

# Department of Homeland Security Risk Analysis and Management Approach for Critical Infrastructure Assessment

*The Risk Analysis and Management for Critical Asset Protection (RAMCAP) approach is being developed by the DHS to provide a common methodology that can be used to assess and manage security risks across all infrastructures. RAMCAP will include a screening approach as well as quantitative risk assessment tools. The methodology can be modified to address sector-specific issues.*

## 1 Introduction

The Risk Analysis and Management for Critical Asset Protection (RAMCAP) approach is being designed to provide guidance on approaches and methodologies for the following:

- Analyzing risks associated with adversary attacks
- Identifying and developing countermeasures and consequence-mitigation strategies to reduce risks
- Evaluating countermeasures and consequence-mitigation strategies using benefit-cost and other methods to inform resource allocation decisions.

The RAMCAP approach is intended to be a broadly applicable framework for all critical infrastructure sectors. Sector-specific features and examples can be added to fine-tune the approach for a specific sector. The approaches and methodologies employed by RAMCAP are designed to be general in nature and should only be used by experienced risk-analysis practitioners and decision-makers. Existing asset assessments or new asset assessments based on qualitative methods can be used with this approach. However, translation and calibration methods will need to be developed to jointly assess results from different sectors. It is expected that the RAMCAP approach will become a model for other assessment methods and, that over time these other methods will evolve to use the some of the methodology contained in RAMCAP.

While the RAMCAP approach is not a consensus standard, it does provide a listing of standard terminology with a definition for each term. It is recommended that risk-analysis practitioners and other stakeholders use this terminology to provide a common language for managing, mitigating, and communicating information on risk.

## 2 Technical Approach

In order to provide the most structured basis for decision-making, the RAMCAP approach will use a “scenario-based” rather than an “asset-based” approach. In addition,

in order to provide a basis for comparison of risks across industry sectors and to provide meaningful input to the decision-making process, the RAMCAP methodology is based on quantifying probability, consequence, and risk to the extent practicable. A screening methodology is provided to offer the means to decide which assets may not require the more detailed risk analysis and which of them should be assessed further using the detailed approach in this document. The screening methodology does not employ quantification in most cases, but approaches are provided to quantify some aspects of the results, if necessary. It is intended that existing risk-analysis methods be used, but that they be modified as necessary to make them consistent with the RAMCAP methodology.

### **3 Analysis Approach**

The RAMCAP is suitable for analyzing any of the following cases in a tiered manner so that lower-tier results can feed into higher-tier analyses:

- Analyses of risks for individual critical assets or groups of assets assuming that it would be performed by the asset owners.
- Analyses of risks within a critical infrastructure sector resulting from interdependencies among the critical assets within that sector assuming that the analyses will be performed by government agencies, groups of asset owners, industry associations, or other appropriate organizations.
- Analyses of risks for the nation, as a whole, resulting from interdependencies among critical infrastructure sectors assuming that the analyses will be performed by groups consisting of asset owners, industry associations, consultants, national laboratories, and government agencies.

Such a tiered structure allows for modeling and accounting for asset or sector interdependencies, and countermeasures (or consequence mitigation) strategies across assets or across sectors.

The RAMCAP methodology will consist of several analysis phases with several steps in each phase. The grouping of the steps into phases has been established primarily based on the organizations that are expected to have primary responsibility. In other words, it is anticipated that there would be a “handoff” of material and responsibility between phases. However, it will be important to have significant interaction among all stakeholders within each phase. For example, while it is anticipated that DHS, working with other government agencies, will have the primary responsibility for identifying critical assets and the nature of potential threats to those assets, it should be recognized that this process requires interaction with asset owners.

First Phase:

1. Identify critical assets

2. Identify nature and types of threats to the identified critical assets and estimate the frequency of attacks within broad ranges
3. Communicate with individuals responsible for risk analyses for identified critical assets.

Second Phase:

4. Perform asset-screening analyses to determine if a more detailed risk analysis should be done and to select specific asset/threat combinations for risk analysis.
5. Perform asset risk analyses for the selected asset/threat combinations, considering the short- and long-term consequences of credible attack scenarios for that asset. Damage to the surrounding community should be considered at this stage.
6. Perform Peer Review of the screening and risk analyses, to obtain a confirmatory check on the appropriateness of the methodologies used, reasonableness of key assumptions and results, and consistency of assumptions and results with those used by similar asset owners or in similar sectors.

Third Phase:

7. Perform sector risk analysis with consideration given to lost capacities and capabilities reported by individual asset owners. This analysis has the following steps:
  - a. Define analysis objectives and boundaries.
  - b. Gather pertinent risk analysis results from individual facilities/assets.
  - c. Use computer models that can simulate the short- and long-term consequences of the aggregate lost capacities and capabilities on the economy and on society as a whole based on asset interdependence.
  - d. Use expert elicitation to determine consequences resulting from the reaction of society to attacks (e.g., changes in travel and spending habits).
  - e. Assemble information to construct, with the aid of computer models, event trees that extend the individual facility risk analyses to the regional and national levels, considering interdependencies.
  - f. Determine the risk from individual attacks and the aggregate risk of repeated attacks.
  - g. Develop proposed countermeasures and consequence-mitigation initiatives on an industry sector and/or national basis.
  - h. Evaluate proposed countermeasures and consequence-mitigation strategies using benefit-cost analysis and other measures.

Fourth Phase:

8. Perform risk analysis for multiple sectors:
  - a. Define analysis objectives and boundaries.

- b. Gather pertinent risk analysis results from sectors.
  - c. Assess interdependency among sectors.
  - d. Identify countermeasures and consequence-mitigation strategies.
  - e. Make appropriate decisions.
9. Document, implement, monitor, update, and communicate with all participating organizations throughout the phases.

Several aspects of a risk analysis are applicable regardless of the scope or phase of the process, including

- Documentation of the key inputs, assumptions, and methods
- Monitoring changes in threats and in consequence mitigation and countermeasure capabilities over time
- Updating the risk analysis to reflect the changes and new knowledge and technology
- Communicating appropriate aspects of the analysis with, and obtaining input from key stakeholders

#### **4 Analysis Products**

A variety of products will be generated from this process. The final form of these products is still being designed.

#### **5 Software Aids and References**

A variety of documentation products will be generated to support the RAMCAP. In the general category are:

- Risk Analysis and Management for Critical Asset Protection: General Guidance
- Risk Analysis and Management for Critical Asset Protection: Asset Application Handbook.

For up to 16 different sectors the following specific guidance documents may be produced:

- Risk Analysis and Management for Critical Asset Protection: A Standard for Vulnerability Analysis
- Risk Analysis and Management for Critical Asset Protection: Sector Specific Guidance.