**RAMCAP™ EXECUTIVE SUMMARY**

RAMCAP™ (Risk Analysis and Management for Critical Asset Protection) is a framework for analyzing and managing the risks associated with terrorist attacks against critical infrastructure assets. RAMCAP™ provides a consistent and technically sound methodology to identify, analyze, quantify and communicate the various characteristics and impacts that may lead terrorists to select a particular target, and the impacts from a specific form of attack. It documents a process for identifying security vulnerabilities and provides methods to evaluate the options for improving these weaknesses.

- RAMCAP™ is simple, transparent and capable of being used effectively by participants across the nation’s critical infrastructure sectors.
- RAMCAP™ produces results that allow government to effectively compare and contrast risks among all sectors on a commensurate basis.
- RAMCAP™ methods are mathematically and statistically tractable, and appropriately rigorous.
- RAMCAP™ is forward-looking in that it provides obvious paths to incorporate more sophisticated or higher fidelity methods as they become available.

RAMCAP™ was developed with three major objectives in mind.

I. RAMCAP™ defines a common framework that can be used by owners and operators of critical infrastructure to assess the consequences and vulnerabilities relating to terrorist attacks on their assets and systems.

II. RAMCAP™ provides guidance on methods that can be used to assess and evaluate risk through the use of this common framework.

III. RAMCAP™ provides an efficient and consistent mechanism, which can be applied to diverse elements of both private and governmental (Federal, State and local) sectors to report essential risk information to the U. S. Department of Homeland Security (DHS). This reporting is crucial to the execution of responsibilities assigned to DHS.

DHS is compiling a baseline risk assessment of the entire U.S. critical infrastructure. The intent of DHS is to encourage the early use of simple, first order methods so that essential risk information can be reported and used in the near term. DHS, using the RAMCAP™ process, will foster the development and distribution of more rigorous methods as appropriate to improve the quality and consistency of risk assessments among sectors.
Background

Risk analysis methods have been used for many years for various purposes. For example, risk analysis is used to determine the replacement interval for equipment used in industrial plants. It is also used by insurance companies to determine the cost of insuring virtually anything that may be covered by loss and casualty insurance. Government and military organizations use risk analysis to evaluate the security of military bases and facilities. It is, therefore, reasonable to apply risk analysis to terrorism and homeland security.

The RAMCAP™ method was developed for application to the nation’s critical infrastructure using a general, broad-based approach. Sector-Specific Guidance documents (or SSGs) are currently being developed in various sectors using the RAMCAP™ framework. This is accomplished by adding sector-specific features and examples. It is also expected that different types of users will apply this guidance with different levels of detail, but with the common objective of determining, through consistent analysis, the critical assets and their associated level of risk from terrorist threats. RAMCAP™ is unique in that it facilitates the comparison of risks within a sector and across multiple sectors by employing a common terminology and standardized measurement metrics.

Many industry sectors and individual facilities have already invested significant resources to identify security vulnerabilities. This information has been developed using tools such as CARVER, RAM-D and other risk analysis methods. The results of these activities have been used to define and implement countermeasures and mitigation strategies. The RAMCAP™ methodology integrates the knowledge and data gained from the use of these tools to enhance the overall level of infrastructure protection.

RAMCAP – A 7 Step Approach

The RAMCAP™ framework is both qualitative and quantitative. RAMCAP™ is intended to be a cooperative effort on the part of asset owners and governmental agencies. Each participant strives to meet slightly different goals. Each participant has information valuable to the other. No government agency is in a position to know all of the pertinent details of any given facility or system relevant to risk assessment. No facility or system is in a position to understand the intentions and capabilities of a terrorist advisory. Working together and sharing appropriate knowledge through the use of the RAMCAP™, participants are all able to achieve their goals. Therefore, RAMCAP™ is at times, an owner/operator process and at other times an owner/operator/government process.
RAMCAP™ is comprised of seven (7) inter-related steps of analysis.

1. **Asset Characterization and Screening**
   Asset characterization and screening is the analysis of a facility or system’s operational processes to identify critical assets and hazards, while making a preliminary forecast of potential consequences from a terrorist act. The assets evaluated include both physical and cyber assets. The analysis includes identification of existing layers of protection.

2. **Threat Characterization**
   Threat characterization is the identification of specific and general modes of attack that may be used by terrorists against a given target. DHS has developed a set of baseline threats that are to be evaluated for each asset or system. These threats are based on the collective activities of law enforcement and intelligence organizations that are charged with developing an understanding of the means, methods and motivations of terrorists. The threats include various modes of attack (e.g., air, land, and water), and various sizes of attacks (e.g., small, medium, large). The owner/operator then applies these threats to the facility or system based on in-depth knowledge of the operation’s assets. Consequently, not all threats apply to all assets, so some threats will be screened from further consideration.

3. **Consequence Analysis**
   Consequence analysis is the identification of the worst reasonable consequences that could be generated by the specific threat. This step looks at facility or system design, layout and operation in order to identify the types of consequences that might result. Consequences that are quantified include financial costs, fatalities and injuries. Consequences that are noted qualitatively are psychological impacts and effects on national security or government functions. The SSGs describe the step-by-step approach to consequences based on the spectrum of threats as defined by DHS.

4. **Vulnerability Analysis**
   Vulnerability analysis is the determination of the likelihood for a successful attack using a specific threat on a particular asset. This involves analyzing the existing security capabilities, countermeasures and mitigation strategies and their effectiveness in reducing the probability of a successful attack.

5. **Threat Assessment**
   Threat assessment includes two steps: an evaluation of asset attractiveness and a full threat assessment. Asset assessment considers the perceived value to the terrorist of attacking a given facility or system considering the deterrence value of security measures and the robustness of the potential target. This area is assessed by the owner/operator. Threat assessment is performed by DHS and includes normalized assessments of attractiveness in light of the high level objectives of terrorists and intelligence-based assessments of adversary capabilities and intent.
6. **Risk Assessment**
Risk assessment is a systematic and comprehensive evaluation of the previously developed terrorism related data for a given facility or system. The owner/operator risk assessment creates a foundation for selecting strategies and tactics to defend against terrorist attacks by establishing priorities based on risk.

7. **Risk Management**
Risk management is the deliberate process of understanding risk and deciding upon and implementing action (e.g., defining security countermeasures, consequence mitigation features or characteristics of the asset) to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by the identification, evaluation and control of risks to a level commensurate with an assigned or accepted value.

The owner/operator of the individual asset is responsible for characterizing all assets that are owned or controlled by the person or corporate entity in charge. The asset characterization process includes a consequence-based screening feature. Data from the screening questions are sent to the National Asset Database (NADB). DHS will determine the magnitude of consequence that should be considered for further evaluation. Although an asset may not be considered critical by DHS, the owner may choose to proceed with the RAMCAP™ process for making risk decisions internally.

All assets that are considered critical to DHS will be asked to complete a RAMCAP™ Security Vulnerability Assessment (SVA), the results of which will be reported to DHS and included in the NADB. The asset owner/operator proceeds with the SVA, which is essentially a conditional risk assessment (conditional on the assumption that an attack will occur. The owner/operator also provides data to the NADB regarding the attractiveness of a facility or system to certain attacks, including deterrence features and other special characteristics that may be useful to DHS for determining the overall threat level. The conditional risk characterization from the owner/operator is combined with other information available from intelligence sources so that DHS can undertake a strategic risk assessment. DHS will then have the information that is needed to effectively allocate limited resources for risk reduction due to terrorism on a national scale.

**SUMMARY**

RAMCAP™ is intended to be an overarching and evolving framework for identifying, evaluating and managing risk to critical infrastructure assets related to acts of terrorism. It incorporates strategies and tactics used by industry, law enforcement and government. *It has been developed by industry for industry.* Participation is a cooperative venture between asset owners/operators and the Department of Homeland Security. ASME-ITI is a key partner in this process and continues to work with DHS and many other stakeholders to improve the RAMCAP™ methodology. ASME-ITI is also
leading the effort to develop a RAMCAP™ Standard and coordinate sector-specific activities.

FIGURES

Fig. 1 The RAMCAP™ 7-Step Process
ALL ASSETS

ASSET SCREENED OUT

TOP LEVEL SCREEN

ASSET SCREENED IN

ASSET CHARACTERIZATION

BELOW DHS THRESHOLD

ABOVE DHS THRESHOLD

DHS THRESHOLD

RAMCAP 7-STEP PROCESS WITH SVA BASED ON DHS SCENARIOS

RESULTS FROM SVA

OWNER/OPERATOR RISK MANAGEMENT

OWNER OPERATOR DIRECTED PROCESS

This activity is not requested by DHS. This activity may be conducted by the owner/operator for internal decision making.

CONSEQUENCE VULNERABILITY ATTRACTIVENESS INFORMATION FOR SCENARIOS

NATIONAL ASSET DATA BASE FOR USE BY DHS

BASIC INFORMATION FROM TOP SCREEN REPORT TO DHS

Fig. 2 RAMCAP™ Process Flow Diagram

Periodic Re-Evaluation of RAMCAP
Owners/Operators Provide Asset Information to DHS

Selected Facilities Provide DHS with Security Vulnerability Assessment

Apply Benchmark Threat Scenarios

Assess Consequences

Assess Vulnerabilities

Estimate Attractiveness/Deterrence

Consequence

Vulnerability

Threat

Conditional Risk Characterization

Strategic Comparative Risk Assessment

Government Intelligence

**References and Further Reading**


CREATE- Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, [www.USC.EDU/CREATE](http://www.USC.EDU/CREATE) (contains terrorism risk analysis papers from various CREATE symposia).


[http://www.memagazine.org/backissues/jan05/features/calcrisk/calcrisk.html](http://www.memagazine.org/backissues/jan05/features/calcrisk/calcrisk.html)

