

Security Risk Management and Investment Decisions

by John Piper

John Piper is Senior Security Consultant, Talisman International, LLC. He presented this paper “Five Years After 9/11: What Needs To Be Done” at a conference sponsored by FPRI’s Center on Terrorism, Counterterrorism, and Homeland Security, held December 4-5, 2006 in Philadelphia. The Center is supported by grants from the Department of Community and Economic Development and the Department of Education, Commonwealth of Pennsylvania.

The methodology used in this presentation has been used on over 350 major projects for over 12 years by a global petroleum and chemical company. It was first developed by Los Alamos National Laboratory and refined for security applications by the U.S. Department of Transportation’s Volpe Laboratories in Cambridge, Massachusetts. The key components for financial analysis (VAM) were developed by Stephen Gale and Bill Malampy (University of Pennsylvania and FPRI).

In the post-9/11 context, the methodology presented has been a key contributor to the methodologies now in use by the American Petroleum Institute and American Chemistry Council. All these models are broadly termed “Qualitative Risk Assessment through Risk Scenario Analysis.” This methodology also integrates some elements of the U.S. Department of Homeland Security (DHS) security risk assessment methodology, Risk Assessment and Management for Critical Asset Protection (RAMCAP™), which was created and developed by ASME-ITI, and is primarily focused on terrorist threats as they relate to attacks on the critical infrastructure of the United States.

The main goals of risk management are to mitigate the actions of various threats by reducing the probability of event occurrence, and/or success, and to reduce impacts of undesirable events. Generally, through a structured process, vulnerabilities are identified that postulate undesired events and their possible causes, effects and safeguards. This allows credible scenarios (credible meaning highest probability worst-case scenarios) to be developed, and separate descriptions of how each event may occur and qualitative estimates made of the consequence and probability of each scenario.

The new integrated methodology can be applied to address levels of protection in an array of areas and events, including operations, activities, information security (systems and otherwise), significant changes in threat levels and security configuration after major security incidents. Generally this process takes seven-to-ten days to complete at a major facility, such as a refinery or chemical plant, and uses a multidisciplinary team of five to eight personnel.

At the sector level and national levels (defined by RAMCAP™), the team evaluates prescribed RAMCAP scenarios. These scenarios are evaluated in terms of likelihood of success, rather than likelihood of attack, and use specific RAMCAP consequence tables to calculate risk scores. In both cases (asset and RAMCAP), countermeasures are developed followed by a risk recalculation of scenarios, assuming implementation of recommendations.

The risk mitigating recommendations are then subject to several types of financial analysis. First, they are prioritized by five different weighting elements--one of which is cost. Second, the cost-

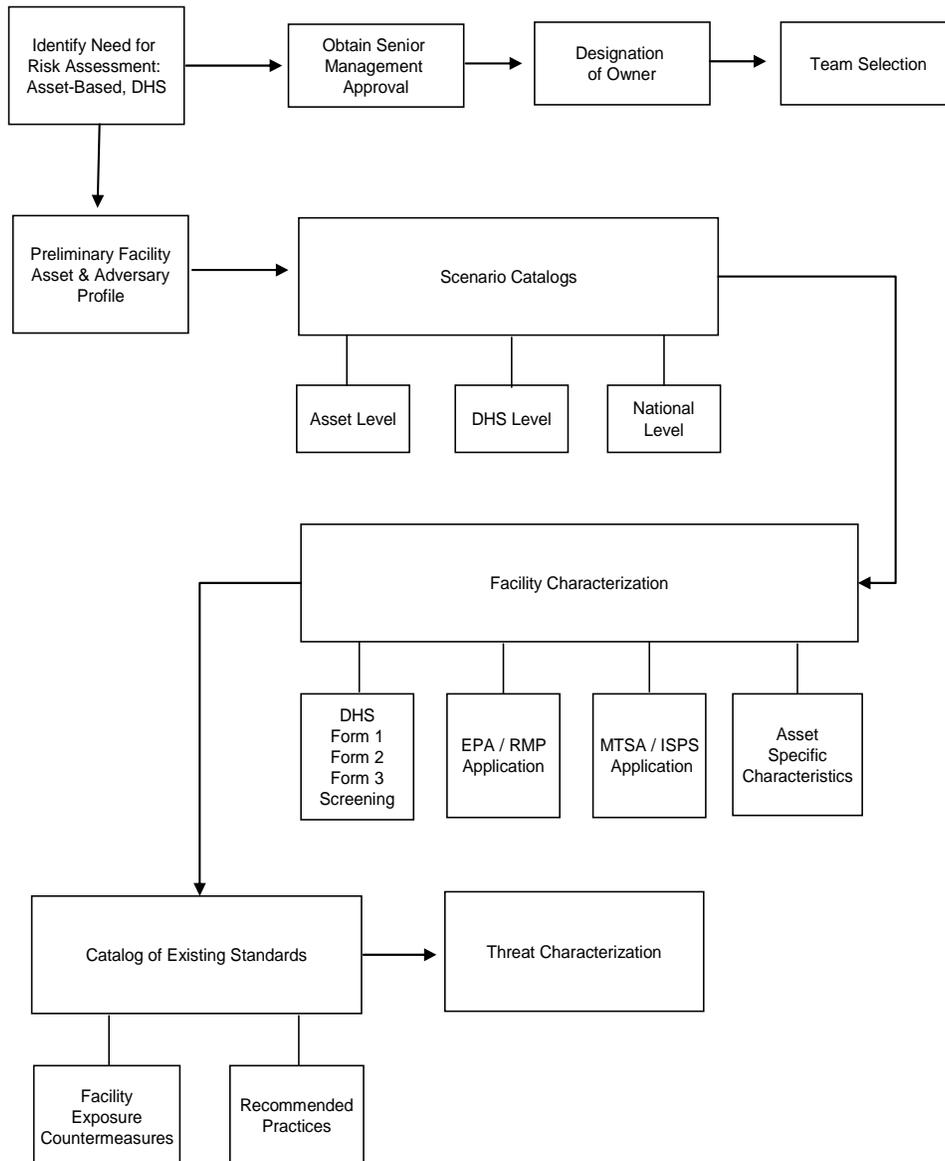
related recommendations are subjected to the VAM calculation. Third, the recommendations are analyzed and incorporated into semi-annual Risk Management Summary Reports (RMSRs), which capture trends, best practices, lessons learned, etc. The RMSRs are then incorporated into facility security baseline line requirements (roughly 100 elements—such as perimeter intrusion detection systems) which are captured on a four-tier Facility Exposure Matrix (red, black, gray, white). Facilities (over 1300 major facilities, to date) are then classified according to the matrix determinations and baselines applied. Fourth, the final set of facility security requirements are then subject to traditional cost estimating through a five gate corporate project management system.

Section 1

PHASE I: PROJECT PLANNING AND EXECUTION

Figure 1 presents the essential delivery/action steps required for project execution.

Figure 1. Project Planning Flow Chart



In accordance with safety and process risk management programs in the petroleum and chemical sectors, criteria for conducting security risk management activities should mirror the criteria in those programs. Those criteria are generally: by schedule, new project, major change in a project or program, or a major incident. The RAMCAP criteria present an additional element generally not in safety or process programs. Criteria usually involves the specific nature of the asset, for example, does it meet thresholds in terms of consequences that warrant the assessment, does it threaten national security, cause mass casualties or weaken the economy?

Management at the asset being assessed should designate a project owner. The owner should ensure that key elements of the project execution plan, such as data, drawings, layouts existing safeguards, system information, interviewees, and team composition, are satisfied. With regard to team composition, the owner should also designate the following additional roles:

- Facilitator;
- Scribe;
- Owner representatives;
- Representative of key stakeholder groups;
- Security experts; and,
- Technical experts.

Preliminary Facility, Asset, and Adversary Profile

Scenario Catalogs

The project execution plan should contain catalogs of existing scenarios from similar studies and selective RAMCAP scenarios. (This methodology, in concert with advice from Sandia National Laboratory, has selected only five RAMCAP scenarios for team deliberation--those thought to represent highest probability worst case.¹)

Table 1. DHS Sector-Level Scenarios (Modified)

Type	Weapons
Maritime (boat as weapon)	400lbs-2000 lbs of TNT equivalent
Vehicle Bourne IED	400lbs—4000lbs of TNT equivalent
Airplane	12,500 lbs-450,000 lbs
Assault 1-8 attackers	with automatic weapons, 400 lbs of TNT equivalent
Cyber attack	Insider/outsider -- sabotage, theft diversion

¹ Note: The reduction was based on discussions with risk experts at Sandia National Laboratory who believe that the smaller scenario set has a higher probability to generate more productive security improvements.

Facility (or Asset) Characterization

Facility characterization begins with a review of the facility to determine which assets have the greatest loss potential from threats. Facilities with significant impacts are subjected to further evaluation on an asset-by-asset basis (asset characterization). The results of this will be a list of candidate-critical assets that may warrant further RAMCAP consideration.

A general procedure for characterizing assets is outlined in the following sequential steps:

1. Identify Critical Assets
2. Identify Critical Functions
3. Identify Critical Infrastructures and Interdependencies
4. Identify Existing Countermeasures
5. Identify Consequences

The screening process looks at the same factors that are considered in the follow-on risk analysis (e.g., the risk scenario worksheet process in Figure 7) making it possible to develop the knowledge in the screening process, and modify it appropriately during consideration of a defined threat scenario. The first step of this process is to characterize individual assets within the facility. This includes both the determination of the hazards of the asset being compromised, as well as the specific consequences of loss. The team should consider relevant process and hazard information (such as the EPA Risk Management Plan data or applicable European SEVESO standards), as well as information about the facility. Particular consideration should be given to the hazards of fire, explosion, toxic release, radioactive exposure and environmental contamination. Further contributing to facility characterization are DHS screening forms, and marine transportation codes.

DHS Screening Forms

DHS has developed a screening process that will allow for uniform reporting of facility characteristics from multiple sectors. These are to be completed by asset security personnel in concert with site management. These should be completed even if the asset is outside the U.S. (DHS is influencing international partners to implement RAMCAP). The screening forms are presented in Table 2 and are supported by DHS detailed questionnaires.

Table 2. Screening Forms

Form 1	This form consists of basic screening information. This includes facility ownership, EPA identification numbers, location, hazardous chemicals, flammable processes and storage of chemicals of interest to adversaries
Form 2	This form is intended to screen out facilities that are deemed by DHS to be of “low” risk in terms of severe consequences and/or national security.
Form 3	For facilities that did not screen out in the Form 2 process, Form 3 captures specific information with regard to the following security-related impacts: health and human safety; economic; national security and government functionality; and, psychological. Form 3 requires specific calculations of asset replacement costs, remediation costs, business interruption costs, regional market share, military mission importance, and critical services.

Catalog of Existing Security Standards

Facility characterization should now be linked to the asset's set of existing security standards. This ensures team awareness and minimizes the chance of the team's making redundant recommendations.

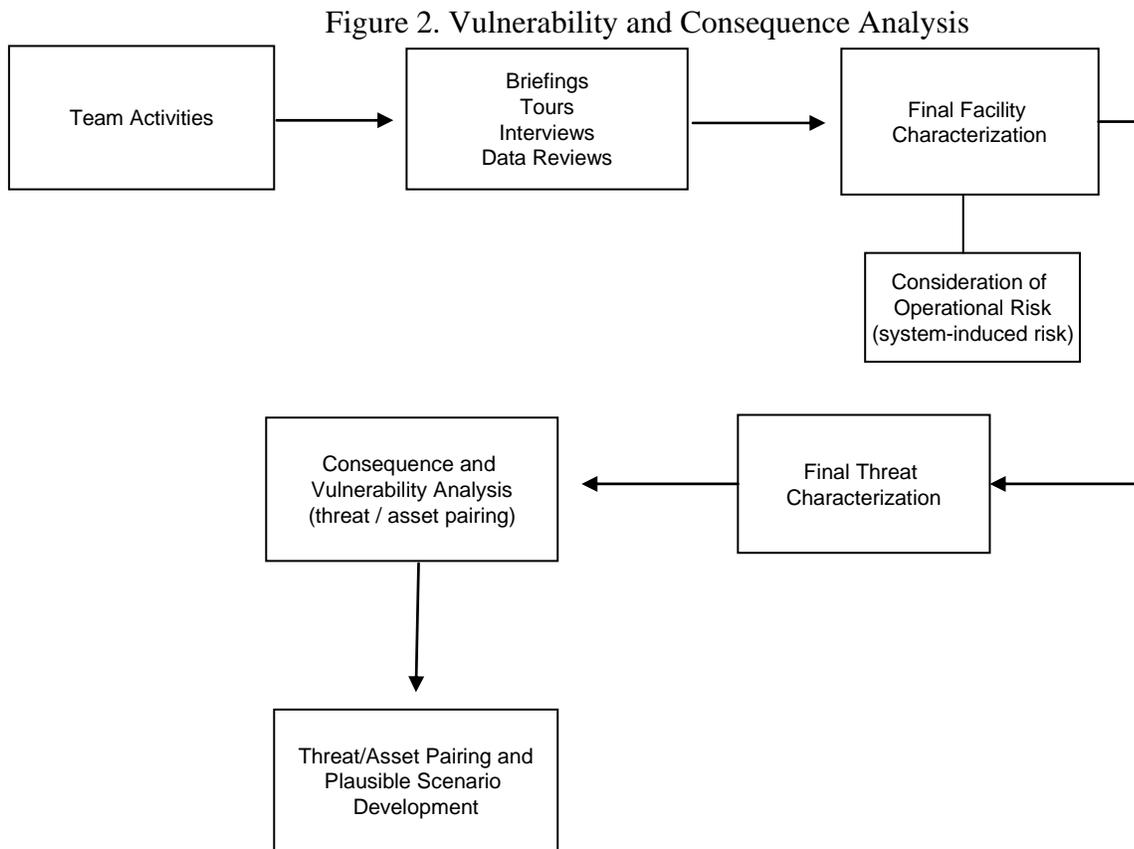
Threat Characterization

Threat is any entity that can exploit an asset. An analysis of threat information is critical to the RA process. Threats should be evaluated in terms of insider threats, outsider threats, and threats posed by collusion with insiders assisting outsiders.

Threat characterization seeks to identify specific and general means that may be used by threat agents against a given asset or facility. For most sectors this set would typically include insiders (i.e., employees/contractors), activists, contraband, fraud and corruption, labor unions with a history of violence, and terrorists. Using a scaled approach, RA teams select the threats that are appropriate for analysis and document the reasons that other levels were not done (i.e., existing stand-off distance prevents significant consequence). The resulting knowledge facilitates comparisons between the risks in a diverse set of potential targets.

Section 3
PHASE II: VULNERABILITY AND CONSEQUENCE ANALYSIS

Figure 2 captures the essential steps required for vulnerability and consequence analysis.



Team Activities

It is the joint responsibility of the sponsor's representative and team leader to assemble useful summary information and provide it to other team members before assessments. The data should be assembled and cataloged for quick reference.

Information generated from these questions flows into follow-on activities, to include:

- Site management briefing: the Team's goal is to solicit information and seek ownership;
- Facility/Process Tour: identify assets, identify hazards and hazardous processes;
- Interviews: two team members interview mid-level management in all relevant areas; and
- Document reviews: facility descriptions, plans, existing security procedures, HAZOPS reports, operations integrity reports.
-

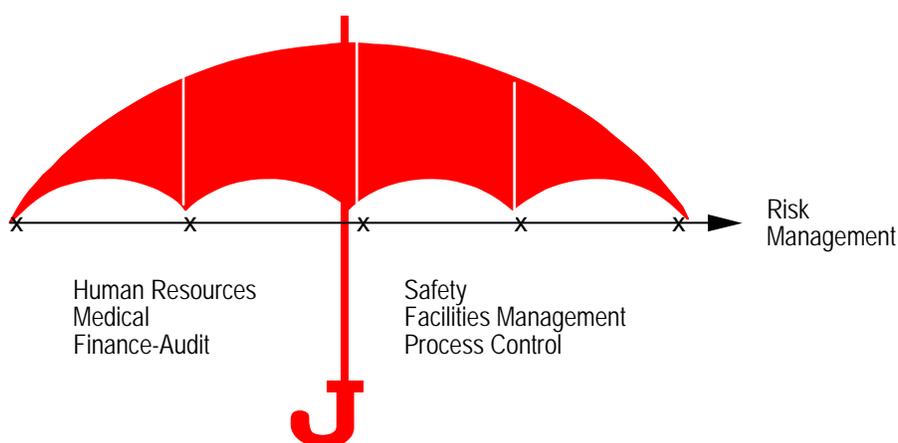
Consideration of Operational Risks (OR)

The "umbrella" in Figure 5 is from the Los Alamos National Laboratory and illustrates the OR concept. OR can also be characterized as system-induced risk. OR is an evaluation of relationships

and is a critical element of risk management. For this company, history has demonstrated that some of the most important highest-ranked recommendations have been derived from OR consideration.

The umbrella's vertical lines represent typical boundaries such as different organizations, a department within organization context, or a unit within the department context. The curved lines at the umbrella base represent the OR process, a process that examines relationships that exist between boundaries. This inter-relational concept is what distinguishes OR from traditional risk assessments.

Figure 3. Risk Management Umbrella Concept



The OR approach requires an understanding of the totality of an activity, knowledge of the activity and an imperative to cross organizational boundaries in activities which involve more than one entity (such as control centers, failure points, and computers within the refinery). Most subjects of risk assessments do involve more than one entity (e.g., a unique manufacturing capability program that involves the R&D department, personnel and procurement departments). By crossing boundaries, a risk assessment team can become aware of critical assets beyond the scope of traditional program performance reviews because those reviews tend to address a single organization or entity, and observe organizational proprieties. These "traditional" program reviews are vital and necessary. But, through a focus on critical processes and assets and discerning where they *reside* and *flow* (the "Umbrella" concept) within and between organizational boundaries, a risk assessment team can and must identify a new and important set of vulnerabilities.

In the DHS context, OR would evaluate the communication and cooperation between government agencies, between the government and private sector, law enforcement relationships with the assets, and so forth. OR should be a consideration in all team interviews, fact finding, deliberations, and scenario development. At this point, DHS risk experts have decided not to incorporate this vitally important feature into RAMCAP. With completion of OR, teams should prepare the final facility and threat characterization statements. These will serve as the basis for subsequent steps.

Consequence and Vulnerability Analysis (Threat-Asset Pairing)

Consequence analysis estimates the results of threat analysis (and scenario analysis) using common metrics. Consequences include loss of property, people, resources and capability to produce a product. For example, a scenario that leads to a release of a hazardous chemical may have outcomes

that can be measured by the amounts of chemicals released. The consequences of the release are estimated as the effects on people, the environment and the economy.

Vulnerability Analysis

Analyzing vulnerabilities is a core phase of the RA process. Vulnerability analysis identifies weaknesses that, if exploited, could result in deviation from intended operations due to loss of critical assets.

Enhanced Threat-Asset Pairing and Plausible Scenario Development

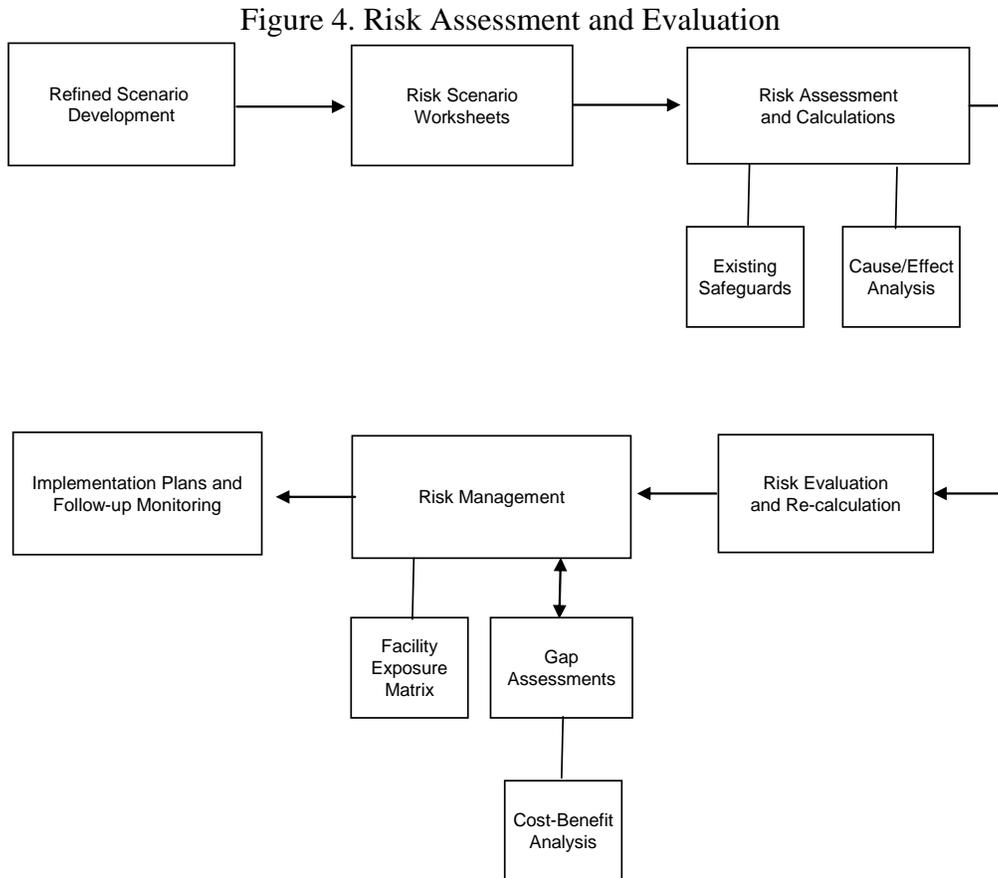
As stated previously, the consequence and vulnerability analyses require the pairing of asset and threat which leads to plausible scenario development. The asset owner should balance the rigor of analysis against severity of the consequences, complexity of the system and requirements of the decision. The team should utilize existing models developed by others to estimate damage to the facility (such as by the EPA RMP data). This can help to quickly identify the most severe outcomes for a given threat scenario which will greatly reduce the effort required to estimate vulnerability.

Section 4

PHASE III: RISK ASSESSMENT AND EVALUATION

The purpose of this phase is to describe two key processes that calculate risk: risk assessment and risk evaluation. Both processes and their results are captured in Risk Scenario Worksheets (see Figure 5). The end product is a risk index calculation, a set of countermeasures that mitigate risk, and data that influences the risk management and resource allocation network.

Figure 4 presents steps in risk assessment and evaluation, and the follow-on risk management framework.

*Refined Scenario Development*

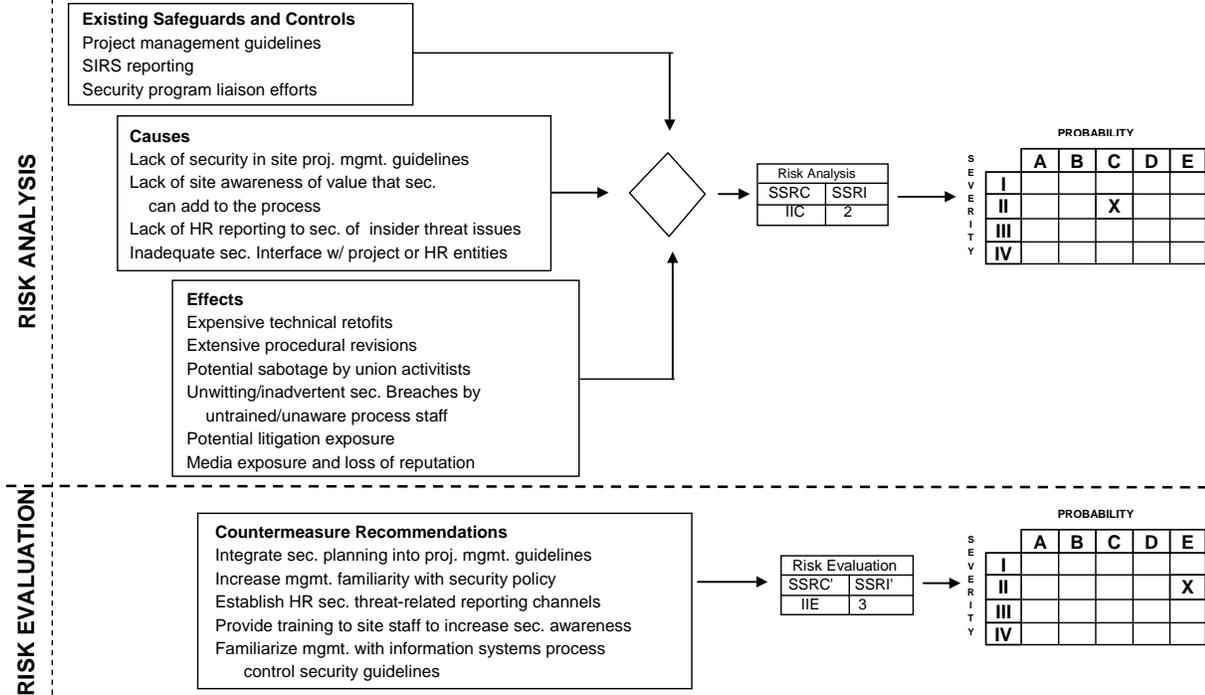
The qualitative approach uses the detailed analysis strategy and the Team brainstorms a list of scenarios to understand how the undesired event might be accomplished. Facility and threat characterization serve as a roster for detailed evaluation.

Scenarios should not focus on low-probability maximum-consequence outcomes, or high-probability low-consequence outcomes, but rather should attempt to address the most probable high-consequence outcomes.

Once plausible scenarios from the previous phase are evaluated, a refined scenario is developed; it should be challenged and crafted to represent a realistic event. Scenarios should be developed using a systematic method and clearly documented in; for example, risk scenario worksheets.

Figure 5. Risk Scenario Worksheets

Ctl. #	Scenario	SSRC	SSRI	SSRC'	SSRI'
1.10	Due to the lack of security requirements in site project management guidelines, security is not included in major projects at early project gates causing increased exposure to changing threats and expensive technical and procedural retrofits.	II.C	2	III.E	3



Cause/Effect Analysis: Severity and Probability

To establish an understanding of risk, scenarios must be assessed in terms of the severity of consequences and the probability of occurrence. While these are subjective calculations, they are based on available quantitative data and on the judgment of knowledgeable multidisciplinary team members.

The risk matrix is the basis for a qualitative approach to risk determination. The risk matrix is a graphical portrayal of risk as the product of probability and consequence. The Risk Assessment Matrix serves the following purposes. First, it lists four levels of risk and recommends specific management actions. Secondly, it calculates the Safeguards and Security Risk Category (SSRC) in a weighted fashion. And, thirdly it indicates the Safeguards and Security Risk Index (SSRI).

The relative index of associated risk or consequence is based on the probability that undesired events may occur. Table 3 identifies how to classify scenario outcomes based upon their severity.

Table 3. Severity of Scenario Outcomes

Severity	Characteristics
<p style="text-align: center;">I Critical</p>	<p>Fatality (Loss of life) Loss of restricted proprietary information with critical consequences to Company Loss of essential assets Significant impairment of mission Loss of system Evacuation of > 1,000 individuals Extended negative world-wide news coverage Loss of more than \$10M USD</p>
<p style="text-align: center;">II Serious</p>	<p>Nonfatal Lost Time Incident or Injury requiring hospitalization (severe injury, in-patient care needed, did not return to work) Loss of proprietary information with serious consequences to company Serious loss of physical equipment Unacceptable mission delays Evacuation of 25 to 999 individuals Extended negative national news coverage or one international mention Unacceptable system and operations disruption Loss of \$1M to \$10M USD</p>
<p style="text-align: center;">III Moderate</p>	<p>Medical Treatment Incident (MTI) other than First Aid - non lost workday (out patient, but returned to work) Undetected or delay in the detection of unauthorized entry resulting in moderate loss of assets or sensitive materials Moderate mission impairment Less than 25 individuals evacuated One time negative mention on national news or extended local news coverage Moderate system and operations disruption Loss of \$100K-\$1M USD</p>
<p style="text-align: center;">IV Minor</p>	<p>First aid (treated on site and immediately returned to duty) Undetected delay in the detection of unauthorized entry No evacuation Minor public disruption One time mention on the local news Minor systems or operations disruption Loss of \$10-100k</p>

Table 4 presents an estimate of the probability of occurrence of the selected events or factors. These estimates are subjective. The estimates require that both the vulnerability *and* the inability or failure to control the vulnerability must occur for the undesired event to result.

Risk assessment teams must agree on two numbers in order to assess probability. They must agree on the assessment time duration of the study (such as the years 1997 to 2010), and what the language representation in Table 8 means in numerical terms (such as "frequent" means the undesired event will occur once in annual operations for the time duration of the study).

Table 4. Event Probability

Probability Category	Level	Specific Event
A	Frequent	Possibility of repeated incidents (> 1 event per year)
B	Probable	Possibility of isolated incidents (1 event in 5 years)
C	Occasional	Possibility of occurring sometime (1 event in 10 years)
D	Remote	Not likely to occur (10% chance of occurrence in 10 years)
E	Improbable	Practically impossible (1% chance of occurrence in 10 years)

Probability and severity calculations are then plotted on the risk matrix in Table 5 to estimate risk. Level of risk is categorized by the shaded areas of high (risk index of one), medium (risk index of two), moderate (risk index of three), and low (risk index of four). Higher risk scenarios are considered to have the highest priority for consideration of risk reduction actions. Medium and moderate risk scenarios require further analysis of enhancement options. Low risk scenarios are subject to the normal security review.

Table 5. Risk Matrix

Severity Categories	Probability of Occurrence				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	IA	IB	IC	ID	IE
II	IIA	IIB	IIC	IID	IIIE
III	IIIA	IIIB	IIIC	IIID	IIIE
IV	IIVA	IIVB	IIVC	IIVD	IIVE

Risk Category (RC)	Risk Index		RI Number (RI)
IA, IB, IC, IIA, IIB, IIIA		Implement countermeasures that reduce risk to an SSRI of a level 2, or seek senior management approval to accept risk	1
ID, IIC, IID, IIIB, IIIC		Not acceptable without management re-evaluation	2
IE, IIE, IIID, IIIE, IIVA, IIVB		Acceptable with review by management	3
IIVC, IIVD, IIVE		Acceptable without review	4

The Risk Matrix has broad applicability for qualitative risk determination. It is adaptable to varying levels of information and depths of evaluation. It may be used to identify areas for further evaluation, as part of a screening effort or to summarize detailed systematic studies. It has a built-in presentation format that lends itself to review.

DHS Severity Tables

Teams should consider the DHS screening forms and severity tables. These capture replacement costs, remediation costs, and business interruption costs. When coupled with the VAM and the project management system (to be discussed later), these can be variables in the financial consideration of risk.

Risk Evaluation

In this phase, teams identify corrective actions to address the causes and/or mitigate the effects of identified vulnerabilities. They should select appropriate countermeasures based on the following criteria:

1. Does it reduce the likelihood of adversary success?
2. Does it reduce the probability of occurrence?
3. Does it reduce the severity of consequence?

Teams should recommend the most appropriate cost-effective countermeasures that address the causes and effects of identified vulnerabilities. Recommendations that are interdependent must reference the other recommendation(s) that relate to the interdependence.

Using the risk matrix, teams should then recalculate risks and the likelihood of adversarial success based on the effect of all recommendations for the scenario, assuming that the recommended countermeasures are implemented.

The team should then conduct a ranking process for the scenarios and the recommendations. This algorithm (based on scores of one-to-ten), developed by Gale/Malumpy, starts with a ranking each recommendation within the scenario to which it applies. Then the level of *difficulty* to implement each recommendation is ranked. The difficulty ranking also includes cost consideration. To assist in this, the company uses the VAM referenced earlier. This tool calculates the return on security investments over time—it is vital to the screening process and feeds into the facility exposure matrix to be discussed later. The team should rank the scenarios that comprise the risk assessment in terms of importance to the overall risk assessment, and rate the *importance* of each recommendation in terms of the overall risk assessment, independent of the specific scenario to which it applies. Lastly, teams should average the weight to prioritize—using the Gale algorithm--all recommendations based on all of the rating and ranking factors, and then order recommendations in terms of priority.

Reporting and Implementation Plan

At the conclusion of the risk assessment, it is important to brief management on the observations and recommendations to solicit their immediate feedback and understanding of those recommendations and key observations. The briefing should include a discussion of the effectiveness of the current safeguards and security program and provide an overview of the risk assessment, recapping the major recommendations.

With management endorsement of the recommendations, an implementation plan should be produced to reflect recommendation, owner, timeline for implementation, and any changes to the original recommendation. These plans should be centrally monitored and reviewed according to a proscribed schedule. Risk management coordinators should also work with owners to ensure that implemented countermeasures have not created new, unforeseen, vulnerabilities.

Risk Management Summary Reports and the Facility Exposure Matrix

This global petroleum and chemical company prepares semi-annual Risk Management Summary Reports which capture results from 40~ risk assessments conducted annually.

These tend to be a quantitative analysis of the qualitative project output. For example, they evaluate common recommendations from different projects. These trends are then used to develop security countermeasure baselines for corporate assets—more-or-less the set of security requirements or a catalog of existing standards.

The Facility Exposure Matrix (see Table 6) is the tool² used to capture the catalog of existing standards. This company has classified over 1300 major facilities using this tool. These standards are subject to general corporate cost-benefit analysis and are also subject—at the project implementation level—to intense cost scrutiny through the corporate gate review process. So, in addition to the VAM model and the Gale ranking calculations tools, corporate tools are applied to round out the cost-benefit equation.

Table 6. Facility Exposure Matrix

FACILITY EXPOSURE Color-coded Matrix

		4 Critical Threat	3 High Threat	2 Mod Threat	1 Low Threat		
4 Critical Value	16	12	8	4	4 Critical Value		
	12	9	6	3			
	8	6	4	2			
	4	3	2	1			
		4 Critical Threat	3 High Threat	2 Mod Threat	1 Low Threat		

“**Threat**” is defined as any entity, circumstance, or event with the potential to exploit, cause the loss of or damage to an asset or operations as estimated using the “country / Regional Threat Level Consideration Matrix”

“**Value**” is defined as relative worth, utility, or importance and includes people, dollar loss, environment, operational criticality, throughput, business continuity, government relations, location, executive functionality, and Company reputation

Each matrix level has a specific set of technologies and procedures. RA teams should re-evaluate the facility designations and technical and procedural measures in light of the facility characterization and, later in the process, the risk assessment recommendations.

² Note: It is recognized that many other modes capture existing security standards.

There should be a comparison between risk assessment recommendations and existing standards. RA recommendations comparison should be documented in the form of a separate gap assessment in the RA report. This step is critical because it moves the project from a risk assessment into the area of long-term risk management.