

Security Risk Assessment Methodology for Communities (RAM-C™)

INTRODUCTION

Sandia National Laboratories (SNL) has developed a number of security risk assessment methodologies (RAMs) for various infrastructures including dams, water systems, electrical transmission, chemical facilities and communities. All of these RAMs consider potential malevolent attacks from different threats, possible undesired events and consequences and determine potential adversary success. They focus on the assessment of these infrastructures to help identify security weaknesses and develop measures to help mitigate the consequences from possible adversary attacks. This paper will focus on RAM-C™, the security risk assessment methodology for communities.

There are many reasons for a community to conduct a security risk assessment. They include: providing a way to identify vulnerabilities, helping a community to be better prepared in the event of an adversary attack, providing justification for resources to address identified vulnerabilities and planning for future projects. RAM-C™ provides a systematic, risk-based approach useable by public safety and emergency planners to determine relative risk and provides useful information in making security risk decisions.

RAM-C™ consists of a number of steps starting with a screening step which selects facilities based on a documented process; characterization of the community and facilities; determination of severity of consequences for identified undesired events; determination of the community protection goals and defining the threat; defining existing baseline safeguard measures; analyzing protection system effectiveness against identified scenarios, determining a relative risk and finally deciding if that risk is too high. If the risk is too high then possible countermeasures and mitigation measures are considered.

RAM-C™ has been used by a number of communities within the United States. From these assessments there have been many results. Some communities have been surprised by the vulnerabilities that have been identified; have identified the need to test procedures and responses to many different situations; have identified the need to have redundancy in certain systems and have identified who within their community are valuable resources. The RAM-C™ process is a systematic way to assess vulnerabilities and make decisions based on risk. It has provided valuable information to community planners.

RAM-C™ PROCESS

RAM-C™ is a risk-based security risk assessment methodology. The benefits of using risk are that it combines three relevant factors (i.e. Likelihood of Attack, Consequences and Protection System Effectiveness) into a single parameter; allows threat, security system, and consequence; and helps in prioritizing/justifying requirements and budgeting. The following shows the process used in RAM-C™.

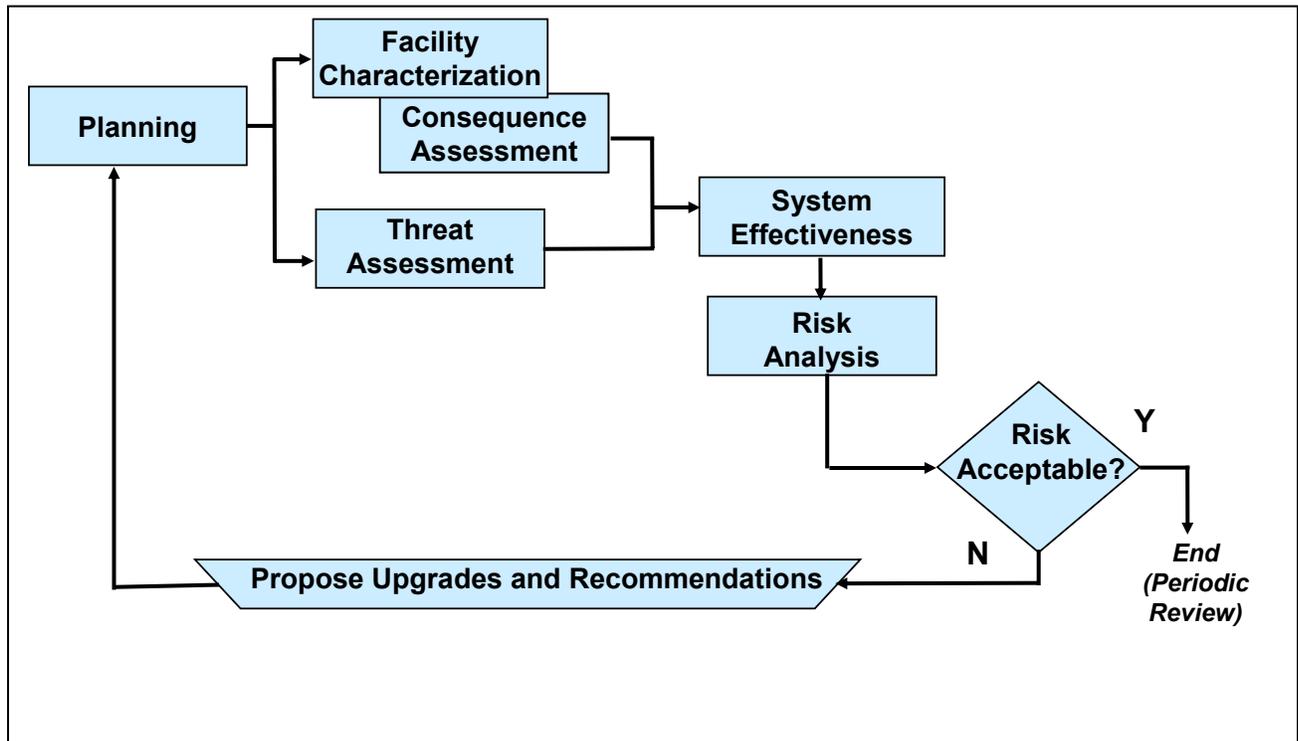


Figure 1. RAM-C™ Process

The process must support security decisions. The output from the RAM-C™ analysis will (1) identify how well people and assets are protected, (2) what is the relative risk, (3) what are the vulnerabilities, and (4) how can those vulnerabilities be minimized. Based on the analysis, decisions makers must determine how much risk is tolerable and how reduction in risk can be funded. The community defines its security goals. These will include what is important to the community, financial resources available and the acceptability of the potential consequences of an adversary action. Security goals could include protecting lives, protect property, preventing loss of services and other areas.

RAM-C™ can help the community make security decisions based on a systematic process. In the following sections each of the RAM-C™ process steps are discussed in more detail.

Planning

Community leaders take a lead role in this step in helping to establish criteria for prioritizing facilities/activities. In addition others in the community should be involved. This could include personnel involved in emergency management, police, fire departments, civic leaders, financial leadership and others. Members of the team are

identified. The team should include the facility owner, facility engineer, security supervisor, vulnerability assessment analyst, operations manager and others. The objectives and scope of the analysis effort are defined. The community screening helps select the facilities of most concern using a formalized structured process. Consideration of facilities needed to continue critical community operations are identified. A global view must be taken to cost-effectively spend the limited resources available. The process takes time and requires detailed information about the community. It requires difficult decisions.

Facility Characterization

In this step the undesired events are identified. Undesired events could include loss of lives, economic loss, loss of services or loss of mission. Assets/targets and target locations are identified. Security procedures and policies are reviewed. In many cases a number of different organizations may have identified and prioritized community critical assets. This information should be considered when identifying/prioritizing the assets. Information on facilities is also collected. This could include the purpose/mission of the facility, description of the facility, facility operations and workers at the facility (i.e. numbers, roles and responsibilities). Facility information includes floor plans, entry points and existing security features.

Determine Consequences

In this step a community-specific consequence matrix is developed which includes the consequence parameters and criteria for these parameters. It is not uncommon for there to be a considerable amount of discussion about this matrix. Guidance and approval from community leaders should be sought. When prioritizing the targets a number of criteria can be considered including: the number of people affected, loss of critical mission/function, duration of loss, replacement value, economic impact, environmental impact and loss of public confidence.

Define Threats

In this step sources of threat information are identified. These could include local, state and Federal agencies and could also include industry intelligence sharing exchanges. The threat spectrum, which will be considered during the analysis, must be defined. This would include adversary types and capabilities. The threat assessment is a judgment based on available intelligence, law enforcement, and other open source information, of the actual or potential threat to one or more facilities or programs. The Design Basis Threat (DBT) is the threat against which the facility or target will be protected (i.e. the maximum credible threat). The DBT is a management decision which helps to identify what level of threat to protect the facility. The DBT would usually cover a range of threat levels. Although in some RAMs during this step the likelihood of attack is determined it is not the most important activity in this step. The likelihood of attack is very difficult to determine and is a very qualitative and subjective effort. Factors considered for determining the likelihood of attack include the value of the asset/target, usefulness to achieving the adversary goals, publicity value, availability and ease of attacking and the adversary's perception of the possibility of success.

Determine Protection System Effectiveness

In this step the current physical protection system (PPS) for an identified facility are identified. This would include determining the protective components that contribute to

detection, delay and response. It is also important to understand the integration of these PPS components. This step evaluates the performance of the security features. In addition to PPS measures, mitigation measures are also identified and evaluated. If time permits, performance tests should be conducted. Policies and procedures are reviewed. The protection system effectiveness is then estimated. As part of the system effectiveness determination step the adversary objectives are identified, credible worst-case paths are identified, adversary scenarios for each undesired event and threat type are developed and an estimate of system effectiveness made for each scenario. The identification of the adversary objective considers protection system weaknesses, facility states, and worst consequence results. The adversary objective is generally one sentence which states who (DBT), what (critical asset) and how (intention). The worst-case scenarios for the adversary paths include those with the lowest early detection and delay after detection. Protection system effectiveness is the performance on the worst-case adversary scenario for each undesired event. Scenarios must be plausible, consistent with the defined threat and take advantage of observed weaknesses.

Risk Analysis and Reduction

Now that all of the components of risk have been determined a relative risk value is determined. The decision makers must then decide if this risk is acceptable and what impacts it may have on operations, resources etc. If it is determined that the risk is too high then measures are identified that can help mitigate the risk. This could include exploring ways to reduce the consequences but in many cases focuses on implementation of physical security or mitigation measures.

Summary

RAM-C™ is both a risk assessment and a risk management tool. A relative risk value is determined from the likelihood of attack, consequence of adversary success and system effectiveness. Then decisions makers determine if this risk is too high and if so decide ways to reduce the risk.

The RAM-C™ approach has been taught to a number of major communities in the United States as well as representatives of several States organizations. It provides a systematic, risk-based approach which provides an orderly and rigorous process. The process includes worksheets, which are used to address the steps within the process. These worksheets also serve to provide documentation and support for decisions.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL8500