ELSEVIER

Journal of Hazardous Materials 142 (2007) 689–694

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Development of a security vulnerability assessment process for the RAMCAP chemical sector☆

David A. Moore[a,*], Brad Fuller[a], Michael Hazzan[a], J. William Jones[b]

[a] *AcuTech Consulting Group, 2001 North Beauregard Street, Suite 100, Alexandria, VA 22311, United States*[1]

[b] *RAMCAP, ASME ITI, LLC, 1828 L Street NW, Washington, DC 20036, United States*[2]

Available online 6 July 2006

Abstract

The Department of Homeland Security (DHS), Directorate of Information Analysis & Infrastructure Protection (IAIP), Protective Services Division (PSD), contracted the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME ITI, LLC) to develop guidance on Risk Analysis and Management for Critical Asset Protection (RAMCAP). AcuTech Consulting Group (AcuTech) has been contracted by ASME ITI, LLC, to provide assistance by facilitating the development of sector-specific guidance on vulnerability analysis and management for critical asset protection for the chemical manufacturing, petroleum refining, and liquefied natural gas (LNG) sectors. This activity involves two key tasks for these three sectors:

- Development of a screening to supplement DHS understanding of the assets that are important to protect against terrorist attack and to prioritize the activities.
- Development of a standard security vulnerability analysis (SVA) framework for the analysis of consequences, vulnerabilities, and threats.

This project involves the cooperative effort of numerous leading industrial companies, industry trade associations, professional societies, and security and safety consultants representative of those sectors. Since RAMCAP is a voluntary program for ongoing risk management for homeland security, sector coordinating councils are being asked to assist in communicating the goals of the program and in encouraging participation.

The RAMCAP project will have a profound and positive impact on all sectors as it is fully developed, rolled-out and implemented. It will help define the facilities and operations of national and regional interest for the threat of terrorism, define standardized methods for analyzing consequences, vulnerabilities, and threats, and describe best security practices of the industry.

This paper will describe the results of the security vulnerability analysis process that was developed and field tested for the chemical manufacturing sector. This method was developed through the cooperation of the many organizations and the individuals involved from the chemical sector RAMCAP development activities. The RAMCAP SVA method is intended to provide a common basis for making vulnerability assessments and risk-based decisions for homeland security.

Mr. Moore serves as the coordinator for the chemical manufacturing, petroleum refining, and LNG sectors for the RAMCAP project and Dr. Jones is the chief technology officer for ASME-ITI, LLC for RAMCAP.

Keywords: SVA; RAMCAP; DHS

1. Introduction

Security vulnerability analysis (SVA) has been extensively conducted since 9/11 on numerous assets across the United States including those of the chemical sector. SVA methods such as the American Institute of Chemical Engineers' "Guidelines for managing and analyzing the security vulnerabilities

☆ Mary Kay O'Connor Process Safety Center, Texas A&M University System, 2005 Annual Symposium, October 25–26, 2005, Reed Arena, Texas A&M University, College Station, Texas.

* Corresponding author. Tel.: +1 415 772 5972; fax: +1 415 772 9044.
E-mail address: dmoore@acutech-consulting.com (D.A. Moore).

[1] http://www.acutech-consulting.com.

[2] http://www.asme-iti.org.

0304-3894/$ – see front matter © 2006 Published by Elsevier B.V.
doi:10.1016/j.jhazmat.2006.06.133

of fixed chemical sites"[3] have been published to help structure the analysis process for the chemical industry. The American Petroleum Institute (API) and the National Petrochemical and Refiner's Association (NPRA) have developed a guideline for conducting SVAs of petroleum and petrochemical facilities in May, 2003. In 2004, API/NPRA enhanced their guidelines by extending their methodology from addressing the risk at fixed facilities to transportation security risks (i.e. pipeline, truck, and rail). These processes are designed and employed to identify potential point targets of terrorism, and to classify these potential targets in broad terms. By doing so, industry can begin the process of deciding how best to address their specific vulnerabilities.

As the Department of Homeland Security (DHS) stood up as a new Federal agency in March 2003, many of these processes were already in practice throughout industry. DHS wanted to capitalize on the many good efforts of industry, but recognized that this was difficult within some sectors or across sectors since most of the methodologies being used had somewhat differing approaches, terminology, criteria, scales, and outputs. No existing process existed that accomplished all of the needs of DHS in determining sector and cross sector vulnerabilities and consequences. They wanted a process that met their strategic risk assessment needs as well as those needs of the asset owner.

Underlying the need for a technical vulnerability process was the realization that the potential for infrastructure protection initiatives far exceeds the resources available. A process is needed to identify the priorities for allocating these limited resources. This process should be based on guidance that defines consistent, objective, and integrated application of risk analysis methods.

2. RAMCAP project

These issues led DHS to contract with the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME ITI, LLC) to develop guidance on Risk Analysis and Management for Critical Asset Protection (RAMCAP). ASME had been contracted in 2003 by the Office of Domestic Preparedness to develop the core concepts for RAMCAP. In 2004 DHS initiated the pilot phase where the concept was implemented at the sector and sub-sector level. The initial pilots included the chemical manufacturing, petroleum refining, liquefied natural gas, nuclear, and nuclear spent fuel sectors, which are to be implemented in 2005–2006. Additional sectors are to follow upon completion of the pilot sectors.

As a complement to these analytical approaches, companies may want to develop risk acceptance criteria and decision tools to guide SVA teams in their counter-measures selection. RAMCAP may highlight vulnerabilities that the asset owner would like to address, but the need to address any risks or recommendations from the analysis is optional. The RAMCAP framework guidance may indicate the degree of vulnerability to higher consequence events, thereby indicating to management the importance of risk reduction measures.

3. RAMCAP overview

RAMCAP stands for Risk Analysis and Management for Critical Asset Protection, and is a framework for analyzing and managing the risks associated with terrorist attacks against critical infrastructure assets in the United States. RAMCAP provides a consistent and technically sound methodology for analyzing consequences of attack, identifying security vulnerabilities and developing threat information based on both asset owner and government information. Additionally RAMCAP provides methods for DHS to analyze risk, and to evaluate countermeasures and mitigation procedures aimed at reducing vulnerabilities in the infrastructure to a terrorist attack.

RAMCAP was developed with three major objectives in mind:

- To define a common framework that can be used by owners and operators of critical infrastructure to assess vulnerability from terrorist acts to their assets and systems.
- To provide guidance on methods that can be used to assess and evaluate risk information developed through the use of this common framework.
- To provide 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.

4. Challenges

The RAMCAP project is challenging given its ambitious objectives, national scale and multi-sector nature. Ultimately the project has to efficiently produce a characterization of the industry and consequence, vulnerability, and threat information that was otherwise not available in a common form or place. There is urgency to having this information given the current threat to homeland security, and the challenge DHS faces in understanding the vulnerabilities of the infrastructure.

All parties will naturally benefit from clearer insight to the nature of the most critical facilities in the country. Government can make use of this information to improve their knowledge and direction to put resources where they would be the most effective. Industry can validate their SVA information against a national homeland security framework and become more informed of possible security threats.

Some goals and constraints of the project were to develop a strategic process that had the following attributes:

- A simple assessment process that produced enhanced information to allow industry and government to better understand national terrorism consequences, vulnerabilities, and threats to the chemical manufacturing industry.

[3] Guidelines for managing and analyzing the security vulnerabilities of fixed chemical sites, American Institute of Chemical Engineers, August 2002.

- A process that is compatible with the existing SVA processes and that will eventually help to align them in a common framework without interfering with their past efforts.
- An assessment that can be done efficiently by plant personnel at a major facility without outside assistance.
- A process that scales threats against infrastructure in a uniform way to allow for inter and intra sector comparisons, when SVA methods and infrastructure issues vary widely.
- A set of common terminology and assumptions allowing for more accurate comparisons.

A particular challenge was to resolve the issues of quantitative versus a qualitative approach. Feedback from the chemical industry was that they believed a quantitative method that attempted to put a predictive estimate on the probability of an attack on a particular asset at the outset of the analysis was not currently practicable. The reasons for this are that there is insufficient experience with terrorist acts, particularly in the United States, to be able to predict these acts on an absolute basis. Thus, the first step will be to determine "conditional risk", i.e. the risk to a facility or asset assuming that a threat actually does occur.

5. RAMCAP screening

A preliminary step to implementing the RAMCAP SVA approach is to screen sector assets to a prioritized list of assets of interest to national homeland security. As shown in Fig. 1, the screening tool is intended for use by the chemical sector to collect information on sector assets to allow for screening of higher priority sites for RAMCAP. This would supplement the information in the National Asset Database (NADB) for the chemical sector. In addition the RAMCAP data developed for the sector would allow DHS to analyze:

- Potential national impacts.
- Necessary thresholds for performing and reviewing RAMCAP SVAs and/or site visits or for other site specific follow-up activities.
- Necessity for buffer zone protection programs (BZPP) and resource application.
- Chemical sector assets to other lists of assets in other sectors.
- Interdependencies and how to focus resources on specific unique assets.
- Asset information against threat stream data to assist industry for operational security.

Additionally, it must have the following characteristics:

- Consistent and rational metrics across all sectors to allow for cross sector comparisons.
- Fairly granular (i.e. of sufficient detail) to allow for definition of assets across the spectrum of assets included.
- Datum points (parameters, as shown in Table 1).
- Subject to data verification and analysis within DHS.
- Ease of use to accomplish and produce value for all.
- Proper and appropriate security from the input stage to any ultimate use of the information, consistency with government

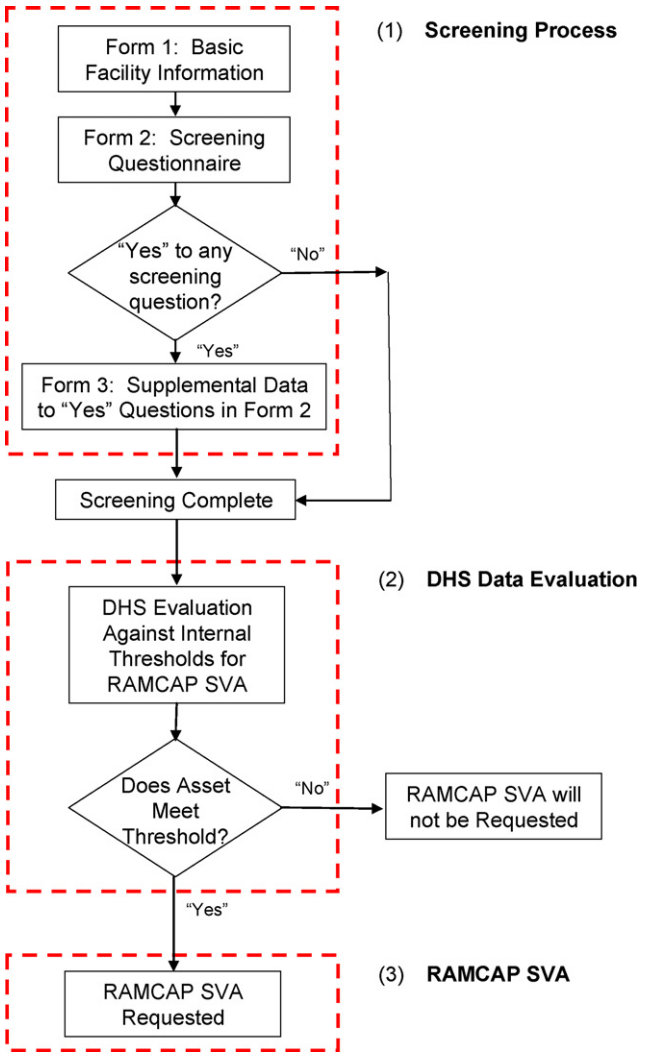

Fig. 1. RAMCAP screening tool concept diagram.

Table 1
DHS screening database parameters

1. Human health and safety impacts
(a) Exposed population
(b) Acute fatalities
(c) Chemical weapons precursors/weapons of mass destruction onsite
(d) Final food or pharmaceutical products made onsite
2. Economic impacts
(a) Asset replacement costs
(b) Remediation costs
(c) Business interruption costs
(d) National/regional economic importance/multiple sector impact
3. National security and government functionality impacts
(a) Military mission importance
(a) Delivery of public health services
(a) Critical potable water or electrical energy services
4. Psychological impacts
(a) Iconic/symbolic assets
(b) High profile and/or symbolic casualties

procedures for classified information, critical infrastructure information, and other categories of protected information.

The DHS RAMCAP screening tool is envisioned as a web-based application to collect specific information that will allow the agency to better analyze and manage the risks associated with the security of the chemical sector. The concept is depicted in Fig. 1 and consists basically of three forms that are self-completed by industry online. Each of these forms is described below:

- *Form 1*: this form consists of basic facility information that will allow DHS to identify the facility, supporting administrative information regarding the facility (e.g. ownership, EPA identifier numbers, etc.), location, and the chemicals held at the site and their quantities.
- *Form 2*: this form consists of the screening questions that are intended to filter out those facilities that, by the nature of their business, location/proximity to significant population groups or other parts of the infrastructure of the nation, or importance to the national economy or military capability pose a "low" national security consequence.
- *Form 3*: only those facilities that did not screen-out after completing Form 2 (i.e. those facilities that answered any screening question "yes") would complete Form 3. This form consists of the actual parameters that will provide data to describe a facility's security-related risks in the following four impact types:
  - Human health and safety.
  - Economic.
  - National security and government functionality.
  - Psychological.

6. RAMCAP SVA approach

The RAMCAP SVA is comprised of seven (7) inter-related areas of analysis as illustrated in Fig. 2:

(1) *Asset characterization*: asset characterization analyzes the technical details and operational processes of a facility to identify the critical assets of the facility that have the potential for human health and safety, economic, government functionality, and psychological impacts on a national scale. The identified critical assets will be the only facility assets analyzed in the remaining six steps.
(2) *Threat characterization*: threat characterization seeks to identify specific and general modes of attack that may be used by terrorists against a given target. DHS bases its characterizations 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. These efforts are aided by the in-depth facility knowledge and perspective of the facility operator, whose own analysis may identify threats not readily recognized by DHS. DHS poses standard RAMCAP threats including various modes of attack (e.g. air, land, and water), and various sizes of attacks (small, medium, and large).
(3) *Consequence analysis*: consequence analysis identifies the worst reasonable consequences that could be generated by the specific RAMCAP threat scenarios. This step looks at facility design, layout and operation in order to identify the types of consequences that might result. Both causality and financial impacts resulting from different damage scenarios are estimated and ranked on a standard consequence scale. The RAMCAP guidance provides a set of rules and assumptions for consistent analysis of consequences against the benchmark threats introduced in Step (2).
(4) *Vulnerability analysis*: vulnerability analysis seeks to determine the strength or weakness of targeted asset and inherent protective systems to a specified threat. This involves analyzing the existing capabilities and countermeasures at the asset or entire facility, and their effectiveness in reducing the overall vulnerability to the threat scenarios evaluated.
(5) *Threat assessment*: the RAMCAP threat assessment is comprised of two analyzes, one performed by the asset owner and one performed by government. In this step, the asset owner is limited to an assessment of their facility/asset attractiveness. Using the information from the asset owner, DHS performs the overall threat assessment combining the attractiveness information with high-level objects of terrorists and government.
(6) *Risk assessment* (*optional for asset owner*): for the purposes of RAMCAP, security risk can be estimated by considering the analysis and aggregation of consequence, vulnerability and threat. The risk assessment is a systematic and comprehensive evaluation of the previously developed terrorism related data for a given facility. 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* (*optional for asset owner*): 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 identifying, evaluating, and controlling 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. The Department of Homeland Security will determine the magnitude of consequence that should be considered for further evaluation. Assets that are not considered to be critical to DHS may be of such importance to the asset owner that they may choose to proceed with the RAMCAP process for their own decision making process.

7. DHS strategic risk assessment process

All assets that are considered in the screening process are reported to DHS and included in a database. A smaller subset of

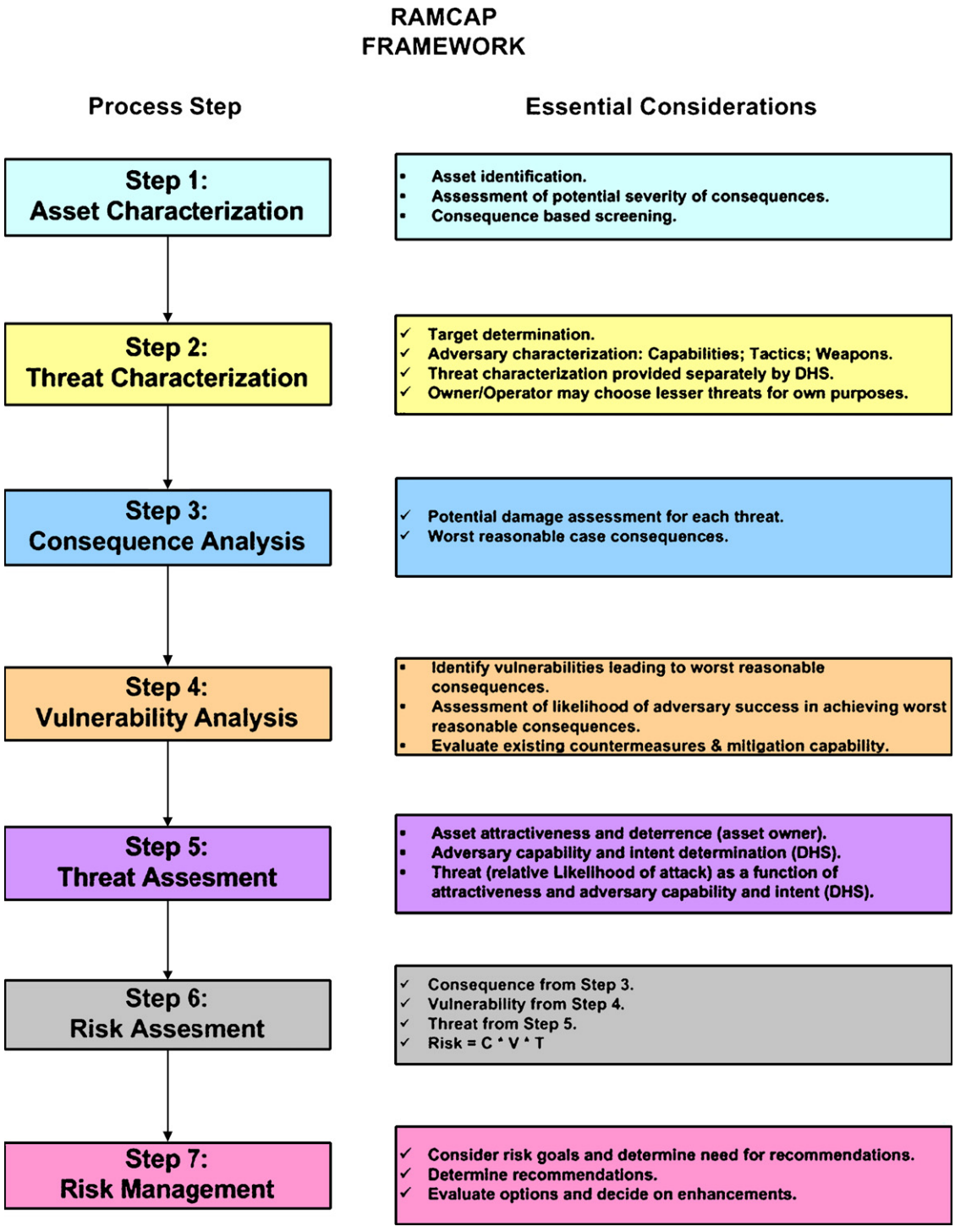

Fig. 2. The seven steps in the RAMCAP process.

assets is subjected to the remaining steps in the process based on criteria established by DHS. The asset owner/operator proceeds with a conditional risk assessment. The owner/operator provides information to DHS regarding the attractiveness of their facility to certain attacks, deterrence features, and any other special characteristics that may be useful to DHS for determining the overall threat to the asset. The conditional risk characterization from the owner/operator is combined by DHS with other information available from intelligence sources to provide a strategic risk assessment. This information is collected in a national database that will provide decision makers with information needed to allocate resources to reduce overall terrorist risk as much as possible as illustrated in Fig. 3.

8. Closing

The methodology is currently in a pilot testing phase at several large and small chemical facilities. Both the screening

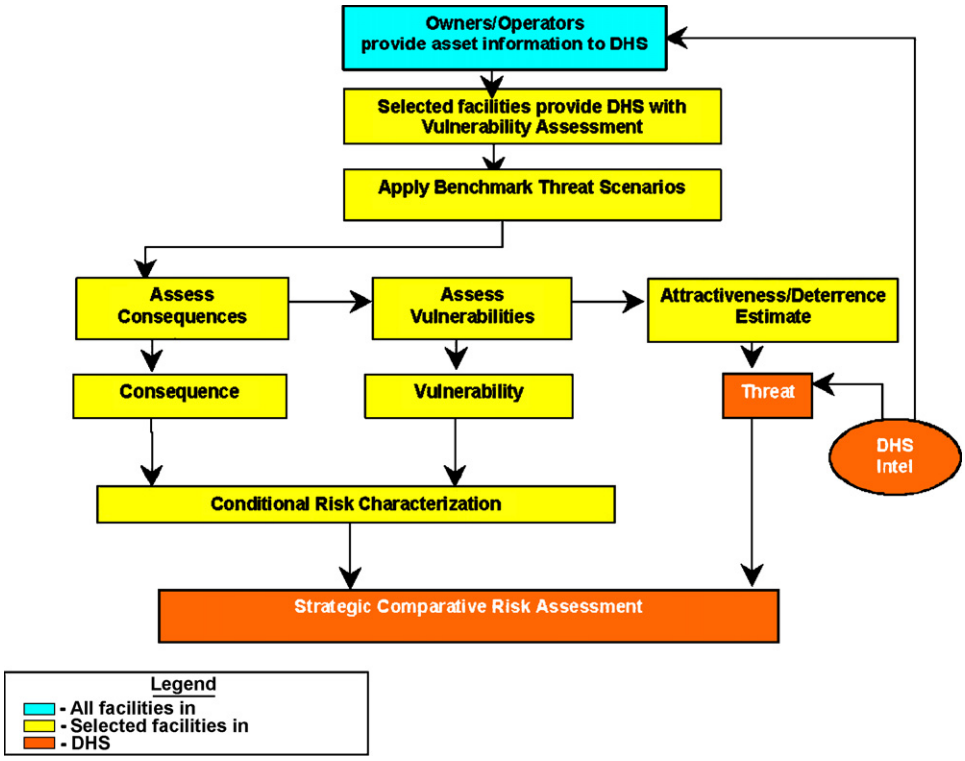

Fig. 3. DHS strategic risk assessment process.

process and the RAMCAP chemical sector SVA process will be tested. The details of the methodology will be reported at a later date in the form of a guidance document.

Preliminary results indicate that the process proves to be useful at identifying vulnerabilities over and above the existing methodologies that had been used at the sites evaluated to date. This is primarily because the threat scenarios used were in some cases beyond the range of threats previously considered by the asset owners, therefore new issues were identified. While the development of risk management measures to reduce these vulnerabilities were not a required part of the process, useful ideas came from the analysis that the asset owners performed in the course of the SVA. Based on these pilot results the RAMCAP SVA guidance will be further developed. Screening and guidance processes will be implemented in 2005–2006.

The primary objective of the RAMCAP project is to develop a risk based methodology that can be easily applied by industry that will assist both government and industry in the allocation of limited resources to fight terrorist threat. RAMCAP will improve the overall understanding of risk and, using common metrics and common procedures, allow risk to be compared both within and across industry sectors.