
### *Pharmaceutical Industry*

- Research Scientist: the probability that a particular compound will go into development
- Development Scientist: the probability that the compound will be approved by the regulatory authority
- Marketing Manager: the probability that the drug will be a commercial success

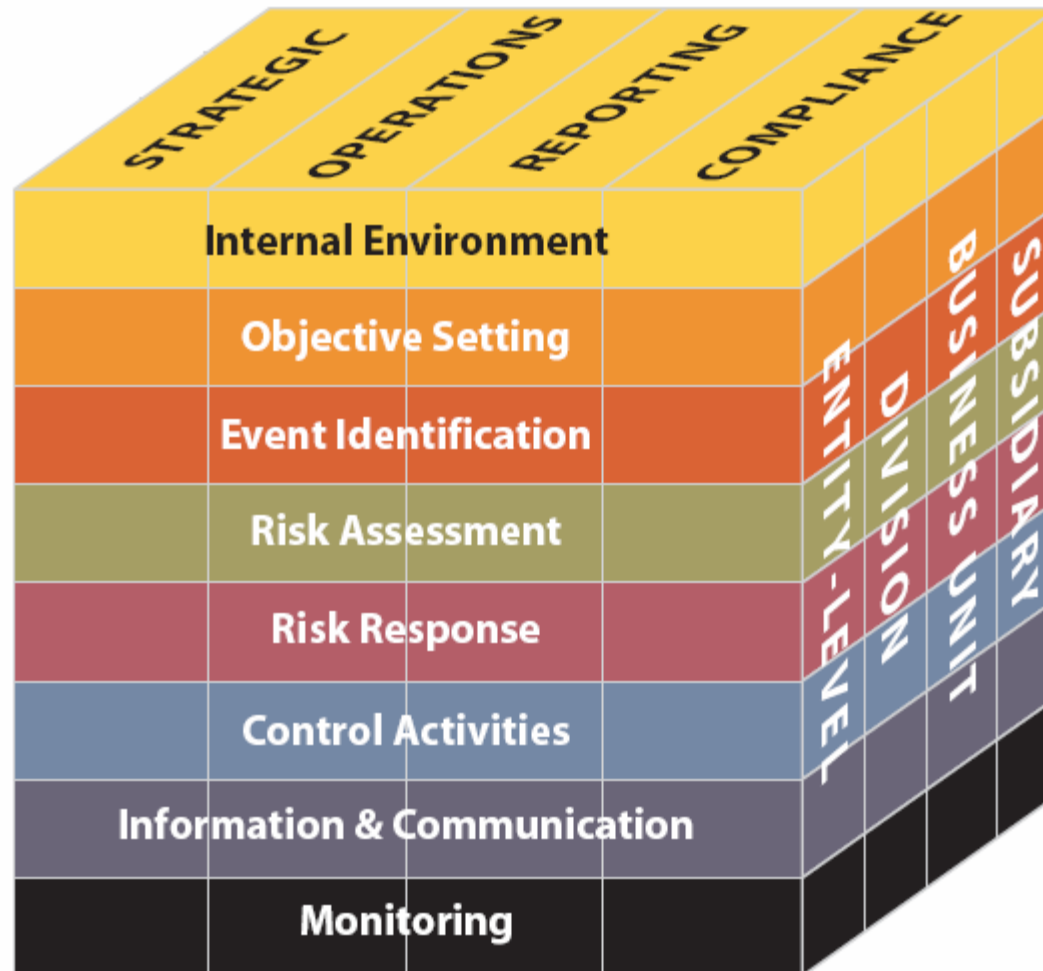


- Historically, mission-specific agency concerns:
  - Safety
  - Defense
  - Health
  - Investments
  - Natural Events
- Evolving mindsets, tools, and criteria for evaluating risk and integrating within specific decision contexts
- The events of 9/11 brought new visibility to this issue





## *Executive Summary*





## ***Risk Management: A GAO Analysts' Guide***

### **I. Introduction**

- A. GAO Risk Management Guide**
- B. Risk Management: An Evolving Practice**

### **II. The Elements of GAO's Default Risk Management Approach**

- A. Five Steps in GAO's Default Risk Management Approach**
- B. Evaluation Questions for the Framework's Five Steps**
  - 1. Strategic Goals, Objectives, and Constraints***
  - 2. Risk Assessment***
  - 3. Alternatives Evaluation***
  - 4. Management Selection***
  - 5. Implementation and Monitoring***

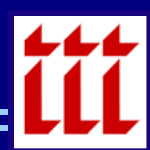
### **III. A Design Matrix for an Agency's Risk Management Process**

#### **Module**

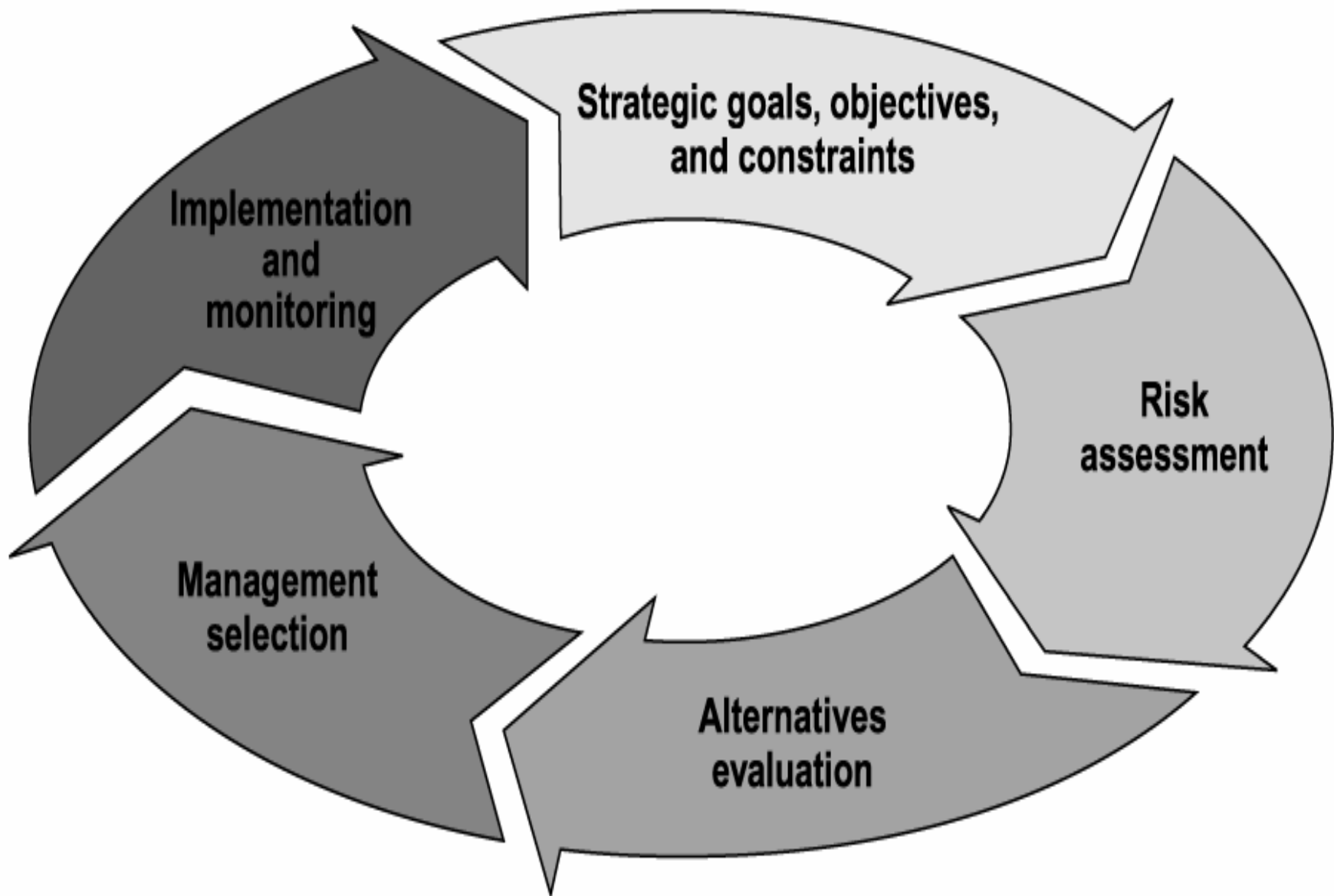
- I Applying the Framework to Homeland Security**

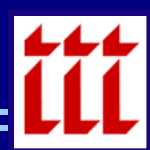
#### **Appendix**

- I Evolving GAO Risk Management and Homeland Security Graphics**

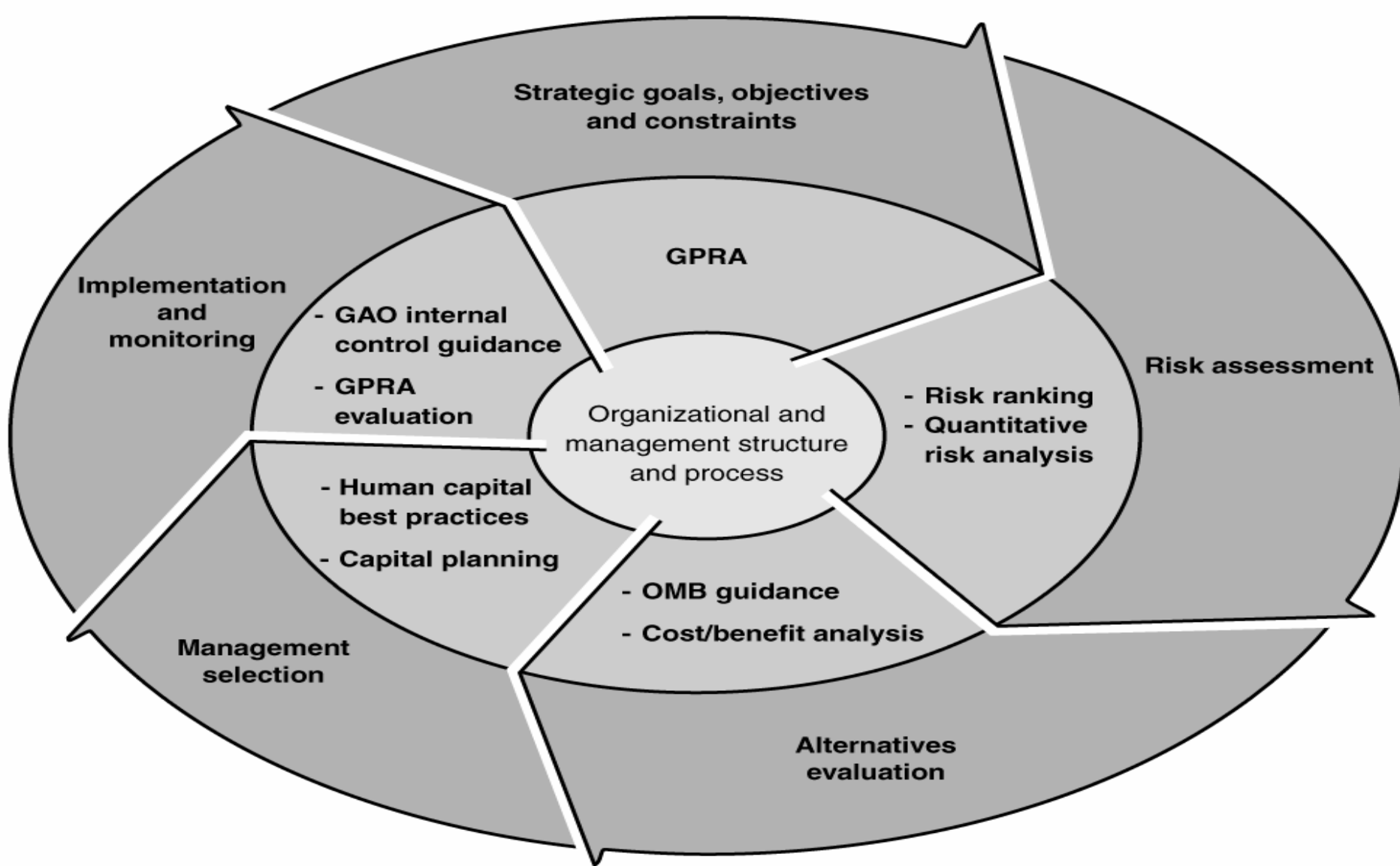


# Top Level: The GAO Risk Management Cycle



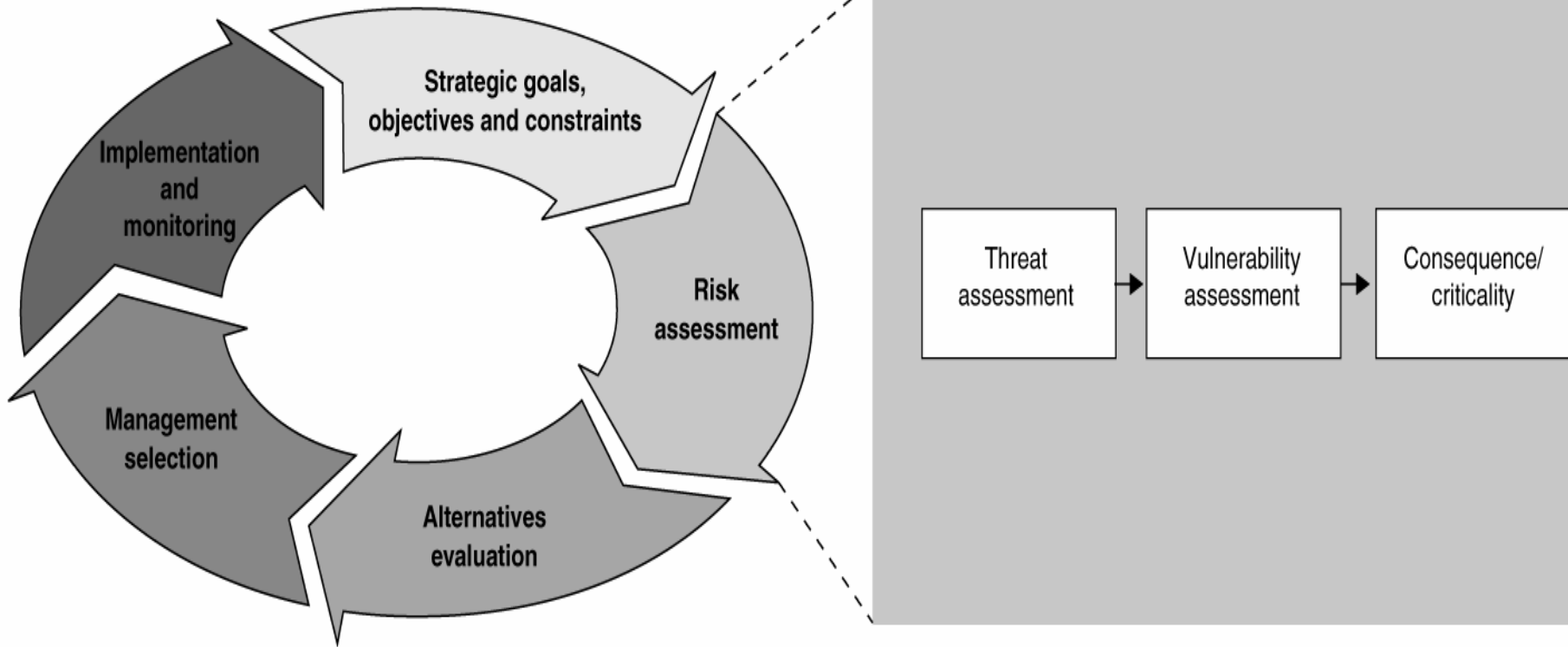


# Cross-cutting Criteria Sources





# Application-Specific Risk Assessment Steps: Security Applications



Source: GAO.



- 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



- 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.



- 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



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

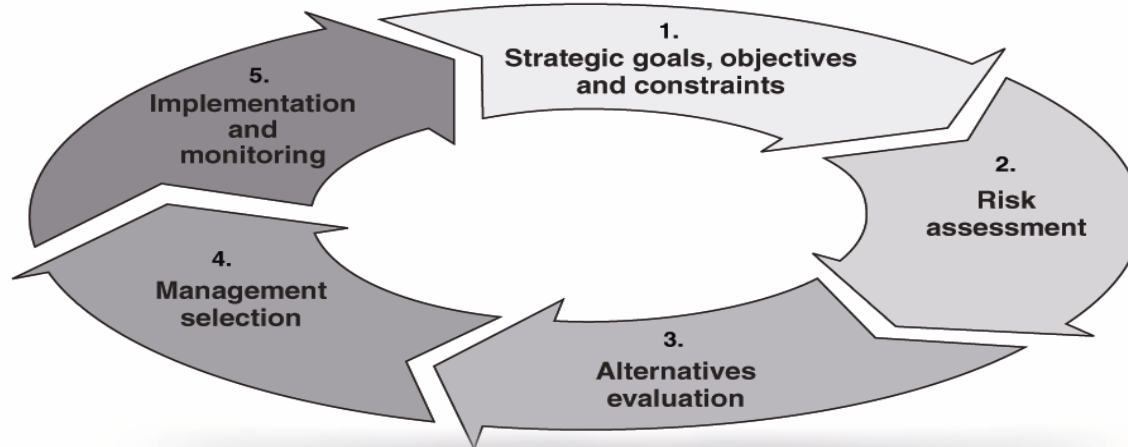


- Criteria for evaluating implementation are frequently contained in planning documents and federal guidance
- GAO's work focuses on internal controls and performance measurement
  - GAO's recommends that internal controls should generally be designed to ensure continual monitoring
  - GAO supports program evaluation for assessing *efficiency* and *effectiveness*.



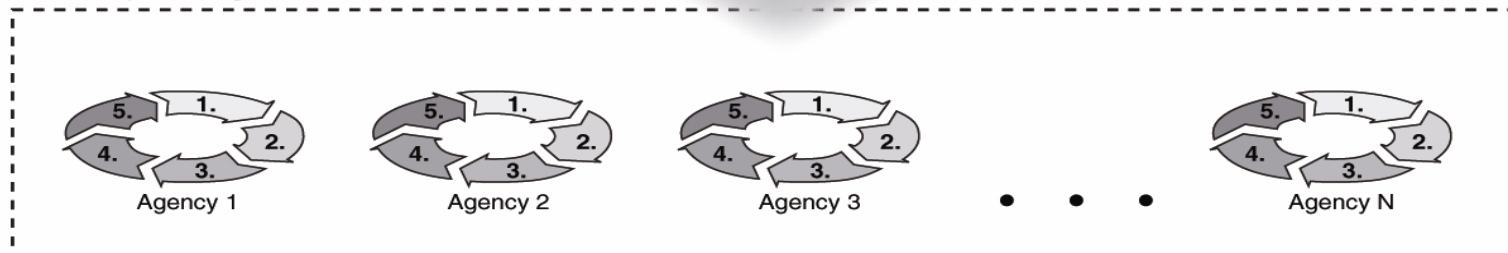
## Adaptability of the Framework:

- 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



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

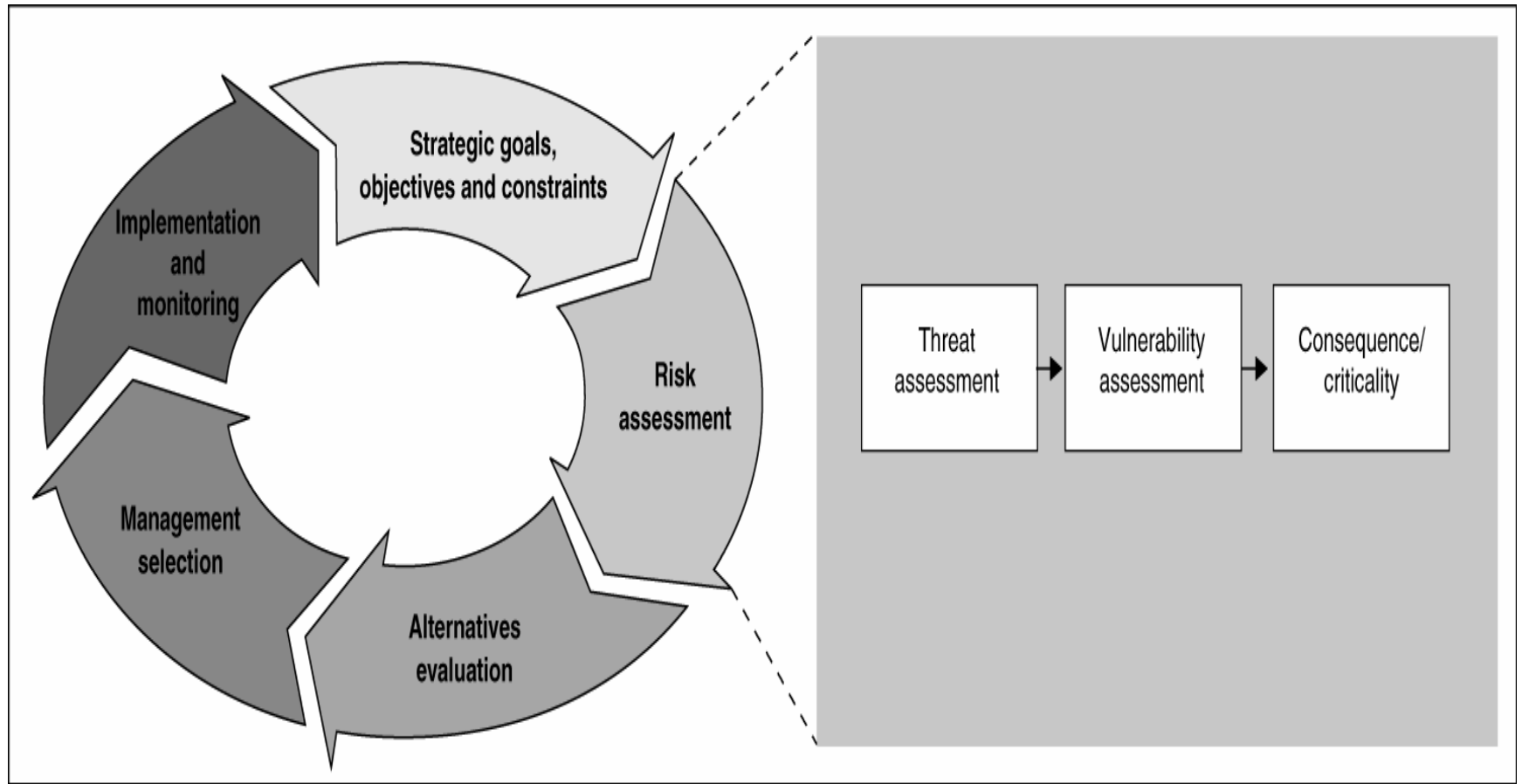
Sector-specific agencies



Risk management process is adopted for each sector-specific agency



# Risk Assessment: Applications to Homeland Security



Source: GAO.



- 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

## Threat Analysis

Attack Scenario  
Development  
 $\{A_i\}$

Probability of  
an Attack  
 $p(A_i)$

## Vulnerability Analysis

Probability of  
Success, Given  
an Attack  
 $q(S|A_i)$

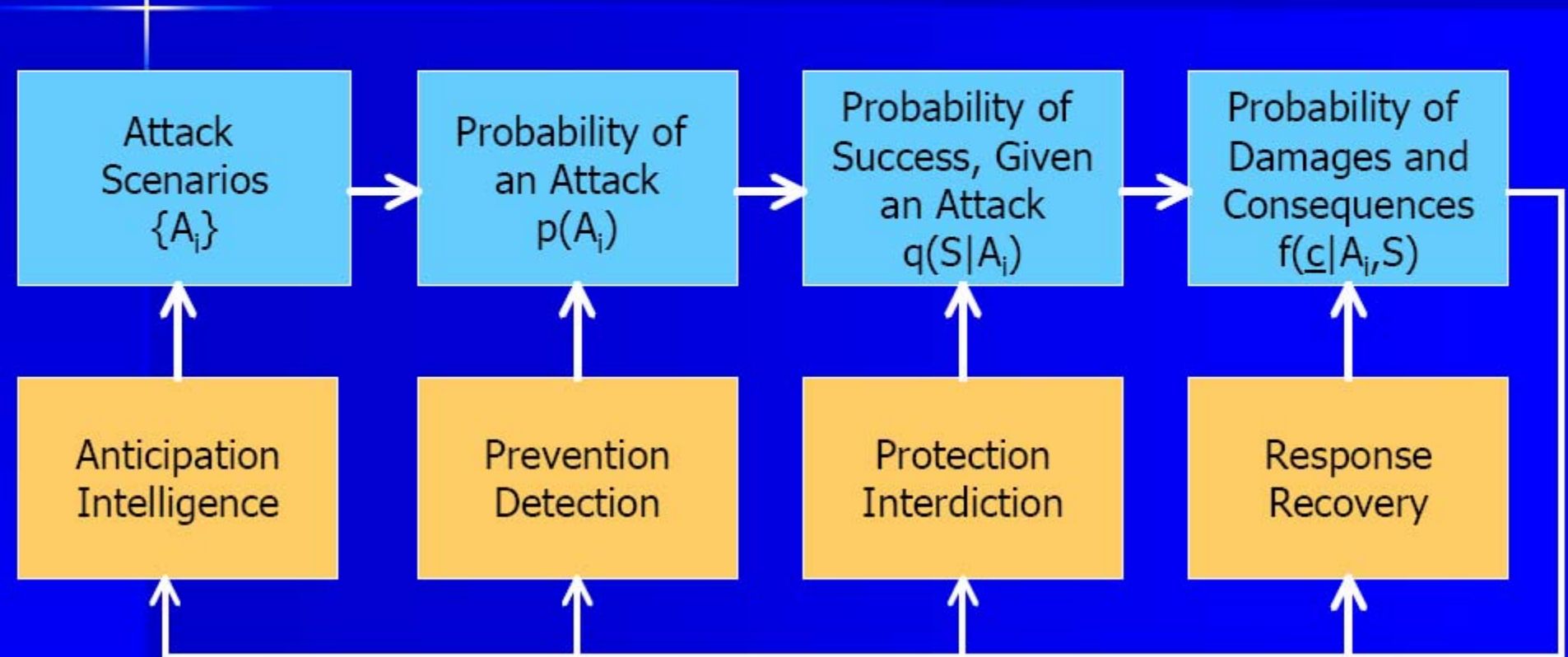
## Consequence Analysis

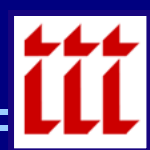
Probability of  
Damages and  
Consequences  
 $f(c|A_i, S)$





# Risk Analysis with Interventions

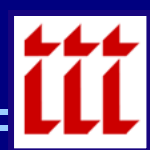




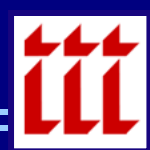
- Risk Assessment and reliability analysis often focus on the task of *probabilistic evaluation* of failure or accident scenarios
- A *failure scenario* can be described by a sequence of events
- Two commonly used analytical approaches:
  - Event tree analysis
  - Fault tree analysis



- 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



- 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



- 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



## **Applications to Port Security**



## Safe Harbors?



*The port of Charleston, S.C., is one of only five U.S. ports to have completed a detailed survey of its security needs as mandated by Congress.*

- Many people seem to fear port exposure
- New York, Norfolk, Charleston, Ft. Lauderdale, Los Angeles, Seattle all cited as making progress
- Canadian Exposure: 3 million containers travel in/out of Canada each year valued at C\$70 billion
- 27% of the 1.5 million containers imported into Canada wind up in the U.S.

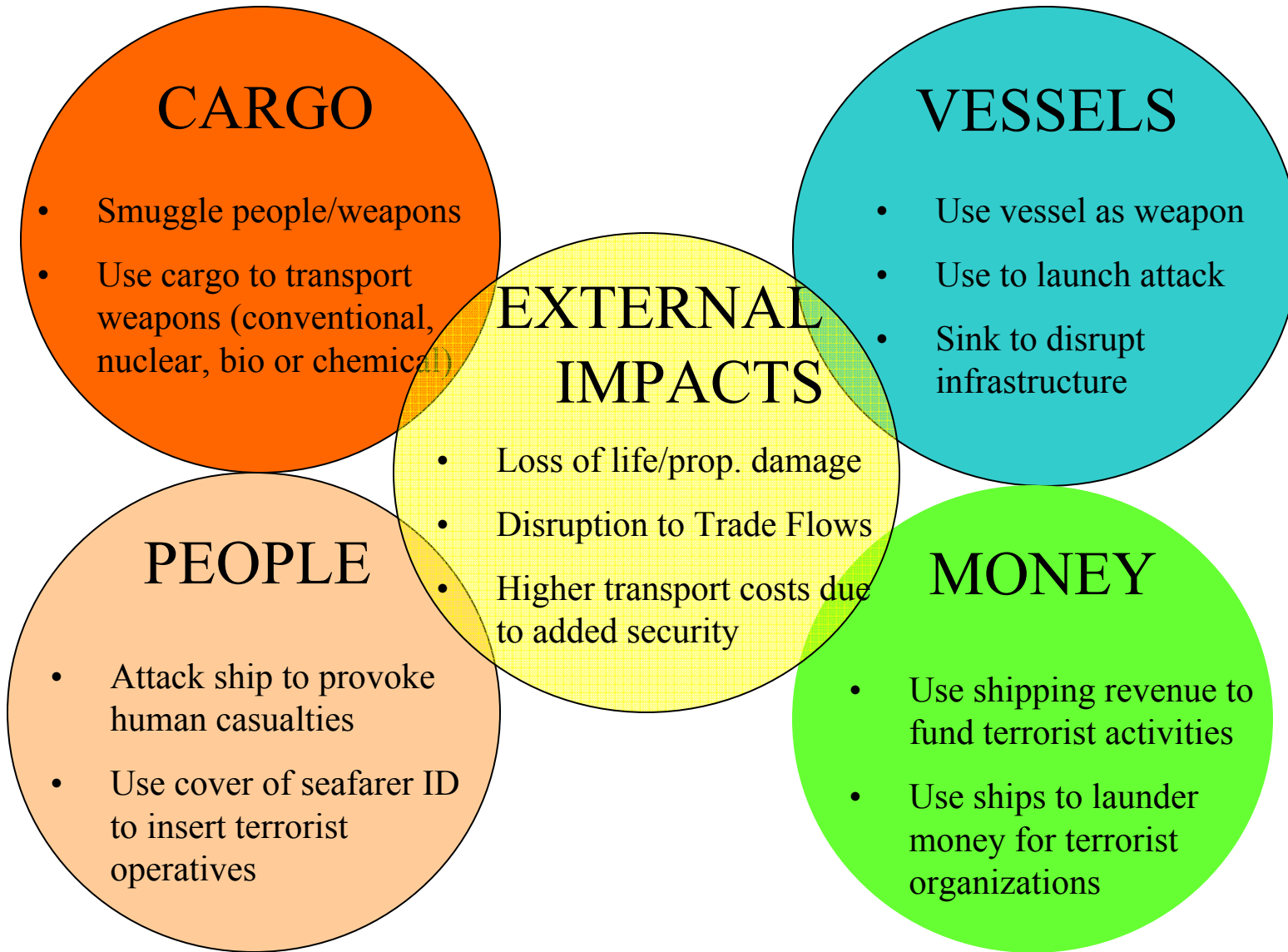


# The Realities of Port Security in the Post-9/11 Era





# Terrorist Risk Factors from Shipping





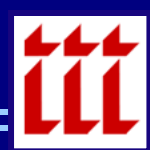
- Soon after 9/11, the U.S. Coast Guard began several risk-based activities and initiatives aimed at improving and managing port security
- The U.S. Coast Guard has developed numerous security plans — called *Area Maritime Security Plans* — to identify and address risks and vulnerabilities in and around the nation's key ports
- Other initiatives include the development of computer-based tools for assessing risks at specific port locations
- Another key initiative is the Port Security Grant Program. This program has awarded more than \$500 million in security grants to port authorities and industry stakeholders



- DHS efforts to tighten maritime container security have been criticized for:
  - Poor supervision
  - Lack of comprehensive strategy for keeping dangerous cargo from reaching U.S. ports
- Container Security Initiative has been widely criticized for failing to inspect all high-risk cargo.
- A bill recently introduced in the U.S. Senate may quell some of this criticism. The bill seeks to:
  - Codify existing programs and inspect and track shipping containers
  - Set minimum standards for all U.S.-bound containers
- Cause for concern: the standards will be enforced by a new Office of Maritime Cargo Security created within DHS.



- The conception of the PS-RAT was driven by the immediate needs that followed the events of 9-11
  - The need to prioritize the allocation of scarce Coast Guard resources to key activities
  - Risk-based Information needed to help frame resource constrained decision-making
- The PS-RAT was intended for use at the local level by Captains of the Port to establish priorities within their areas of responsibility
  - N-RAT developed to provide a national perspective
- A scenario-based approach is used whereby risk is evaluated for a combination of *target* and *means of attack*
- The prioritization of scenarios is based solely on their *relative risk*



- To characterize the relative risk of the many potential attack scenarios that the USCG must consider, the PS-RAT considers both the estimated *frequency of occurrence* and the *consequence severity* associated with each scenario
- Basic risk equation:

$$\text{Risk}_{\text{scenario}} = \text{Frequency}_{\text{scenario}} \times \text{Consequence}_{\text{scenario}}$$

- Threat, Vulnerability, and Consequence as underlying foundation for how risk is characterized within the PS-RAT



- The threat frequency is a measure of threat intensity
- Five levels of severity are described, and scoring benchmarks are provided
- Each level of threat intensity is assigned a relative probability of occurrence for use in risk calculations
- Captains of the Port could use the tool to vary the threat to conduct sensitivity analysis and contingency planning exercises



## Vulnerability Characterization within the PS-RAT

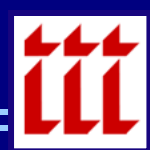
- Vulnerability is defined as the conditional probability of “success”, given that an attack occurs
- Vulnerability is scored based on perceived susceptibilities in each of four types of potential vulnerabilities:
  - Availability
  - Accessibility
  - Organic security
  - Target hardness
- For each type of vulnerability, five levels of severity are described, and scoring benchmarks are provided.
- Each level of severity in each type of vulnerability is assigned a relative probability of allowing an attack scenario to proceed for use in risk calculations.



- The consequence values are measured in a dimensionless value that can be thought of as a “pain index”
- Five levels of severity are described, and scoring benchmarks are provided
- A “pain index” value is assigned to each severity level of consequence, and the sum of these values represents the scenario’s overall level of consequence



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



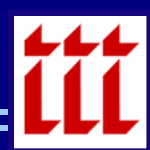
## Relevant Questions To Pose When Evaluating TVC-Based Risk Models

- 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?



## Some GAO Observations on PS-RAT Risk Methodology

- Models only looks at one scenario at a time (the USCG has used the terms “most probable” and “most plausible” to describe these scenarios)
- Cumulative risk profile (combining multiple scenarios) — not being done, but could be helpful at the national level
- Threat level (TL) is static and held constant; vulnerability and conse-quences drive the *entire* analysis; probabilistic interpretation of MARSEC levels
- Weighting (and scaling) of attributes (i.e., vulnerabilities and consequences)
- These issues partially explain some of the discrepancies between COTPS and PS-RAT results (e.g., PS-RAT ranks an asset as “low priority”, whereas COTP has a stark difference of opinion).



## Discussion and Questions



[www.iii.org](http://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](mailto:jamesv@iii.org) [www.iii.org](http://www.iii.org)