Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis

John W. Piper
14526 Lightner Rd.
Haymarket, Virginia 20169
UNITED STATES OF AMERICA
john.w.piper@gmail.com

ABSTRACT

Risk Management is the technical procedure for identifying, characterizing, quantifying and evaluating system weakness and balancing the risk of loss or consequence countermeasures. It is widely used to select a mix that mitigates threats provides adequate protection and threat reduction. Similarly, conflict analysis and resolution (CAR) identifies sources of conflict and suggests tools for resolving conflict. This paper will seek to identify the correspondancies between structured risk management applications and program objectives.

Risk Management strategies have been widely adopted as a mechanism for assessing conditions and allocating resources to maximize attainment of goals and objectives and can serve as an enduring framework underlying the basis for decision-making. Risk Management and Risk Assessment are key components of operations integrity management systems across a wide array of sectors.

This document addresses the risk management framework. The process is technical and deliberate. As such, risk management efforts evolve into an objective system to classify risk that can be statistically valid and reliable. This document further constructs a framework for Risk Management planning, assignment of roles and responsibilities, team development/training, monitoring and follow-up tracking.

1.0 SAFEGUARDS AND SECURITY QUALITATIVE RISK ASSESSMENT (SSQRA)

1.1 Introduction

Risk Management is the technical procedure for identifying, characterizing, quantifying and evaluating system weakness and balancing the risk of loss or damage of disclosure against the cost of countermeasures. It is widely used to select a mix that provides adequate security and safeguards protection without excessive cost in dollars or in ready access to assets and information for authorized users.

Risk Management strategies have been widely adopted as a mechanism for assessing conditions and allocating resources to maximize attainment of goals and objectives and can serve as an enduring framework underlying the basis for security decision making. Risk Management and Risk Assessment are key components of operations integrity management systems (OIMS).

This document addresses the risk management framework. The process is technical and deliberate. As such, risk management efforts evolve into an objective system to classify risk that can be statistically valid and reliable. This document further constructs a framework for Risk Management planning, assignment of roles and responsibilities, team development/training, monitoring and follow-up tracking.

Qualitative Risk Assessment **-** Risk Assessment is the key component of Risk Management programs. The Qualitative Risk Assessment methodology is the approach that has been adopted by leading engineering organizations and possibly by NATO Noteworthy Assets (NN). The methodology can be applied at project stages from conceptual through detailed design, post-construction and operations, and can be adapted to varying levels of available information and depths of evaluation. This model has been approved by US DHS and—for cyber security risk assessments—by US Department of Energy.

In the methodology, a team of 5 to 8 with expertise in engineering, operations, and risk assessment techniques uses its knowledge and experience along with appropriate vulnerability identification methods, to identify potential vulnerabilities associated with the system of interest. The team then uses a structured brain-storming approach to identify credible unplanned event sequences or scenarios that could result in the threats exploiting vulnerabilities. The team then analyzes each scenario to identify potential causes, consequences, and assumed or existing safeguards. Each scenario is assigned a qualitative risk rating based on the team's judgment of its severity and likelihood of occurrence or probability.

Risk Assessment Process **-** The process can be viewed as a multi-step procedure:

1. *Asset valuation and judgment about consequences of loss*. This step determines what is to be protected and appraise its value. Value can be tangible (e.g. dollars) or intangible (e.g. reputation). Part of asset valuation is understanding that assets may have a value to an adversary that is different from their value to us.
2. *Identification and characterization of the threats to specific assets*. Intelligence assessments must address threats to the asset in as much detail as possible, based on the needs of the customer. These assessments may be commissioned to feed the development of security policies and standards, to guide systems design, or to plan security support for operations.
3. *Identification and characterization of the vulnerability of specific assets*. Vulnerability assessments help us identify weaknesses in the asset that could be exploited by threats. This threat-asset pairing enables preliminary design or operational changes to reduce risk levels by altering the nature of the asset itself. Preliminary cost estimating is an important factor in these decisions, as design changes can be expensive and can impact other mission areas.
4. *Risk assessment*. Asset valuation, threat analysis, and vulnerability assessments are considered, along with the acceptable level of risk and any uncertainties, to decide how great the risk is and what countermeasures to apply.
5. *Identification of countermeasures, costs, and tradeoffs.* There may be a number of different countermeasures available to protect an asset, each with varying costs and effectiveness. In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

This process is depicted in the following Figure:

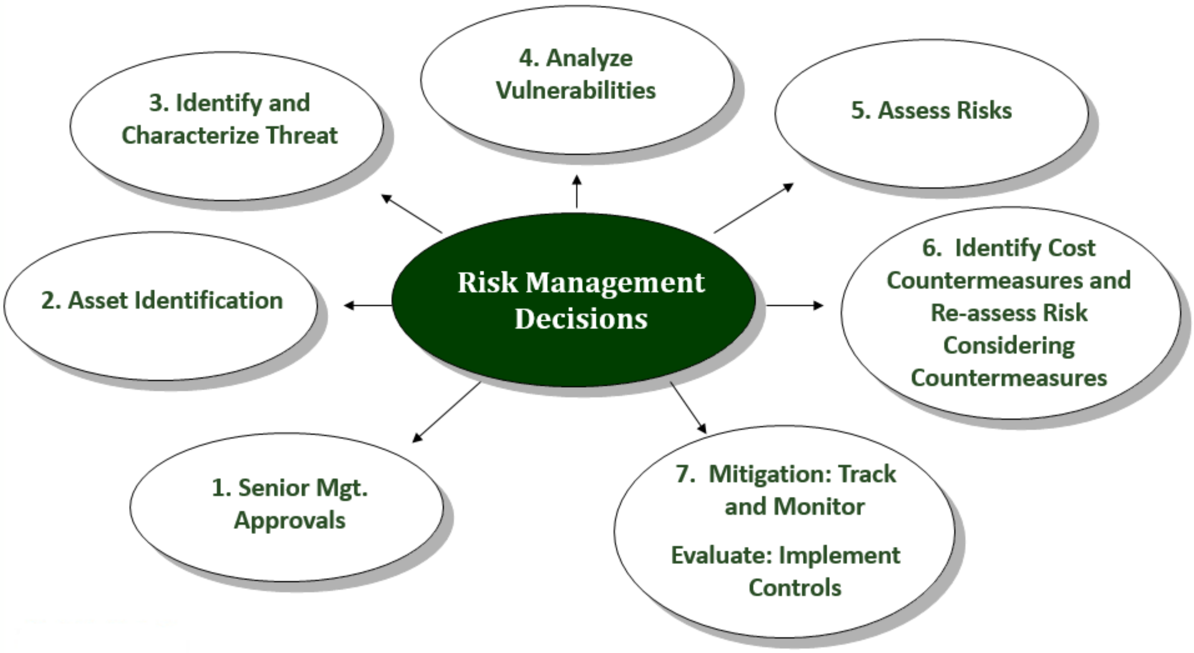

4. Analyze Vulnerabilities
3. Identify and Characterize Threat
5. Assess Risks
2. Asset Identification
Risk Management Decisions
6. Identify Cost Countermeasures and Re-assess Risk Considering Countermeasures
1. Senior Mgt. Approvals
7. Mitigation: Track and Monitor
Evaluate: Implement Controls

Figure 1: The Risk Management process

When any of these steps are left out, the result can either be inadequate protection or unnecessary and overly expensive protection. Frequently, the missing element is incorporation of specific, up-to-date threat assessments in development of security policies. With no documented threat information, countermeasures are often based on worst case scenarios.

In addition to these core steps, there are two additional steps that add value to the process. The first, which should occur prior to asset evaluation, is *senior management approval* for the conduct and scope of the assessment. This will ensure cooperation at the management levels and enhance the quality of information received by assessment teams. The second (and last step) is an evaluation, at a prescribed time interval, of the effectiveness of implemented controls and a review of those controls to insure they have not created new, unforeseen, vulnerabilities

It must be stressed that managers must make trade-offs during the decision phase between cost and risk, balancing the cost in dollars and manpower against possible asset compromise or loss. Policy decisions resulting from this process can then guide security planning. These decisions should form the backbone of, and provide the standards for, the safeguards and security system. The resulting standards promote consistency, coherence, and reciprocity across programs.

The "umbrella" in Figure 2 is a further illustration of the safeguards and security risk management concept. The vertical lines represent typical organization domain boundaries (such as a department within organization context, or a unit within the department context). The curved lines at the umbrella base represent the risk management/assessment process – a process that examines relationships that exist *between domains*. This interrelational concept is what separates risk management from traditional inspection or audit programs (which tend to examine programs vertically for "efficiency" rather than horizontally for "effectiveness").

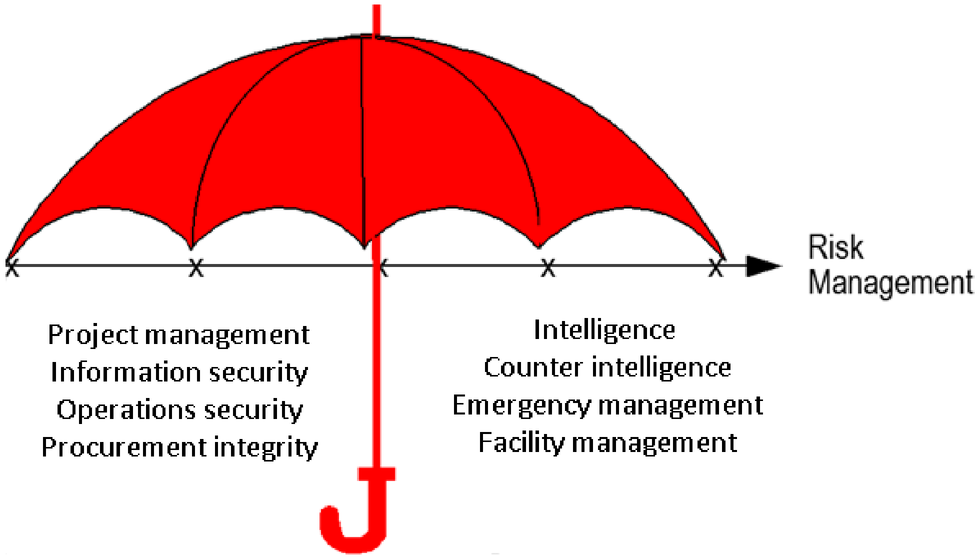
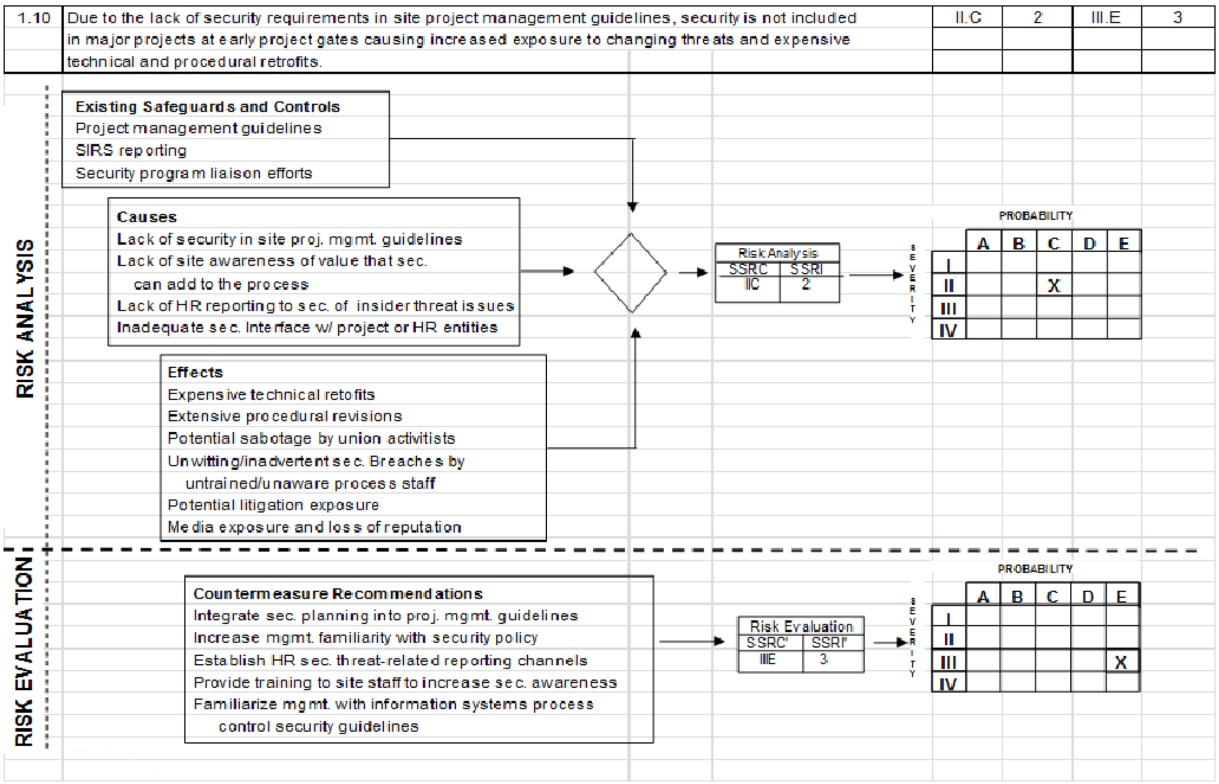


Figure 2: Risk Management Umbrella Concept

Risks are assessed and evaluated using developed Safeguards and Security Qualitative Risk Assessment (SSQRA) tools and the SSQRA Risk Scenario Worksheet (Figure 3).



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

Existing Safeguards and Controls
Project management guidelines
SIRS reporting
Security program liaison efforts

Causes
Lack of security in site proj. mgmt. guidelines
Lack of site awareness of value that sec. can add to the process
Lack of HR reporting to sec. of insider threat issues
Inadequate sec. Interface w/ project or HR entities

Effects
Expensive technical retofits
Extensive procedural revisions
Potential sabotage by union activitists
Unwitting/inadvertent sec. Breaches by untrained/unaware process staff
Potential litigation exposure
Media exposure and loss of reputation

Risk Analysis	
SSRC	SSRI
IIC	2

PROBABILITY

SEVERITY	A	B	C	D	E
I					
II			X		
III					
IV					

Countermeasure Recommendations
Integrate sec. planning into proj. mgmt. guidelines
Increase mgmt. familiarity with security policy
Establish HR sec. threat-related reporting channels
Provide training to site staff to increase sec. awareness
Familiarize mgmt. with information systems process control security guidelines

Risk Evaluation	
SSRC'	SSRI'
IIIE	3

PROBABILITY

SEVERITY	A	B	C	D	E
I					
II					
III					X
IV					

Figure 3: Risk scenario Worksheet

Definitions **-** To better understand QRA, the following definitions are presented:

- ***Risk*** is the potential of loss to an organization or entity;
- ***Risk Managemen*t** is analysis of an organization's existing resources and its vulnerabilities – it determines loss potential for each resource or combination of resources to establish potential loss levels. Both tangible (dollar losses, or to an undetected intrusion) and intangible (loss of sensitive information, damage to reputation) resources must be considered;
- ***Threat*** is an entity – individuals, programs, policies, hazards and events, which is capable of exploiting a vulnerability;
- ***Security –*** procedures and engineered features that mitigate the consequences of assumed off normal operations or undesired events.
- ***Vulnerability*** is a condition that may be exploited by a threat thus causing deviation from intended outcomes or requirements resulting in negative impact on assets; and,
- ***Countermeasure*** is an entity which reduces risk by decreasing harmful effects and/or their frequency of occurrence.
- ***Risk Management Coordinator(s)*** are security staff at NN or Regional Centers functionally responsible security risk management.
- ***Owner*** is a manager in whose operation the QRA was conducted and has responsibility for the follow-on and close out process.
- ***Assignee*** is a person the owner assigns to implement specific follow-on items.

To summarize, the risk assessment process provides a mechanism that:

- Addresses cost-risk benefit
- Emphasizes back-up systems and in-depth protection
- Determines appropriate levels of protection for assets
- Reviews potential threats to security interests
- Promotes decisions that accept certain levels of risk
- Promotes action to reduce risks that are not acceptable
- Provides a means to judge whether the resultant risks meet acceptability criteria.

1.2 Management of Risk

This report describes the Qualitative Risk Assessment methodology. That methodology consists of distinct phases, including; a qualitative risk assessment phase of threat or vulnerability identification, characterization and ranking; and a risk evaluation phase entailing risk mitigation and re-estimation of the occurrence probabilities and the consequences of weaknesses or hazardous events, including catastrophic ones. Following the capture of risk, appropriate risk management options can be devised and considered. Risk-benefit or cost-benefit analysis may be undertaken and risk management (or countermeasure) policies and/or procedures may be formulated and implemented. The main goals of risk management are to prevent actions of threat agents by reducing the probability of their occurrence (e.g., practice "surprise" avoidance), to reduce impacts of undesirable events (e.g., prepare and adopt emergency responses) and to transfer risk (e.g., via insurance coverage). As noted in the introduction, the conduct of risk assessments is a key component of Risk Management programs.

Qualitative Risk Assessment (QRA) - QRA is a structured brain-storming technique in which a team uses its knowledge and experience to identify potential vulnerabilities and qualitatively assess the risks associated with those vulnerabilities. Vulnerabilities are identified using one or more methodologies such as brainstorming, and a What-if/Checklist.

Risk Scenario Analysis (RSA) refers to the process of converting identified vulnerabilities into risk scenarios, and the systematic analysis of these scenarios to determine the risk level they represent. It is intended to supplement and extend vulnerability evaluation by explicitly considering the two components of risk, consequence and probability. In risk scenario analysis, identified vulnerabilities are used to postulate undesired events and their possible causes, consequences and safeguards; credible scenarios are developed to describe how each event may occur; and qualitative estimates are made of the consequence and probability of each scenario.

Uses - Because of flexibility in approach, especially in choice of vulnerability identification tools (such as questionnaires, surveys, interviews) and subsystem analysis (such as H/R, Medical, Process Control), QRA using RSA can be applied to almost any activity involving risk (an entire facility, a division/department within a facility, or an operation). It is useful over a broad range of projects and work scopes, from early stages of a project (pre-conceptual design), through life cycle gates. The basic approach is further applicable to risks associated with use of technology in operations.

Benefits - Like some traditional vulnerability evaluation methods, benefits of QRA center on the team concept. By security elements involving personnel responsible for both engineering and operations of a facility under study, both groups gain a better understanding of the facility and its vulnerabilities. The experience base of the team brings historical operational perspective to the process.

Limitations - A potential limitation of QRA is that it may not capture the total risk picture for a given operation. Furthermore, its success depends heavily on the knowledge, experience and creativity of the team. The nature of the process and risk rating system make direct comparisons between studies difficult. Apparent risk differences between different operations may be greater or less than indicated in the results of separate studies conducted by different teams. These differences are primarily in the risk ratings, which are only one part of the risk assessment results. Differences in follow-up considerations depend on team make-up, the quality of available information, and depth of analysis. Also, as the system under study becomes more complex, it may be necessary to supplement QRA with other tools such as software-based quantitative methods.

Keys to Success - The limitations of QRA are reduced by:

- Careful planning and team selection (including the security element selection of both engineering and operations personnel);

- Providing all relevant information to the team prior to and during the QRA, by using a systematic approach to vulnerability (scenario) identification; and,

- Choosing the depth of analysis appropriate to the magnitude of vulnerabilities and degree of system definition. Further benefit is gained by encouraging open discussion during team meetings, and by prompt reporting of results.

1.2.1 Document Organization

The remainder of this document describes in more detail QRA. Chapter 1.3 describes QRA planning, assignment of roles and responsibilities, team development and training.

Chapter 0 describes QRA steps, to include:

1. Management approval, planning and preparation;
2. Identification of critical assets;
3. Analysis of threat agents;
4. Analysis of vulnerabilities;
5. Assessment of risks;
6. Application of appropriate countermeasures;
7. Monitoring and Follow-up Tracking; and,
8. Effectiveness reviews of implemented countermeasures.

1.3 Risk management Planning, Roles and Responsibilities, Team Composition and training

Project Risk Assessment Planning – QRA should be planned and scheduled "regularly" for ongoing operations and activities, being triggered by perceived changes in risk and at key milestones on major projects. Risk managers AND/OR organizational security managers should define the frequency of each ongoing operation or activity and communicate such timing to management who, in turn, must make plans as to the timing and availability of resources. Risk managers should also develop an overall QRA plan for review by organizational management.

Requirements for QRA - A QRA should be required in these instances:

As required by schedule,

Prior to any **significant** change in a facility or operation,

After a serious security incident, and

Whenever new scenarios – not originally identified by risk assessment teams – are identified during the overall risk management process and that require a response under the stewardship management programs.

It should be recognized that other elements might require risk assessments in accordance with legal requirements, insurance considerations, and integrity-critical processes. Managers should monitor these activities and be cognizant of identified risks that may have an impact on security planning.

Risk Identification and Reporting during Routine Activities - Information that may identify new risks or change existing evaluations from outside the structured risk assessment process should be captured and entered into a type of Risk Management Summary Report (RMSR). The new risk may come from another evaluation (e.g., safety hazards assessments) or from another inside or outside source. Line management is responsible for reporting such risks in the RMSR and for notifying SSQRA owners and/or other risk managers. An abbreviated report (the RMSR “short form”) or a memorandum should be used to document, evaluate, and transmit this new information. However, line management, consulting with security elements, must carefully screen the information before incorporating the new risk data into the RMSR.

If incorporating the data is warranted, an abbreviated RMSR Short Form should be completed to facilitate entry of the pertinent information into a type of Risk Registry Database. If the new risk has an impact on any existing scenarios, the scenario reference should be identified, but if the scenario is totally new, the Risk management Coordinators (RMCs) should document the new element.

Use of the RMSR Short Form requires a decision as to whether the new risk requires a team risk assessment. If the new risk is categorized as Risk Index 1 or 2, it is considered significant and may warrant team attention. If not, completion of the Short Form should be sufficient. The RMCs should then log the new information into the Risk Registry Database. Corrective action and close out of the new risk will usually be the responsibility of the reporting line manager and/or the owner.

Changes **-** Organizational procedures (such as other asset integrity systems) specifically address change management. In accordance with published change management procedures, modifications in operations may require a recycle of previous QRAs or an entirely new assessment when a change results in a situation that has not been addressed by earlier assessments. The change procedure should document risk aspects of change. If change is considered significant, constitution of a formal RA Team may be required. Examples of “significant change” include: major modifications; new standards, regulatory mandates, laws; political/community changes; and new technology. A revision process should be also initiated when new information alters planned follow-up activities. The process for revising the original assessment and the owner's follow-up plan should:

- Charter, in concert with line management and the owner, a new QRA (no fewer than two Level 2 or Level 3 practitioners) to verify changes to the original risk index,

- Verify risk index ratings with the original team leader(s),

- Develop a response plan that notifies appropriate management,

- Incorporate the response into the follow-up and tracking process that clearly identify revisions to original recommendation(s), and

- Provide copies of the plan to the RMCs.

If the risk aspect of change is not significant, a single Level 2 or Level 3 practitioner should be able to conduct a Limited Scope QRA, and complete a Short Form to document impact due to change on the risk scenarios of previous assessment(s). The form should be distributed to the owner of the original QRA and to RMCs for tracking purposes.

Transition Management **-** An important element of a comprehensive RMSR is transition of risk findings from one operational or activity phase to another. This transaction ensures that responsible individuals continue to be assigned to follow-up and close-out risk mitigation activities, throughout the entire life cycle of the project. The owner should prepare a memorandum documenting or referring to all necessary follow-up and close-out activities and forward to the new owner, assignee, security management and the RMCs.

Special Risk Studies **-** The scope of each QRA must be identified, and any previous QRAs and other similar evaluations should be reviewed prior to beginning a new QRA. However, the base plan developed by risk managers may account for special risk studies that have been or will be conducted. Special risk studies are generally aimed at developing an understanding of findings from other risk assessments. Their goal should be to provide a better understanding of exposure from the assessment findings. Methods used in special risk studies should be coordinated with the risk managers and tailored to fit the specific objectives being examined (e.g. personnel suitability investigations).

1.3.1 Planning Elements

The basic steps in organizing a QRA include:

- Identifying an owner and a qualified Team Leader,
- Identifying other multi-disciplined participants,
- Developing a detailed schedule (duration), including requirements of support facilities,
- Identifying data and individuals who must be interviewed,
- Defining deliverables,
- Providing an adequate budget,
- Agreeing on scope (NN program security) and assumptions (such as threat levels),
- Agreeing on report review procedures, and
- Agreeing that the owner develops the follow-up plan.

***Roles and Responsibilities* –** As part of the process, the team members work together to determine the risk index for each of the scenarios developed (see Section 0 for methodology). Developing this index is an independent process and intervention from the QRA owner should not occur at this stage. To further ensure accuracy of their findings, the team should conduct an "error of fact" review with the owner at the conclusion of the assessment (this may be an element of the exit briefing). The team should explain what led to risk calculations as they will appear in the DRAFT report.

***Owners* -** Owners should be responsible for post QRA follow-up actions. In this context, the owner is defined as a manager in whose operation the risk assessment is being conducted and has overall responsibility for the follow-up and close-out process including:

Evaluating possible mitigative alternatives and related impact(s) upon risk levels,

Assist in FINAL Draft preparation (after which, modifications should be limited)

Assigning corrective action responsibilities (to assignees), and

Communicating results to affected personnel.

The owner is responsible for communicating risk levels associated with operations and activities to management. The owner documents risk to management by preparing and submitting the Risk Management Summary Report (RMSR). Management approval of the RMSR acknowledges the existence of the risks and the related mitigation countermeasures.

***Assignee* -** An “assignee” is a person whom the owner appoints to implement specific follow-up actions. The owner should identify assignees and their responsibilities in the RMSR documentation. The owner must clearly communicate information and expectations relating to follow-up actions. Organization-wide responsibility for risk management falls to a single Risk Management Coordinators (RMCs). Owners are responsible for providing the RMCs with follow-up documentation, including identification of assignees and their respective responsibilities.

1.3.2 QRA Team Composition and Training

QRA quality depends on team composition, experience, and qualifications. One RMC objective is to provide guidance to owners in assembling high quality teams. Generally, security staff should represent no more than one third of a team and those security team members, most importantly the Team Leader, should be from outside the element being assessed. Other suggested team members include: safety; process control; logistics; intelligence; facility operations; audit (so long as the assessment is NOT perceived as being audit oriented); human resources; or other risk assessment experts (such as safety and process risk analysts). Members should come from mid-level management with the goal having cognizance of senior management strategic and tactical planning and day-to-day operations. Use of knowledgeable, non-organizational third parties as members (such as consultants or senior university staff), is strongly encouraged.

***Capabilities, Classifications and Requirements* -** Classification of team members is helpful in developing a balanced team with sufficient depth of knowledge and breadth of experience to ensure a high quality risk assessment. Level 1 corresponds to the basic training required for general support staff, Level 2 encompasses the capabilities needed by senior team members, and Level 3 is required of Team Leaders.

- **Level 1** includes, at a minimum, all functional support staff involved with security and safeguards risks or operations/project functions on a day-to-day basis. Personnel functional responsibilities should include identifying, reporting, and managing risk as a key component of every employee's job.
- **Level 2** includes highly experienced personnel who are directly involved in technology, operations, and project execution. These personnel should participate, but not necessarily lead risk assessments during their normal duties. This level should include security managers involved in making risk management decisions.
- **Level 3** includes selected personnel who lead risk assessments and make risk assessment and related management decisions on a routine basis.

In general, individual and group composite experience should be tailored to the scope and technical sophistication of the QRA. A team must be comprised of at least five core members, preferably with senior-level qualifications:

- **Level 3 Team Leader,** responsible for managing activities, completing the QRA study, and complying with all aspects of reporting requirements of the risk management system.
- **Level 2 Assistant Team Leader,** responsible for capturing and documenting all assessment activities, findings, and recommendations in the proscribed format. This person may serve as the Scribe or guide the activities of a third-party Scribe. This position may be a training position leading to Level 3 qualification.
- **Level 2 Representatives,** should either be security personnel with sufficient experience and authority such that they are qualified to manage security operations at the facilities being assessed. Or operations/project personnel with sufficient experience, expertise, and knowledge to accurately describe, articulate, and clarify the purpose, function, and the structure of the facilities or organizations being assessed.

All team members (including third parties) should be approved by the owner and documented in the QRA Execution Plan. In those cases when team qualifications cannot ensure the conduct of a high-quality assessment, the owner should consult with management to enhance team capabilities or restrict scope/technical depth.

To identify potential team members, the RMCs maintain a database of staff training and experience. The RMCs should approve all candidates for Level 2/3 designation. Nominations should emphasize relevant *substantive* experience in previous assessments. Security management should ensure that appropriate numbers of security personnel with the requisite depth and mix of skill levels are maintained within their group or available through third-party sources.

***Training Team Members* -** Training should maintain capabilities of team members and qualify potential candidates. Training should include:

- **Level 1** – QRA orientation briefing that: gives examples of security risks and related mitigation measures; discusses risk identification techniques; and provides an overview of the RMS – addressing team composition, individual responsibilities, and general risk assessment reporting requirements.

- **Level 2 -** Formal training comprised of: a brief history of vulnerability analysis and risk assessment; experiences gleaned from organization-specific security risk assessments; and in-depth exploration of the Risk Matrix concept, the , related analysis techniques (such as HAZOPS, Fault Tree Analysis, consequence analysis, and probabilistic risk analysis), the operational integrity processes, emergency management, Level 2 individual responsibility, and specific reporting requirements. Level 2 includes participation in at least one major, complex, full scope risk assessment and contributions to development of an execution plan and to the review of the DRAFT report.
- **Level 3 -** (all Level 2 requirements plus) direct participation as a senior team member on at least two major, complex, full-scope risk assessments and co-authorship of at least one full-scope QRA report.

Refresher training should be provided every three years at all levels. For Level 2 and Level 3, additional specialty training should take place every five years if these personnel have not directly participated in major risk assessments during that period of time. Refresher training for Level 3 staff should also focus on progressive courses that teach new techniques (e.g., university courses, training seminars, and professional industry/government risk assessment conferences). The RMCs should be responsible for identifying and endorsing this training.

1.3.3 QRA Reporting

In order to facilitate the Safeguard and Security Qualitative Risk Assessment (SSQRA) process, it is possible to utilize commercial or custom developed software applications (such as Microsoft ACCESS). WORD and EXCEL also can be deployed to document results. The tracking features potentially allow for easy transfer of findings (causes, effects, and recommendations) into a central Risk Registry Database. It facilitates risk management which includes broad based application of risk findings, prevention, mitigation, and alternative strategies and tactics. In cases where management requires additional clarification of methodologies or to desires to address unresolved questions, the RMCs should be contacted.

After the conduct of a risk assessment, the RA Team Leader should complete the first DRAFT report in no more than two weeks. This DRAFT report should only be sent for review to the owner and the specific team members, with a two-week turnaround requirement. During this timeframe, the Team Leader should conduct an "error of fact" review with the owner. This is a critical step that could later serve to maximize risk mitigation/prevention alternatives. The Team Leader should then complete the FINAL DRAFT report within one week of the review phase. The FINAL DRAFT report should be sent to the owner and to all team members. Distribution decisions beyond that phase should rest with the owner. The owner should modify the SSQRA data – and therefore the RMSR – to reflect review results.

The Qualitative Risk Assessment Process

As noted, the key process within risk management programs is the conduct of risk assessments. The following seven elements are interpreted as comprising a QRA:

STEP 1 - MANAGEMENT APPROVAL, PLANNING AND PREPARATION

QRAs are normally commissioned by management responsible for operations being assessed, in coordination with the NN Security Centers and RMCs. Subject, scope, team composition, and organizational concerns and constraints should be addressed. This approval should be granted with an emphasis that risk assessment is a **"fact" finding, not a "fault" finding** system's analysis. This approval will generally improve quality and speed by insuring cooperation of mid-level management.

This approval initiates formal planning. This phase begins with preparation of the ***Risk Assessment Execution Plan***. The Plan consists of – identification of team leader; scribe and team member designations; methodology discussion; questionnaire, time duration; logistics; and costs. **The risk assessment methodology requires between 5 and 8 full-time members.**

Quantifiable data (discussed later) should also be enclosed. Local team members should prepare a detailed interview matrix showing interviewees with associated dates and times. Generally, interviews take the first 3-to-4 days of an assessment (with scenario discussion daily) and the risk calculation phase another 3-to-4 days. Cost calculations prioritization of recommendations, and exit briefing preparation take another 1-to-1.5 days. The management exit briefing usually takes two hours and finishes the in-facility phase.

Objectives and scope are communicated to the Team. The Team should then subdivide the risk assessment into components and determine which members will conduct what activities. Generally, these assignments include who will: interview key staff, review what data, analyze processes and operations, etc. Logistics must also be addressed at this time (travel, hotel, work areas, computer support, costs, etc.). In terms of team meetings, effectiveness is enhanced if members have a visual display of analysis results via computer screen projection (which allows for copying, printing), flip charts, etc.

***Team Activities* -** Team activities should initially key on a presentation by senior staff. The Team Leader should then introduce the Team to the QRA process. It is particularly important that the Team reach a common understanding as to the use of the SSQRA risk scenario classifications and the risk matrix (see Figure 4. through Figure 6), which both provide a framework for classification by vulnerability type, consequence and probability. The Team leader should also encourage Team members to express concerns.

Keys to success - Step 1

- *Select multidisciplined Team with scope and assumptions defined*
- *Team understanding of QRA Process*

The risk assessment Team is prepared to begin the core steps.

STEP 2 - IDENTIFICATION OF CRITICAL ASSETS: SYSTEM DEFINITION

Identification of assets is a crucial step in the process because it provides the basis for subsequent steps. The evaluation methodology presented here is CA/EECA.

CA/EECA - Identification of Critical Assets (CA) and Identification of Essential Elements of Critical Assets (EECA) - In this approach CA are those assets that are most important to keep from exploitation and EECA are elements that lead to those assets most important to protect. Identification of the "elements" refers to the policy, programs, processes, audit controls, and procedures that threats exploit to cause CA vulnerability. For example, from an adversarial perspective one might ask "If my task were to disrupt operations of a process control center, what would disrupt it, and where are the attributes that support it operationally?" The "what" is the CA, and the "where" is the EECA.

The concern with critical assets is what distinguishes a security program based on risk assessment from a security program that primarily focuses on generic protection (such as only securing a refinery perimeter). This broader approach requires an understanding of the totality of an activity, knowledge of threats, and an imperative to cross organizational boundaries (reference the Umbrella Figure 2) in activities which involve more than one entity (such as control centers, failure points, and computers within the asssets). Most 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 team can become aware of critical assets beyond the scope of traditional program reviews (such as program reviews) because those reviews tend to address a single organization or entity and observe organizational proprieties. These "traditional" reviews are vital and necessary. But through a focus on critical assets and discerning where they reside and flow (the "Umbrella" concept) within and between organizational boundaries, a team can identify vulnerabilities and make contributions to program effectiveness.

CA and EECA should be developed by the team in conjunction with a multidisciplined group of senior administrators and specific program managers (most of whom are interviewees in the risk assessment).

CA and EECA must be examined from a full-life cycle perspective which should include: Conceptualization; Research and Development; Prototype Development; Fabrication and Testing; Shipping/Delivery; Installation, Commissioning, Operations; Maintenance; and Decommissioning/Obsolescence/Removal. Other CA/EECA elements to consider include:

- Recognizability as a critical asset
- Effect of the loss of the asset
- Recoverability of asset – if breached, the time period for the asset to be re-deployed

Knowledgeable individuals must analyze and prioritize items in terms of relative importance and scored using a weighted system in terms of their value to a threat agent and, inversely, in terms of program damage. The four-descriptor system has these categories in order of importance: • Catastrophic

- Critical
- Marginal
- Negligible

Team assignment of descriptors to prioritize assets (such as personnel, information, and facilities) is vital for input to the SSQRA process.

As noted, relative (*catastrophic through negligible*) ranking is a common method of ranking asset exposure levels. This enables decision-makers to define acceptable risk thresholds and the range of unacceptably high exposure that would require resources for reduction and prevention. Although risk managers often strive to assess absolute levels of risk, the relative ranking of risks is an appropriate risk assessment strategy for risk control resource allocation. Cost-benefit analysis is often required to bring the burdens of risk control strategies to acceptable levels.

Keys to Success - Step 2:

- *The major elements that define a system should be identified by the Team.*
- *These system elements are typically equipment and facilities, procedures, people and environment.*

STEP 3 - ANALYSIS OF THREATS

Knowledge of the threat aids in identification of vulnerabilities that could be exploited by threat agents. The term threat refers to range of events or hazards that can exploit an asset. Threat agents consist of two elements; *static* (or relatively constant background) threats; and *dynamic* (or changing) threats. The threat component measures identifiable threat against safeguards (controls and mechanisms that protect assets from threats).

NN should consider preparation of a Design-Basis Threat Statement that characterizes the broad-based threat. Teams must use this generic statement as the basis from which to tailor the threat definition for the scope of an assessment.

Analysis of threat enables team members to assume a "threat agent perspective". This perspective is assumed by almost everyone in a competitive situation – from football opponents to the poker table. In assuming this role, a Team must examine the totality of a threat agent process.

By examining threat totality and assuming "threat agent perspective", a team can construct a threat strategy – that is, the probable sequence of steps that threat would go through to achieve an objective. These steps will be able to identify how an asset can be exploited. This is important in devising countermeasures to control vulnerabilities identified.

Asset determination and pairing with threat agents enable teams to develop scenarios (defined as the potential for real world undesired events). These scenarios are intended to briefly outline potential situations that could impact on security and safeguards functions. Sample scenarios are presented in Section 1.3.4 of this report. Each of these situations is the result of a number of concerns and causal effects and involves a variety of events and conditions. Scenarios may also prove to assist in identifying the potential for future security vulnerabilities.

Knowledge of threat and scenario development enables a Team to identify vulnerabilities and indicators in programs and activities that might otherwise remain undetected through reliance upon application of standard program reviews.

Keys to Success - Step 3:

- *At the conclusion of this step the Team should understand the system and have a preliminary understanding (through threat/asset pairing and scenario development) of potential vulnerabilities and potential causes of vulnerabilities.*

STEP 4 - ANALYSIS OF VULNERABILITY (Scenario Development)

In this step team members should begin classifying the specific vulnerabilities of prioritized assets. Completion of this step will provide:

	Item #
Control number	*1*
Scenario description—brief and full text	*2*
Existing safeguards (where available)	*3*
Potential causes	*4*
Potential effects	*5*
Safeguards and Security Risk Category (SSRC)	*6*
Safeguards and Security Risk Index (SSRI)	*7*
Recommendations	*8*
Recalculation of SSRC/SSRI (Effect of recommendation)	*9*
Notes	*10*

This is the core step and involves an examination of the totality of an activity to identify vulnerabilities. Vulnerability analysis identifies weaknesses that result in deviation from intended operations. Sources of information used to assess vulnerabilities include:

1. Evaluation of data developed during direct surveys

2. Evaluation of historic data from related incidents and/or system operating experience

3. Threat information, scenario development, and judgment by knowledgeable individuals

4. Use of generic checklists, structured interviews and questionnaires

5. Formal vulnerability analysis techniques--such as fault/event tree analysis, etc.

Team Review of Data from Evaluations of the Current Security Program - Existing NN security, safeguards, and, to some extent, safety procedures should be evaluated in terms of day-to-day operations. Previous evaluations (including audits) should be reviewed and facilities and assets toured. Security programs should be evaluated against certain standards, such as those associated with fire codes, government laws, regulations and directives. These will be required to complete the SSQRA process. Also, when applicable, teams should calculate the dollar value of existing safeguards (for example, if an access control system is deemed an existing safeguard the original cost should be indicated in the dialog box).

Team Review Data from Previous Security Incidents – Examination of previous security incidents – that is, what happened in the past, can provide insight into what may happen in the future. Previous “Insider”, "outsider", and “system induced” threats should be evaluated. It is the joint responsibility of the sponsor's representative and the Team leader to assemble useful summary information and provide it to other Team members prior to assessments. The data should be assembled and catalogued for quick reference.

Expert Opinion and Risk Scenario Development - The judgments of knowledgeable Team members – a multi-disciplined group of recognized experts, should be used as a starting point for final refinement of types of security vulnerabilities that could realistically occur from developed scenarios (what-if brainstorming). These scenarios should be used to assist in understanding the mechanism by which security incidents occur — the causes and effects. The scenarios should correspond, to the maximum extent possible, with asset priorities/threats determined in previous steps.

Checklists, Structured Interviews, and Questionnaires for Scenario Development - Generic checklists may be used to identify potential vulnerabilities. With this approach, the amount of detail in and applicability of checklists affect quality and quantity of vulnerabilities identified. The drawback is that no checklist anticipates every potentially hazardous situation, is created at a fixed point in time, and is not generally indicative of change, and the longest checklists tend to be both thorough and tedious to complete.

The Team should identify *key individuals* for interviews. Questions should be formatted according to the person's responsibilities (a doctor would have different questions than an auditor). A wide array of individuals should be slated for interviews (ranging from senior managers to protective force members) and both inside staff and outside staff should be considered (e.g. support contractors, military, law enforcement, other agencies, and similar industries). Use of standard interview questions should be encouraged to guide these interviews.

Structured questionnaires should also be considered. These are generally distributed randomly to a large cross-section of the operation before the assessment. These are intended to generate a "snap-shot" of security program effectiveness, identify assets and solicit suggestions for improvement from a broad base. Results tend to enhance the quality of structured interviews.

Scenario Development - Also known as vulnerability analysis – should begin based on definitions of the current security subsystem and how it relates to other subsystems (again, reference the umbrella figure). This data is presented in Chapter 0 of the Risk Assessment document. The primary domain elements are identified as the security management, information security, personnel security, etc. If the assessment scope is just information security, sub-elements that comprise the information security element, and therefore define the subsystem, would be significantly different (e.g., primarily the information security attributes). The following functional areas should be evaluated relative to the performance of the main elements (similar to the discussion of CA and EECA):

- Operations and Processes
- Policies and Procedures
- Physical and Technical Security
- Information Security
- Personnel Security
- Operations Security
- Security Management
- Security Configuration
- Audit and Control Mechanisms (as they relate to security)

Potential vulnerabilities and causes/effects should be identified for each of the systems and subsystems within the functional areas. Vulnerabilities should be identified through a review of the analysis of results.

Focus on "Totality of an Activity" **-** Through this analysis, the risk team will discern *where* and *how* critical assets reside, and how they operate, and how they relate and impact from one location or organization to another. As the Team collects data arrays, the team, almost invariably, will recognize indicators of critical assets. What keeps the systems analysis from bogging down in an endless accumulation of data and a mire of details, however, is the focus on those few **"golden nuggets"** called critical assets and a solid knowledge of the threat-agent potential.

One basic approach that a team may use in their systems analysis is to construct a chronological description of the actual or predicted unfolding of the activity or operation. In doing so, they are literally determining who does what, when, where, why and how, not only in the organization that has primary responsibility for the conduct of the activity, but also all supporting or related organizations. This is what is implied in examining the "totality of an activity".

By tracing assets throughout the entire "system", the risk team can identify vulnerabilities and indicators that would have been difficult or impossible to identify through a more restricted, traditional inspection of a single functional area within a single organization. For example, the detectable logistics activity of one organization (i.e., mining transportation division) could provide a threat agent with an indicator of the sensitive activity of another, that is the recipient of the logistical support (movement of explosives). Teams are not internal auditors and do not become enmeshed with an organization's compliance with regulations.

Teams will, in the course of their systems analysis, gain a comprehensive and detailed understanding of an entire operation. And, in light of threat, identify vulnerabilities that might logically ***not*** be identified by management and others assigned to a single unit in a multi-unit undertaking.

1.3.4 Examples of Scenarios Derived from Findings

The following are examples of findings derived from results of interviews, expert opinion, data reviews, etc. They represent categories of security system anomalies, which may impact on scenario development:

- Gaps in information security, electronic and otherwise;
- Gaps in intelligence and counter-intelligence;
- Failure of the sensor system to detect or respond to an intrusion;

- Inadequate capability or performance failure of a video system;
- Inadequate response by security staff in the command and control centers;
- Operational failure of the command and control center;
- Inconsistent security response to emergencies;
- Inadequate access control procedures;
- Inadequate security reporting by affiliates;
- Lack of security interface into project management teams;
- Lack of procedures for tracking and control of sensitive information;
- Personnel security assurance concerns.

Scenarios that may be derived from the above findings include:

- Loss or exploitation of classified information;
- Theft of key components of advance systems;
- Removal of sensitive research data results in competitive loss to adversaries;
- Theft of replacement parts from a warehouse results in suspension of operations
- After-hours attempt to access key NN Offices
- Copying of sensitive data from research area by unknown intruder
- Failure of security systems due to damage to the primary power feed at a command center
- Disabling of telecommunications node due to a break and entry
- Access to NN Company gained by a fired, irate, former employee through a lobby
- Chaotic bomb response after improvised explosive device is delivered to a mailroom
- Flawed emergency response;
- Theft of information by a contractor fired from one site and still granted access to another site
- Media publication of sensitive litigation findings copied by "trusted" employee
- Attempts by a competitor to influence litigation after receiving sensitive findings via the media
- Discovery of the removal of sensitive information from a computer but no reporting of incident
- Publication of sensitive data that is electronically scanned and copied
- Theft of sensitive litigation information valued at $25M by a computer hacker
- Management office bugged by cleaning force member working for a foreign competitor
- Acquisition of sensitive information by a foreign business partner from a Company foreign national scientist
- A NN employee, with a history of personal financial mismanagement and an arrest record, gets promoted into a key financial management position.

One scenario may relate to several categories (for example, abduction of an executive may relate to inadequate access control and inadequate sensor detection).

1.3.5 SSQRA Process Description

The specific vulnerabilities of prioritized assets are described and defined below. (An actual Risk Scenario Worksheet is provided in Figure 3).

Control Number – derived from a combination of the security program element window and the sequential number of scenarios attributable to that element. For example, a scenario such as "… a lack of security interface into operations integrity systems results in…." would probably fall into the Security Management element in the dialog box. So, if that was the first such scenario, the control number would be 1.01. The next Security management scenario would be 1.02.

Scenario Description (brief and full text) – a brief and full text description of each refined Risk Scenario. Scenarios **must** contain language that addresses the undesired consequence of the scenario.

Existing Safeguards – applicable sections of regulations, rules, and guidelines that were used as reference sources for the recommendations. In cases where no reference was located, the recommendation is based on expert opinion. Where possible, dollar figures that represent safeguards investments should be noted. When applicable, dollar values should be attributed to the identified safeguards (e.g. alarm system).

Potential Causal Factors – the potential causes of the scenario.

Potential Effects – describes the potential effects of the scenario. The team must consider that this step expands in detail the consequence language in the scenario. In establishing consequences, it may be helpful to supplement the team's judgment with screening level quantitative consequence analyses such as those for fluid release rates, fires or explosions.

Risk Assessment SSRC/SSRI – the Safeguards and Security Risk Category (SSRC) and the Safeguards and Security Risk Index (SSRI). This require use of the Severity/Probability tables and the Risk Matrix. When establishing Probability it may be helpful to think of likelihood of occurrence with the following questions in mind:

- How often has the vulnerability occurred in this operation? In a similar operation? Within this affiliate? Within NN? Within the industry?
- How often has a similar scenario and consequence occurred in this operation? In similar operations? Within this affiliate? Within NN Company? Within the industry?
- How do the existing safeguards compare to those in place for similar incidents in NN Company's or the industry's experience?

The final assessment of scenario severity and likelihood should be based on the team's best judgment in light of the assumed and/or existing safeguards and their perceived effectiveness.

Risk Rating **-** The basis for the risk rating established for each risk scenario by team consensus is the classification system accompanying the Risk Matrix. The SSRC represents risk in terms of both the severity and probability. For example, an SSRC of IIIC, indicates risk is "marginal" and "occasional". SSRI value means risk is "unacceptable, management decision required". This SSRI value is used to determine what management action is necessary. The SSRC and SSRI are expert judgments since adequate data is generally not available to actually determine the probability (unless formal analysis techniques are used).

Countermeasure Recommendation – describe methods that may be used to either eliminate causes or minimize effects of each scenario. Many recommendations are based on regulations, and guidelines.

Effect of Recommendation SSRC2/SSRI2 – the revised SSRC and SSRI reflect a reduction in *probability*, but most often, not *severity*.

Notes – Captures issues that arise during team discussions.

Keys to Success - Step 4:

- *Team Analysis or data, surveys, assessments*
- *Team use of Checklists and Questionnaires*
- *Team pairing of Threats and Assets to develop scenarios*
- *A determination of the existing security and safeguard systems*
- *Development of: a thorough understanding of the system; a final list of refined scenarios; an understanding of causal factors*

STEP 5 - RISK CALCULATION

Assessment of Scenarios (Undesired Events or Vulnerabilities) - It may not be possible to assess in detail each of the vulnerabilities and cause/effect factors identified by analysis. QRA values or calculations should be based on expert opinion (the process values what people think) and assessment results. The following sections address assessment of undesired events. Assessment results provide guidance on future security needs of individual elements and components of NN's security program.

Cause-Effect Analysis – After inputting existing safeguards in the SSQRA Dialog Box, the Team must next consider the causes and effects of the undesired event. The findings serve as the basis for calculating risk. In determining causes, the Team must consider the data, including data sources, and must factor in whether the cause is direct or indirect (i.e. a direct cause for a warehouse intrusion would be failure of a sensor system, an indirect cause could be allowing contractors unrestricted access inside a perimeter). The Team should be aware that there is generally a one-to-one relationship between causes and recommendations — so, for quality recommendations, *teams should vigorously brainstorm causes*.

Effects must be realistically evaluated and not "worst case." Effects must be analysed in terms of whether they are tangible (i.e. dollar based) or intangible (i.e. loss of reputation).

Undesired Event Severity and Probability Estimates - To establish an understanding of vulnerabilities and related countermeasures, the undesired events are assessed for their **severity** and **probability** of occurrence. This assessment is subjective again, it relies on what experts think. It can provide an indication of which undesired events pose the greatest threat. This understanding will determine which available countermeasures address those threats.

To assist in establishing event severity and probability of occurrence, Figure 4 and Figure 5 present severity and probability categories.

Severity of Undesired Events (**Figure 4) -*** Severity or magnitude of consequences of an undesired event will depend on the following factors: (1) type of threat; (2) type of asset being protected; and (3) whether threat can be deterred through application of countermeasures. It is recognized that severity of an individual event may vary considerably. It should be noted **that the potential severity of a compromise cannot be reduced unless the vulnerability is completely eliminated through a major redesign** (i.e. the application of encryption to a "unauthorized interception of a video teleconference" scenario). However, the probability, and therefore the associated risk, can be reduced by incorporation of security controls.

Probability of Occurrence of Undesired Events (**Figure 5.) -*** A calculation based on previous experience is needed to establish the probability that an event will occur. This calculation should consider that the event may have occurred or been reported to occur a certain number of times. Only some security data may be available. With limited quantitative data, such as that contained in a survey questionnaire, the evaluation may have to be based primarily on historical information and judgment of knowledgeable individuals.

Teams must also decide on a definable end date in order to estimate probability. This date can be the lifecycle of a technical security system (generally 10 years), be tied to key project/program milestones, etc. And, once established, that timeline must apply to all scenarios.

QRA Estimates and QRA Matrix (Figure 6.***) -*** Risk associated with an undesired event is the product of event severity and probability of its occurrence. The QRA risk matrix calculation estimate—or SSRC, derives from that product. The matrix (modified from Los Alamos, National Laboratory, U.S.MIL-STD 882e) is used to calculate a risk rating in a weighted fashion. The Risk Index—or SSRI, is a standardized ranking which characterizes a risk-rating system in a format that mandates certain management actions to control risk (levels 1-4 on right side of matrix).

Although in many cases, the probability of occurrence will not be estimated as frequent, the potential severity of certain undesired events requires that some type of action be taken to minimize the risk. Estimates can be useful in determining whether individual vulnerabilities should be eliminated or controlled to reduce the occurrence of the particular undesired event, or whether risk associated should be accepted.

As an example, the undesired event "loss of critical classified information" was assigned a Safeguards and Security Risk Category (SSRC) of IC (highest severity, occasional probability) and a Safeguards and Security Risk Index (SSRI) of **1**, which requires management action to reduce risk to the next lower level. Therefore, assuming correct evaluation, action must be taken to eliminate or control the risk associated with this event. Other risks that fall into this category are represented in IA, IB, IC, IIA, IIB and IIIA. Action should also often be taken to minimize the risk of undesired events with SSRI values of 2. Risks of this category include ID, IIC, IID, IIIB, and IIIC. Such risks require corrective action, although some management discretion is intended.

Keys to Success - Step 5:

- *Assessed Scenarios (including cause-effect analysis) in terms of severity and probability.*

SEVERITY	CHARACTERISTICS
I	Loss of life, loss of critical proprietary information, loss of critical assets, significant impairment of mission, loss of system.
II	Severe injury to employee or other individual, loss of proprietary information and physical equipment resulting from undetected or unauthorized access, unacceptable mission delays, unacceptable system and operations disruption.
III	Minor injury not requiring hospitalization, undetected or delay in the detection of unauthorized entry resulting in limited access to assets or sensitive materials, no mission impairment, minor system and operations disruption.
IV	Less than minor injury, undetected or delay in the detection of unauthorized entry with no asset loss or access to sensitive materials, no system or operations disruption.

Figure 4: Undesired Events Severity Categories[1]

PROBABILITY CATEGORY	LEVEL	SPECIFIC EVENT
A	FREQUENT	POSSIBILITY OF REPEATED INCIDENTS
B	PROBABLE	POSSIBILITY OF ISOLATED INCIDENTS
C	OCCASIONAL	POSSIBILITY OF OCCURRING SOMETIME
D	REMOTE	NOT LIKELY TO OCCUR
E	IMPROBABLE	PRACTICALLY IMPOSSIBLE

Figure 5: Undesired Event Probability Categories[1]

[1] Adapted from MIL-STD 882B

SEVERITY CATEGORIES	PROBABILITY OF OCCURRENCE				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	IA	1B	IC	ID	IE
II	IIA	IIB	IIC	IID	IIE
III	IIIA	IIIB	IIIC	IIID	IIIE
IV	IVA	IVB	IVC	IVD	IVE

Figure 6: Risk Assessment Matrix

Risk Category	Color Code	Risk Index Management Expectation	Risk Index Level
I A, I B, I C, II A, II B, & III A	🟥	Implement Countermeasures that Reduce Risk to an SSRI of a Level 2, at a Minimum.	1
I D, II C, II D, III B, & III C	🟫	Not Acceptable without Management Reevaluation.	2
I E, II E, III D, III E, IV A, & IV B	🟨	Acceptable with Review by Management.	3
IV C, IV D, & IV E	🟩	Acceptable without Review by Management.	4

STEP 6 – RISK EVALUATION—COUNTERMEASURES/RISK RECALCULATION

***Risk Reduction Countermeasure Identification* -** Actions taken to minimize security risks are termed countermeasures. A countermeasure is defined as any action or series of actions that may be taken to reduce the risk of an undesired event and/or the frequency of its occurrence. The majority, described below, emphasizes preventing occurrence of the event (primary countermeasures). The remainder focuses on responding to the event (secondary countermeasures).

The recommendations for corrective actions describe the method selected to eliminate the causes or minimize the effects of each vulnerability. One or more recommendations should be provided for each identified vulnerability or cause, and the Team must **re-calculate risks** based on the effect of a countermeasure on the Scenario. It may be useful for the Team to incorporate a new member at this stage to assist in the evaluation of *risk reduction efforts.* Some methodologies suggest an entirely new Team at this juncture. Also, it may not be possible to re-calculate risks until certain system re-design, re-engineering, etc., is complete. The Team may have to re-calculate risks at a future time, on a case-by-case basis.

Many recommendations should be based on existing codes, standards, and guidelines. These should be considered in the Existing Safeguards. In some cases, reference sources may recommend different criteria; the criteria applied depend on "reasonable" interpretations by the affected organization. Vulnerabilities inherent in the system may be avoided by following new codes, standards, regulations, laws, and general guidelines that have emerged since last updated safety and security systems.

Evaluation of Potential Countermeasures - Countermeasures areas should be identified and described.

Within each of these areas, the Team should identify specific countermeasures that may be applied. In some instances, more than one countermeasure may be identified for a particular element. Furthermore, the undesired event may be the result of the following:

1. Vulnerabilities and causal effects associated with one or more components within the same element; or
2. Vulnerabilities and causal effects in different elements.

Since an undesired event may result from one or more sets of vulnerabilities and causes in one element, or in different elements and components, two or more countermeasures may be required to prevent or reduce the occurrence of that undesired event. It is important that all possible elements and component vulnerabilities and causal effects be examined to identify countermeasures that will prevent occurrence of the undesired event or mitigate its consequences. After identification, the most appropriate countermeasure should be selected based on:

- Effectiveness
  - Does it reduce the probability of occurrence?
  - Does it reduce the severity?
- Cost of implementation
  - Is it incorporated into the design prior to production or operation?
  - Can occurrence be controlled with operational procedures?
  - Does the countermeasure require retrofits?
- Enforcement and audit requirements

The following sections provide guidance on how the individual factors may be evaluated and assessed.

***Effectiveness of Countermeasures* -** Effectiveness requires a judgment on how implementation will influence probability of occurrence and, to some extent, severity (noting that severity can only be reduced through a major re-design). With regard to probability of occurrence, the countermeasure may:

- Result in no change;
- Reduce the probability of occurrence of the event; or
- Totally eliminate the possibility of event occurrence (no event).

Similarly, with regard to event severity, the countermeasure may:

- Result in no change;
- Slightly reduce the severity of the event;
- Minimize the effect of the event; or
- Increase severity.

***Cost of Implementation* -** The cost incurred will depend on when and how the countermeasure is adopted. In general, it is more cost-effective to incorporate the countermeasure into the design of the system or subsystem prior to its production or operation. Generally, a technical retrofit would be approximately ten times more costly than incorporation at the design stage. Furthermore, the cost will be directly related to the element or component into which the countermeasure is adopted. For example, procedural changes (such as enhancing security program interfaces) will generally cost less to implement than changes that involve the acquisition of new or modified equipment. Cost methodology guidelines addresses:

- Design,
- Fabrication,
- Testing,
- Operation,
- Maintenance,
- Retrofit,
- Change of Operations and Procedures.

Within each of the above phases of the life cycle, the cost will depend on the costs of the following:

- Materials,
- Labor,
- Training,
- Operation,
- Downtime, and
- Procedural Modifications.

The cost of implementation must be considered relative to the effectiveness of that countermeasure. For example, the cost associated with a design change early in the design phase may be worth the additional cost if that countermeasure will eliminate a security vulnerability.

Costs for labor and materials should be expended (if possible) in the design and testing phases to eliminate vulnerabilities in the subsystem or component. Labor, training, and downtime costs associated with implementing a countermeasure during operation and maintenance are more likely directed at controlling known vulnerabilities. This approach is not as desirable or as safe as eliminating the vulnerability prior to operation.

***Net Present Value (NPV)* -** In addition, the SSQRA process should contain an NPV. NPV calculates, in accordance with General Accounting Principles (GAP), the Net Present Value (NPV) of security investments. NPV should be used on all assessments where proposed measures either save or spend financial resources.

***Enforcement and Audit Requirements* -** A secondary cost associated with the implementation of a countermeasure is that of ensuring that the countermeasure has actually been implemented, is operating properly, and has not created any new vulnerabilities. This enforcement requirement will require the dedication and expenditure of resources. Enforcement is a function of day-to-day performance, and is not discussed in detail here. However, the cost should be evaluated prior to selecting and implementing countermeasures.

***Risk Reduction Countermeasure Categories* -** Design countermeasures for physical security may relate to the protection and safeguarding of personnel information, equipment, and operational systems within the facilities. Design countermeasures should also address the future expansion of Safeguards and Security Sub-systems.

Some typical Safeguards and Security design countermeasures include:

- Reconfiguration or Protective Forces
    - Shift Rotations
    - Mobil Posts
    - Increased Training
    - Increased Contract Standards
- Intrusion Detection System
- Exterior Video Assessment
    - Signal Transmission
    - Video Switching
    - Video Loss Detection
- Process Control System
- Sensitive Information Protection System
- Technical Security of Sensitive Information
- Technical Surveillance Countermeasures
- Alarm Multiplexer Communication System (AMCS)
    - System Considerations
    - Nuisance Alarm Rate/False Alarm Rate
    - Operational Functions
    - Ease of Operations
    - Availability
- Display Systems
    - Screen Display and Annotation
    - Rapid Alarm Recording and Playback
    - Archival Recording
    - Video System Controller
- Processing Centers
- Personal Security Database Management
- Hazardous Materials Countermeasures

***Testing and Inspection Countermeasures* -** A testing and acceptance program determines if all security-related systems in NN meet operational requirements. All test procedures and results should be documented. These tests should include the following:

- Subsystem tests (e.g., tests of databases, central processing units (CPUs), electrical systems);
- System tests (e.g., tests of access control);
- Operational tests;
- Protective Force Performance Tests;
- Acceptance tests; and
- Periodic emergency system tests.

Each security system and subsystem (including information security) should be certified by before it is used with staff. Tests should demonstrate that operating systems and subsystems match contract parameters. Tests should identify and resolve discrepancies during early design phases. Certification tests should be conducted in their operational environment (such as exterior areas in a refinery).

Guidelines for periodic inspections by the security staff should be prepared. Inspections should be conducted during the following phases: pre-installation testing, installation, maintenance, and operations. Reports should be prepared and submitted to the responsible Security element.

***Configuration Management Countermeasures* -** A configuration management program (or management and documentation of change) should be implemented to ensure that design and development of, and operational changes to, systems and subsystems are subjected to strict configuration control. At a minimum, documentation should include training materials, test, maintenance, and operating and emergency procedures.

***Operational Countermeasures* -** There are guidelines that require manufacturers to define the operational parameters. Design, fabrication, testing, acceptance, and operations could vary, however, depending on intended missions. All components should be approved by Underwriters Laboratory (UL). Countermeasures should be established to address guidelines for the following:

- Development and documentation for operating procedures;

- Staff familiarization; and
- Operations such as process control, technical security, personnel, priority protection, and emergency operations.

Training Countermeasures - Training countermeasures should include minimum qualifications for applicants in critical positions – such as command and control center operators. The training path leading to certification, as well as measurable goals and objectives for each aspect of the training, should be clearly defined.

The training program should represent a systems approach to training and should include:

- An assessment phase to determine training needs and objectives;
- A development phase to select training methods and develop courses;
- A training phase; and
- An evaluation-and-feedback phase to determine whether the training is appropriate for tasks being performed and to help ensure that changes (e.g., use of new security equipment) are included in a continuously revised curriculum.

Maintenance Countermeasures - Maintenance countermeasures include the development of procedures and documentation. This includes routine and preventive maintenance procedures and plans, which should be developed during the design and development phase. In addition, periodic inspections should be conducted.

Repairs, replacement, and normal system changes are part of maintenance, as defined here. Any proposed system should be easy to maintain. Significant expansion capability should exist in all system aspects. All hardware should be commercially available and supported by vendors. Documentation to support the maintenance of any software used should be provided.

Emergency Preparedness Countermeasures - As a result of risk assessment, the emergency preparedness plan should address all aspects of emergency planning and emergency response. This plan should include, at a minimum, emergency operating procedures in light of newly implemented security and safety designs; requirements for operating emergency equipment; and requirements for emergency interface between the Company and relational organizations, such as the Police Departments.

Life Expectancy Countermeasures - The life expectancy of components should be determined during the design phase, and should be reviewed periodically during operational phases to determine consistency with actual experience. Issues to be considered include:

- Failures of procedures and engineered features;
- Erosion of the system, e.g., erosion of electronics (especially exterior electronics) and the pan/tilt/zoom camera features;
- Lack of proper scheduled maintenance;
- System damage; and
- System repairs.

Recertification or Inspection Countermeasures - All systems should be inspected regularly. In addition, they should be inspected after certain events occur or when certain changes are made. Criteria should be developed for determining when a system should be inspected or, if necessary, recertified (as may be the case in some sensitive areas). Recertification is likely at the following times when:

- An unauthorized individual enters a sensitive area;
- A major change is made to operating parameters;
- A system is modified (engineering modifications);
- Major systems are replaced;
- New personnel are assigned in sensitive areas; and
- A critical program has been transferred to another NN Company directorate.

***Degraded Operation Countermeasures* -** Due to system redundancy, no alarm data should be lost in the event of main computer failure or line cuts between the multiplexers. Most sensor and video failures should be detected and reported by the system, ensuring continuous operations.

1.3.6 Monitoring and Follow-up tracking System

A system should be in place to ensure that mitigation recommendations receive proper attention from management so that risks are adequately addressed. To achieve these primary objectives, a follow-on process must ensure that:

- Risks have been captured using the qualitative approach.
- Risks have been analyzed in accordance with risk management planning.
- A risk assessment "owner" has been appointed with long-term stewardship responsibility.
- Management is made aware that other options may exist with regard to risk mitigation alternatives in light of changes in available resources, new technologies, actual incidents, and new scenarios.
- Risk decisions are well documented and effectively communicated.
- Recommendations are implemented in a timely manner and undergo a formal close-out process.
- Individual risk assessment "owners" interface with NN Security risk management stewardship.

***Post Risk Assessment Follow-up* -** Management for pre-and-post risk assessment actions should designate an "owner." The owner is defined as a manager in whose operation the risk assessment is conducted and who has overall responsibility for the follow-up and close-out process. The owner's key follow-up responsibilities include:

- Reviews Team recommendations and prioritization. If necessary revise prioritization in consultation with the RA Team Leader.
- Recommends alternatives in addition to those proposed by the Team. If higher risk scenarios are identified, notifies the RA Team Leader.
- Prepares a Risk Management Summary Report (RMSR) that includes an action plan addressing team recommendations, assigns person(s) to implement specific follow-up actions (assignee), and has management approval.
- Reports critical safety, health, and environmental concerns identified by the team to affected personnel.

- Stewards the implementation plan and provides the Team Leader and RMCs with status reports.
- Communicates changes in the follow-up plan to the RA Team Leader and the RMCs.

Risk Assessment Draft Review - The owner should review the DRAFT QRA report with a view toward "error of fact" analysis and reevaluate risk priorities. During the review process, risk calculations may be modified. However, when the "FINAL DRAFT" report is issued, no further risk calculation should be allowed.

Final Draft QRA Report - Within two months of receiving the FINAL DRAFT Risk Assessment Report, owners are required to develop an action plan that addresses team recommendations. If a recommendation is rejected, owners should document the justification and develop alternatives to all risk index (SSRI) ratings 1 or 2. The action plan for addressing recommendations – and/or new alternatives – should consist of actions to be completed, resource requirements, responsible personnel (assignees) for each action, and a schedule for anticipated completion dates. The plan should also document use of any outside resources. Follow-up plans should be documented in SSQRA software (e.g. ACCESS, WORD, EXCEL), which tracks close out of recommendations.

An “assignee” is a person whom the owner appoints to implement specific follow-up actions. The owner should identify assignees and their respective responsibilities in RMSR documentation. The owner must clearly communicate information and expectations of performance relating to follow-up actions to each assignee. The RMCs, have region-wide responsibility. Owners are responsible for providing the RMCs with follow-up documentation, including identification of assignees and their respective responsibilities.

Owners are responsible for making final decisions (in conjunction with management directives and budget/resources, etc.) needed to address risk mitigation / prevention recommendations. The owner is responsible for communicating risk levels associated with operations and activities to management. The owner documents communication of the risk levels to management by preparing and submitting the Risk Management Summary Report (RMSR) for approval. Management approval of the RMSR acknowledges the existence of risks and related mitigation countermeasures.

A Communications Plan is a required element of each risk assessment and should be included as an “action-list item” in the RMSR. The owner is responsible for developing and implementing this plan, as well as determining its form and content. The purpose of the Communications Plan is to increase risk awareness and commitment to improve security and safeguards, as well as to inform relevant management, contractors, and security staff of the status of risk assessment elements. In support of the Communications Plan, owners should closely monitor integrity-critical items with appropriate personnel throughout the development of the RMSR. Scenarios that have an impact on specific operations (e.g. emergency response) should be communicated to staff in charge of those units.

The owner should also determine timetables for action-item resolution and send RMSR to interested parties for comment. RMSR should document options to manage each risk, as well as the implementation timetable. RMCs should then decide whether to accept or further modify a proposed follow-up plan. Once approved, the follow up plan should be implemented in accordance with specific change-management procedures. It may become apparent through these evaluation cycles that risk severity and probability may have changed and those action plans may have to be re-evaluated.

Addressing Higher Risk (Levels 1 and 2) - The owner should report all higher risk scenarios action items to security management and the RMC within a reasonable time of the assessment. This can be a formal request to continue operations despite the identified high risk or a memorandum notifying management of the higher risk levels inherent in continued operations.

In some cases, the owner may have to adjust prioritizations in light of data that may not have been available to the team (such as budget resources). However, owners must remain cognizant of risk reduction objectives when altering priorities developed by the risk assessment team. Any changes owners make to prioritized risk ratings must be communicated to the Team Leader and the RMC.

RMCs should approve reductions in risk evaluations to lower levels attributable to proposed prevention / mitigation measures. Approval of risk reduction by management should be documented in writing and sent to the RMC for inclusion into a Risk Registry Database containing:

- Risk-related libraries,
- Management response and follow-up plans, and
- Current status of follow-up plans being implemented.

The RMC should include all higher risk scenarios in quarterly and annual status reports along with documented management responses.

***Tracking* -** The SSQRA process documents tracking and close-out of risk assessment recommendations. The follow-up plan, with its action list of due dates and allocated responsibilities, serves as the tracking system. The status of each action item should be monitored until formal close-out or circumstances have changed where any remaining action item no longer relates to unacceptable risk exposure (such as completion of a project phase or cessation of facility activity). In addition, the status of risk assessments that have been undertaken and risk assessments still planned should also be monitored and reported. All of these action-item and status reporting activities constitute the tracking and close-out system. The system depends heavily upon both owner and action item assignee input. NN Security should own the tracking system and the NN RMC is the administrator.

***Close Out* -** Once mitigation countermeasures have been implemented, the owner should close-out the follow-up plan. This report should describe the major action items that resulted from the assessment, any major changes experienced in implementation, and any experience that may be worthwhile for future assessments.

A copy of all close-out reports should be sent to the NN/ Regional RMC. They should log close-out reports into the database and inform management as to the status, especially those actions mitigating high risks.

***Responsible and Accountable Resources* -** RMCs should be responsible for establishing, monitoring, communicating, and maintaining the follow-up plan. RMCs should ensure that procedures are in place and that periodic updates and verification of those procedures occur. Both the risk assessment owners and the RMCs must approve any changes to the risk management procedures.

***Verification and Measurement* -** RMCs should be responsible for evaluating follow-up plan effectiveness at least yearly. Checks should be made to determine if assessments and follow-up activities have occurred as planned and can be easily measured using automated tracking tools (such as SSQRA). Annual verification to assure that the follow-up action plan is providing high quality results should be performed through formal interface with owners and end users. Other elements that help contribute to the effectiveness of evaluations include:

Reviewing risk assessment logs held by RMCs with special emphasis placed on examination of unacceptable risks;

Involving non-security staff in risk assessment reviews;

Conducting field compliance reviews by both security and non-security staff; and

Monitoring the total number of identified risks.

***Reports* -** An electronic copy of all assessments should be made available to the RMCs for input to the tracking system. The QRA reports are the starting point for the tracking system. The RMC should inform involved security staff of due dates, format, and the collection mechanism used for periodic status reports.

The RMCs should prepare quarterly and annual status reports for distribution to management. Distribution of these reports should also include outside elements, such as safety programs. The quarterly status report as to action items should include:

- Total number;
- Number closed in the last quarter;
- Total number that has been closed;
- Number ongoing;
- Overdue list;
- List of assessments with items that have been closed in the last quarter;
- Number closed versus the number scheduled to be closed;
- List of one-person assessments held in the past quarter;
- Identification of assessments that have resulted in new items; and
- A list of QRAs scheduled for the next quarter.

The content of the annual status report should be the annual equivalent to the quarterly status report. The NN RMC should make a presentation to senior management periodically (at least annually) providing an overview of major assessments held, major action items, and the status of those items.

Keys to Success - Step 6:

- *The Team should resolve vulnerabilities and made corrective recommendations to eliminate or control risk.*
- *All QRA data should be presented in draft and final draft reports and entered into the follow-up tracking system as presented in section 1.3.6.*

STEP 7 - AUDIT OF IMPLEMENTED COUNTERMEASURES

This final assessment step also involves quality control and audit reviews of implemented countermeasures to assure they provide the desired effect and have proven system efficiency. This analysis should examine whether additional vulnerabilities have been generated from implementation countermeasures and controls. This should be completed at specific range gates (e.g. one year) after action item close out.

Keys to Success - Step 7:

- *Monitoring should be in place to assess corrective action effectiveness and to detect unexpected new vulnerabilities.*

2.0 ENTRY BRIEFING

This reference includes the Entry Briefing slides of the presentation that initiates the Safeguards and Security Qualitative Risk Assessment (SSQRA) session.

2.1 Scope

- Military Standard 882e Los Alamos, adopted by Nuclear Regulatory Commission and then by the American Institute of Chemical Engineers (AICHE).

- Major global companies adopted the AICHE model as part of the Operations Integrity Management System.

- The methodology relies on a multi-disciplined team of 4 to 6 (depending on Limited Scope vs. Full Scope) subject matter experts to develop undesired event scenarios and make recommendations--through cause-effect analysis--that will reduce risk.

2.2 Why Assess and Manage Risk?

- The term risk denotes the probability and severity of an undesired event. The following are key reasons for us manage risk:

- Organizations and systems (such as safety) expect us to manage risk

- NIST (quantitative/qualitative), expert judgment, Wharton School example

- Every endeavour and must deal with the inevitability of unintended consequences;

- No one will ever know all the risks;

- Risks are not equally consequential;

- All endeavours should balance risk and benefits;

- Resources for identifying, eliminating, and/or controlling risk are very limited;

- Management should identify, eliminate, and control all serious risks and it must be recognized that tactical risk assessments are the key to strategic risk management.

2.3 Terms

Security — procedures and engineered features that mitigate the consequences of assumed off normal operations or undesired events.

Risk — loss potential.

Threat — an entity that can exploit an asset.

Scenario — vulnerability that can cause a deviation from intended operations.

2.4 Goal

- Fact finding, not fault finding.

- Structured, studied, multi-disciplined approach to security decision-making.

- Wide scope applications.

- Sets the stage--defines the road map--for future security applications.

- Assists in all security decision-making.

2.5 Cost-Effective Safeguards and Security Decisions

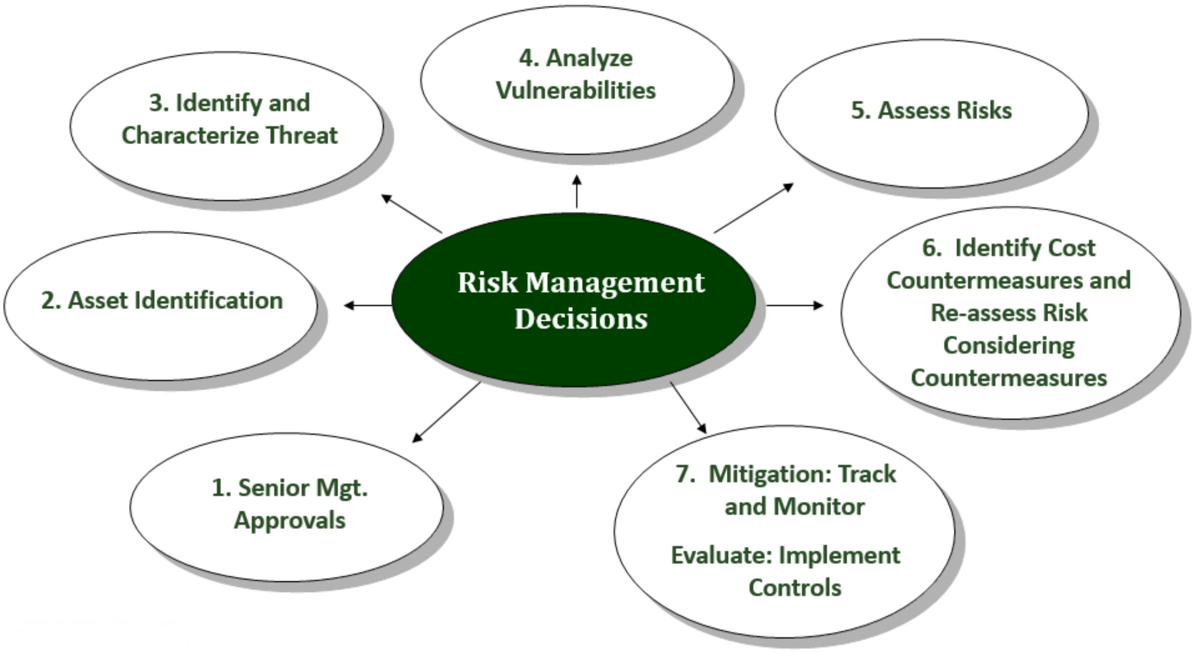

4. Analyze Vulnerabilities
3. Identify and Characterize Threat
5. Assess Risks
2. Asset Identification
Risk Management Decisions
6. Identify Cost Countermeasures and Re-assess Risk Considering Countermeasures
1. Senior Mgt. Approvals
7. Mitigation: Track and Monitor
Evaluate: Implement Controls

Figure 7: Risk Management Process

2.6 Operational Risk Model

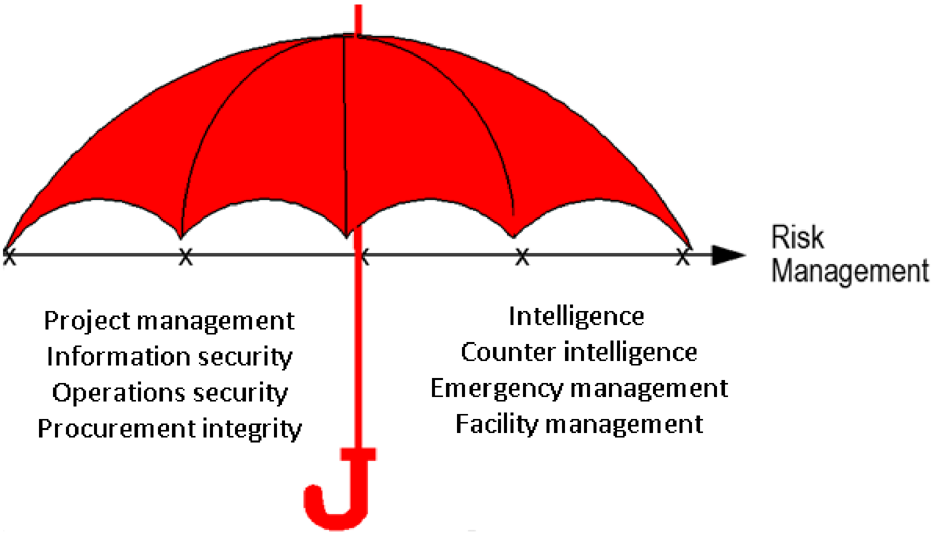


Figure 8 : Risk Management Umbrella Concept

2.7 Step 1: Management Approval, Planning and Preparation

- Four criteria that trigger an assessment:
  1. Security risk assessment schedule;

2. Significant change;
3. Serious incident; and/or
4. Emergence of a new scenario.

- Address subject, scope, team composition, and organizational concerns/constraints with management/owner who commissioned the assessment.
- Get owner's designee on team.
- Build an interactive relationship (emphasize team approaches to decision-making).
- Execution plan (emphasize fact- not fault-finding).
  - Assess appropriate levels of protection for assets to a future definable date (i.e., year 2022).
- Capture the process and the environment (what is unique) in the execution plan:
  - Determine what keeps management awake at night.
  - Obtain support information (incidents, operations, etc.).
  - Finalize the Threat Characterization Statement.
- Determine core team members — multi-disciplined (collateral team members).
- Detailed Execution Plan – beforehand at:
- 2 month point—lock in on specific project, solicit management approvals, ownership, team
  - 1 month – detailed telcons with final team members, explain SSQRA process, send out execution plan strawman to be completed with owner
  - Initiate – 1 day entry briefing, detailed site tour, data
  - Day 2-3 – interviews (~20 staff, outsiders)
  - Day 4-5 – structured brainstorming, team only
  - Day 6 – exit briefing to management
  - Day 7 – complete draft report—send to team only
- Execution plan models

Overall Scope

- Assess all security measures in place for all operations, including security systems and protective force allocation.
- Consideration of risk exposure relative to oil production processes.
- Evaluate off-site consequence analysis of facility loss of operations due to security breach.
- Review existing assets with a view toward prioritization of how their losses would affect its operations and assess appropriate levels of protection.
- Review current and projected safeguards and security systems and evaluate implementation.
- Review command and control functions.
- Assess technical security equipment placement and functionality.
- Assess personnel security (existing background investigations of key personnel).

- Assess the general cyber-security and information security environments.
- If needed, assess opportunities to optimize protection of plant employees (home, office, and travel).

Security Program – Transportation

- Potential measures to provide secure means of transportation (time restrictions, route restrictions, and tracking systems).

Security Program – Office

- Access procedures.
- Visitor and mail screening procedures.
- Logistics:
  - ~7 days consisting of interviews/data reviews, risk assessment.
  - Interview matrix (average about 15-20) – subdivide team, 2 interviewers per interviewee, not in management chain.
  - Interviewees: wide mix of internal/external personnel/agencies.
- Familiarize team with the methodology – particularly the LSSQRA Scenario Worksheet and the Risk Matrix.
- Finalize team roles, solicit team concerns, and assign report writing responsibilities (Scribe=engineer or technical asset).

2.8 Step 2: Identify Critical Assets and Essential Elements of Critical Assets

- “Gold Nuggets/Gold Dust” - define system.
- Defined and prioritized in terms of their importance to the organization and relationships (umbrella).
- They must be weighted both in terms of impact of loss and duration of loss and categorized in terms of the following descriptors (relative ranking) as:
  - Catastrophic.
  - Critical.
  - Marginal.
  - Negligible.

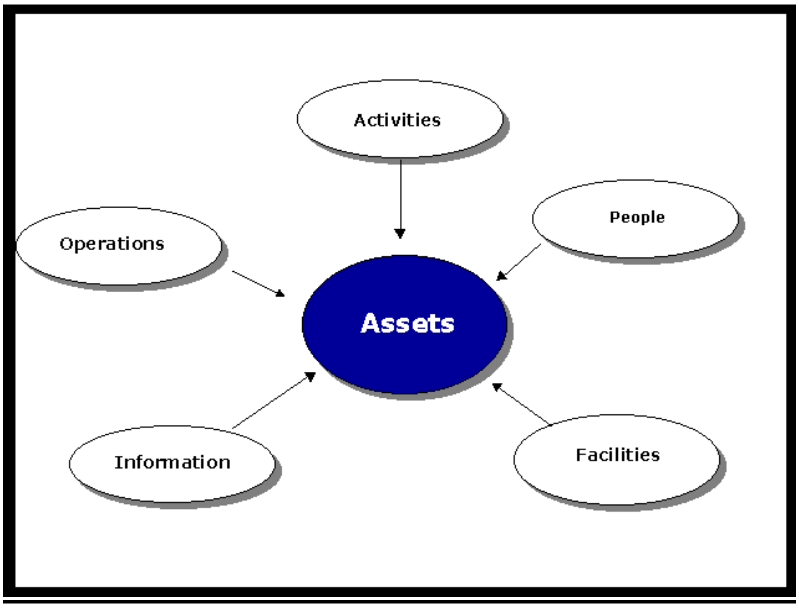


Figure 9: Identifying Assets

- This "relative ranking" is critical for scenario development: Team focuses on important issues.
- Ask:
  - What critical activities take place?
  - What are consequences of asset loss (in-and-out)?
  - What are the activities of personnel?
  - What is the critical information?
  - What is the critical equipment/processes?
    - What supports those?
    - Where are they located (on site and/or off-site)?
  - Detailed Asset Listing
  - PJNDG
  - Rotterdam example

2.9 Step 3: Threat Analysis

- Threat is an event or hazard that can exploit an asset. (determined in Step 2)
- Team must consider both static and dynamic threats.
- Threat statement should discern:
  - Threat goals/objectives;
  - Means/capabilities; and
  - Motivations.

Threat Characterization:

- Insider:

  - Employees (75% problem).
  - Employee Organization Relations (e.g. Union).
  - Contractors.
- Outsider:
  - Terrorism/Criminal.
  - Former Employees.
  - Transportation Phase Threats (i.e. products, explosives)
    - Need life cycle perspectives.
  - Environmental Issues, Media Attention, Legal Complications, Political Uncertainty.
- System Induced (not a focus):
  - Existing programs and organizational units.
  - Security's relationship with other programs.
    - Lack of incident reporting.
  - Background investigation process.
  - Lack of coordination in planning, engineering, design, and development.

o

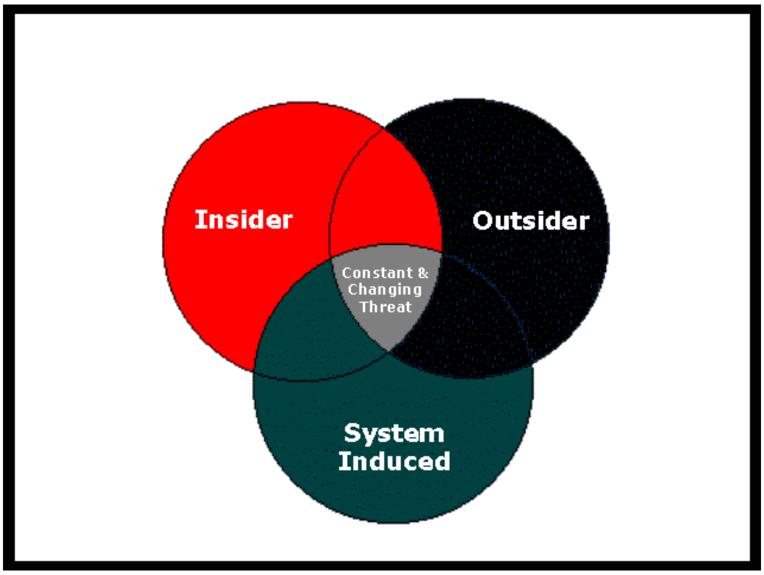


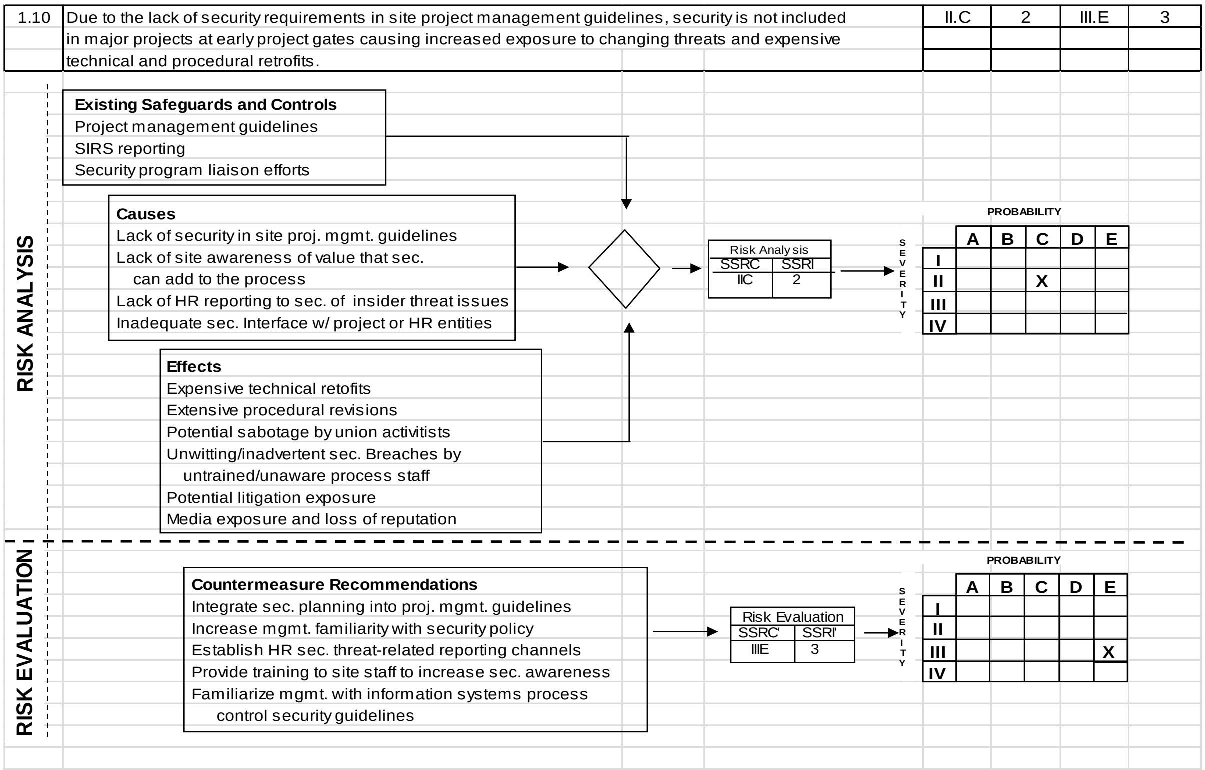
Figure 10: Types of Threats

2.10 Step 4: Scenario Development

- Pairing of Threats/Assets:
  - Vulnerabilities that cause deviation from intended operations, even after consideration of existing safeguards.
- Focus on significant issues.
- Example: "Due to lack of security requirements in project management guidelines, security is not included in major projects at early milestones causing increased exposure to changing threats and

expensive technical and procedural retrofits."

- Scenario must have a consequence ($ = best).
- Relate to "umbrella" (Operational Risk) concept:
    - Personnel surety (employee suitability).
    - Information security (including opsec).
    - Physical and technical security.
    - Security relationships (safety, HAZOPS).
    - Facility operations and processes.
    - Facility policies and procedures.
- Provide informal/positive feedback to senior management.



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

Existing Safeguards and Controls
Project management guidelines
SIRS reporting
Security program liaison efforts

Causes
Lack of security in site proj. mgmt. guidelines
Lack of site awareness of value that sec. can add to the process
Lack of HR reporting to sec. of insider threat issues
Inadequate sec. Interface w/ project or HR entities

Effects
Expensive technical retofits
Extensive procedural revisions
Potential sabotage by union activitists
Unwitting/inadvertent sec. Breaches by untrained/unaware process staff
Potential litigation exposure
Media exposure and loss of reputation

Risk Analysis	
SSRC	SSRI
IIC	2

PROBABILITY

SEVERITY	A	B	C	D	E
I					
II			X		
III					
IV					

Countermeasure Recommendations
Integrate sec. planning into proj. mgmt. guidelines
Increase mgmt. familiarity with security policy
Establish HR sec. threat-related reporting channels
Provide training to site staff to increase sec. awareness
Familiarize mgmt. with information systems process control security guidelines

Risk Evaluation	
SSRC'	SSRI'
IIIE	3

PROBABILITY

SEVERITY	A	B	C	D	E
I					
II					
III					X
IV					

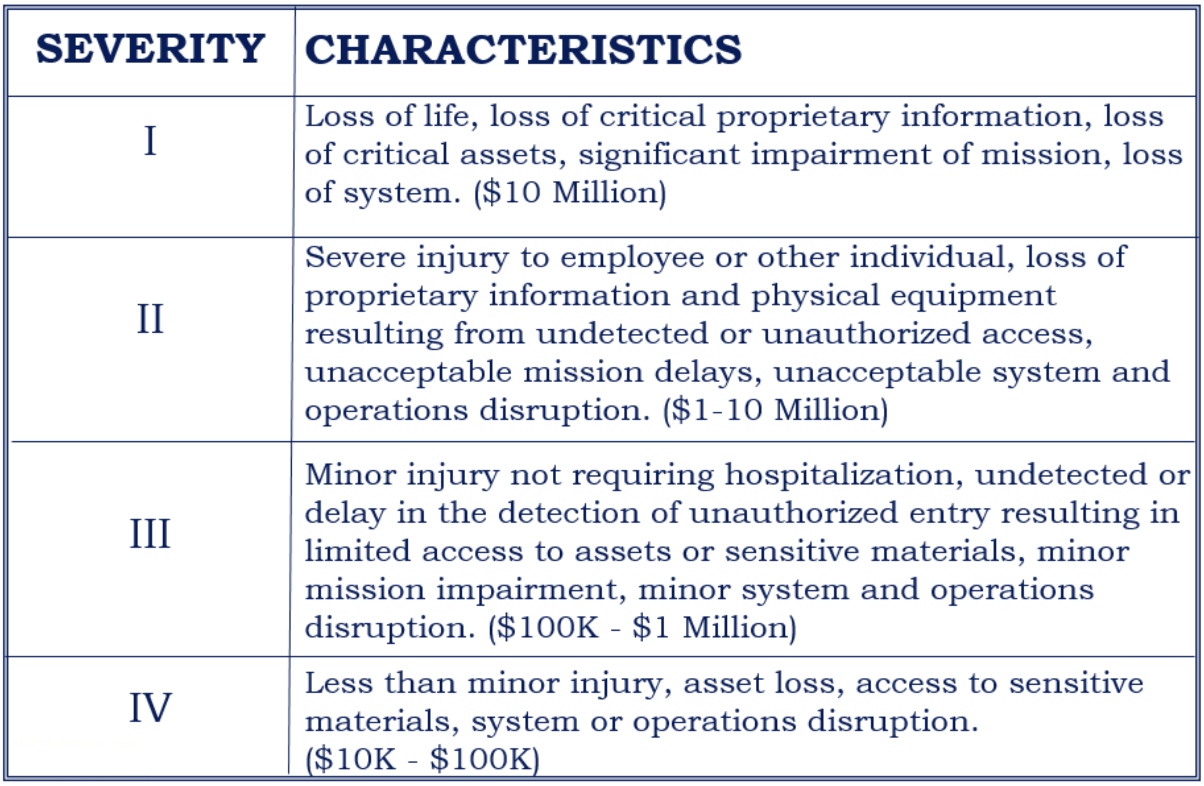
Figure 11: Risk Scenario Worksheet

2.11 Step 5: Risk Assessment

- First phase risk ratings (known as safeguards and security risk index) are based on scenarios, terms of severity and probability of occurrence.

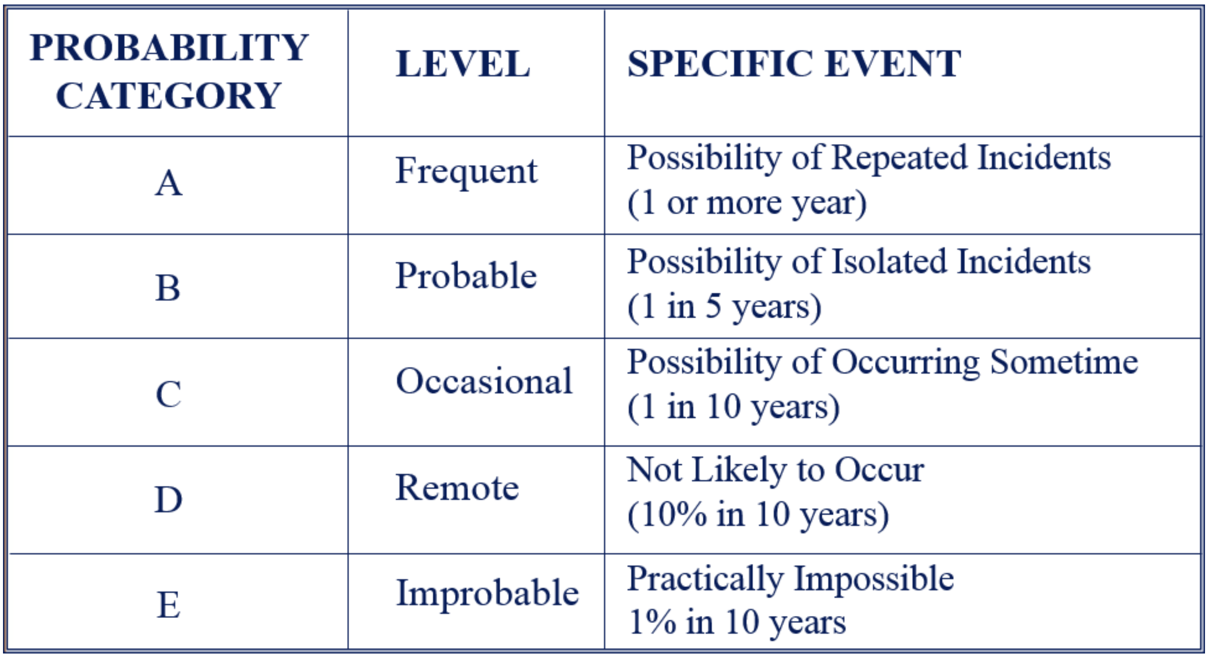
- The safeguards and security risk index presents data in a format that assists decision-makers in determining whether vulnerabilities should be eliminated, controlled, or accepted.

Note: The severity of a compromise cannot be reduced unless the vulnerability is completely eliminated, but the probability, and therefore the associated risk, can be greatly reduced by the application of countermeasures.



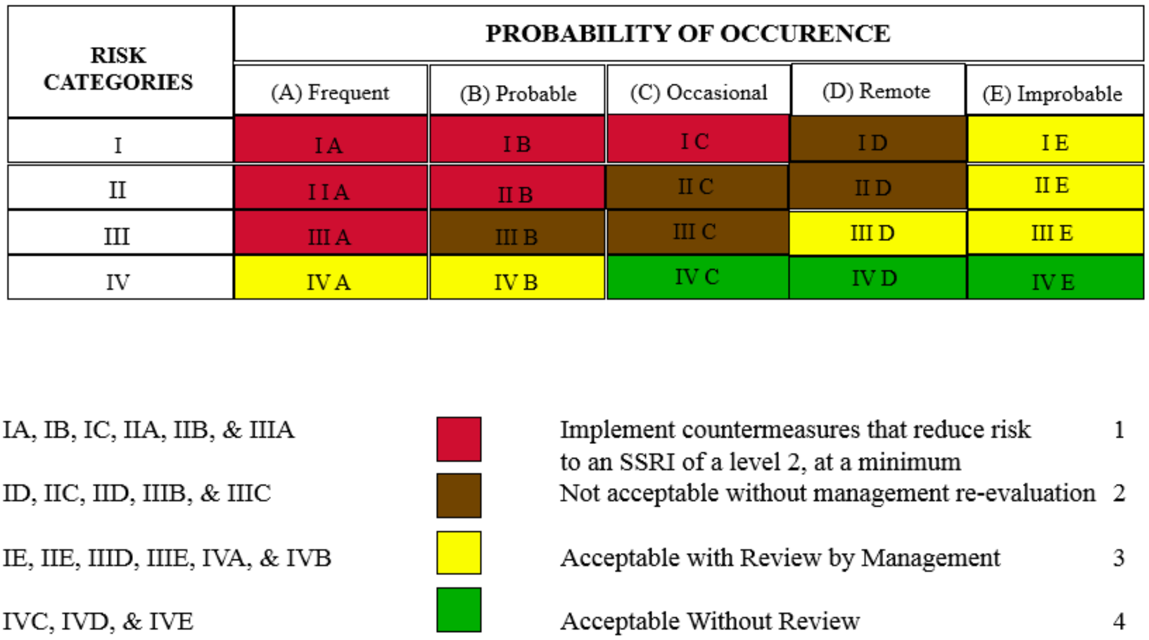
SEVERITY	CHARACTERISTICS
I	Loss of life, loss of critical proprietary information, loss of critical assets, significant impairment of mission, loss of system. ($10 Million)
II	Severe injury to employee or other individual, loss of proprietary information and physical equipment resulting from undetected or unauthorized access, unacceptable mission delays, unacceptable system and operations disruption. ($1-10 Million)
III	Minor injury not requiring hospitalization, undetected or delay in the detection of unauthorized entry resulting in limited access to assets or sensitive materials, minor mission impairment, minor system and operations disruption. ($100K - $1 Million)
IV	Less than minor injury, asset loss, access to sensitive materials, system or operations disruption. ($10K - $100K)

Figure 12: Undesired Event Severity Categories



PROBABILITY CATEGORY	LEVEL	SPECIFIC EVENT
A	Frequent	Possibility of Repeated Incidents (1 or more year)
B	Probable	Possibility of Isolated Incidents (1 in 5 years)
C	Occasional	Possibility of Occurring Sometime (1 in 10 years)
D	Remote	Not Likely to Occur (10% in 10 years)
E	Improbable	Practically Impossible 1% in 10 years

Figure 13: Undesired Event Probability Categories



RISK CATEGORIES	PROBABILITY OF OCCURENCE				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	🟥 I A	🟥 I B	🟥 I C	🟫 I D	🟨 I E
II	🟥 II A	🟥 II B	🟫 II C	🟫 II D	🟨 II E
III	🟥 III A	🟫 III B	🟫 III C	🟨 III D	🟨 III E
IV	🟨 IV A	🟨 IV B	🟩 IV C	🟩 IV D	🟩 IV E

IA, IB, IC, IIA, IIB, & IIIA	🟥	Implement countermeasures that reduce risk to an SSRI of a level 2, at a minimum	1
ID, IIC, IID, IIIB, & IIIC	🟫	Not acceptable without management re-evaluation	2
IE, IIE, IIID, IIIE, IVA, & IVB	🟨	Acceptable with Review by Management	3
IVC, IVD, & IVE	🟩	Acceptable Without Review	4

Figure 14: Risk Assessment Matrix

2.12 Step 6: Risk Evaluation

2.12.1 The Application of Countermeasures

- Corrective actions that describe the methods used to eliminate the causes or minimize the effects of each vulnerability.

- Once those methods are identified, the Team must recalculate the safeguards and security risk index from the risk scenario worksheets.

(In some instances, the recalculation may have to wait for a system re-design.)

2.12.2 Ranking

- Not all recommendations are equal. Prioritization by team is critical in assisting management in the development of implementation plans. We use a weighted sum calculation algorithm, for each recommendation, with the following attributes (10=most important):
  - Importance of the scenario, 1 to 10
  - Importance of recommendation in the scenario, 1 to 10
  - Importance of the recommendation to overall project, 1 to 10
  - Degree of difficulty (10=easy, 1=very difficult)
  - If two recommendations are tied, scribe makes initial decision in DRAFT report

2.13 Exit Briefing

- Interactive atmosphere.
- Capture management thoughts and align with pre-assessment expectations.
- Highlight savings opportunities from start to finish.
- Provide a significant level of detail so as to avoid surprises that may appear in later reports.
- Address resolution steps.
- Identify local ownership and next steps.

3.0 EXECUTION PLANNING

3.1 Introduction

Risk Management is the technical procedure for identifying and evaluating threats and vulnerabilities and for balancing risks against the cost of countermeasures. Safeguards and Security (S&S) Risk Assessments are conducted by multidisciplined teams evaluating a wide array of organizational operations (and security relationships with those operations) to assess the probability and severity of undesired events on ________________ assets in ________ and develop countermeasure recommendations that mitigate identified risks in a cost effective and consistent manner.

3.2 Scope

The Risk Assessment Team will review facilities in accordance with the _____________best practices and related guidance, conduct detailed data gathering, interview a range of __________ personnel, develop and evaluate related risk scenarios to provide recommended countermeasures to reduce, mitigate, or eliminate identified risks. After gathering data, the deliberations will take place at the __________________. The Team will develop a threat characterization statement as the foundation to assess appropriate levels of protection and risk mitigation for activities over a ten-year period. Emphasis will be placed on identifying higher risk scenarios and focus on cost-effective physical and procedural countermeasures. All project information shall be considered company proprietary.

3.3 Objectives

- Review existing assets to assess appropriate levels of protection,
- Review current and projected safeguards and security systems and evaluate implementation,
- Consider developing strategic security best practices that would evolve into global baseline standards,
- Evaluate opportunities to use one project to leverage and optimize security at multiple assets,
- Review command and control functions,
- Consider ways to integrate multiple site into one central command and control center,
- Assess technical security equipment placement and functionality,
- Assess personnel security;
- Assess information security—e.g. consider protective measures for proprietary information and

intellectual property,

- Evaluate security systems and protective force allocation,
- Review current and emerging threats to assets ten years into the future;
- Develop a Threat Characterization Statement (TCS)
- Provide management with a means to accept, reduce or eliminate risks via a security decision-making framework that includes cost-benefit analysis.

3.4 Methodology

This effort will use the Department of Homeland Security (DHS) approved safeguards and security risk assessment methodology "Qualitative Risk Assessment through Risk Scenario Analysis." This methodology has been used by teams over 500 times on a wide array of organizations and operations. The methodology relies upon a multi-disciplined team of subject matter experts to develop undesired event scenarios and make recommendations to reduce risk, a technique that is consistent with the requirements of DHS (for petroleum, nuclear, and chemical sectors).

This full scope S&S risk assessment will provide both hard and electronic copy to facilitate implementation planning and related follow-up tracking system. Individual interviews will focus on questions derived from a standard question format and generally take one hour. The Team will be subdivided so interviews can take place in parallel. Suggested interviewees will include staff from facility organizational elements as well as contractor personnel.

3.5 Team Composition

The methodology requires 5 to 8 full time team members — multi-disciplined mid-level managers are optimal.

3.6 Team Schedule

This full scope Risk Assessment will begin with the security component of the team arriving in ______________________.

3.7 Information Requirements

In addition to information derived from interviews the Team will also examine quantitative data, to include:

- Facility summary information
- Incident data
- Building plans and operations areas plats
- Overall Project and support facility operations
- Office and facility security
- Technical security equipment repair and downtime data
- Personnel security
- Site security costs data
- Emergency management systems

3.8 Logistics

The security component of the team should plan on arriving in_____________. Local staff will arrange lodging for out of town Team members. *All Team members are advised to bring safety shoes/boots for familiarization tours. Safety information will be sent to team members in advance of their arrival.*

The ROUGH DRAFT report will be prepared and distributed for Team review on _________, with the FIRST DRAFT report to the assessment owner for operational and departmental review expected on ___________. The FINAL DRAFT report should be issued by ____________ but issuance will depend upon senior management approvals and related reviews.

All Team members should familiarize themselves with the S&S risk management methodology. Team members will be expected to devote themselves full-time to risk assessment activities. Telephone usage (fixed and cell) will be RESTRICTED during deliberations. Specific breaks for phone use will be scheduled, but group integrity must be maintained during deliberations. Out of town Team members will depart on ___________ unless otherwise excused.

Facilitator: _______________________________

Travel and Accommodations: Team members noted below will coordinate all travel through the facilitator.

Schedule of Interviewees and Logistics

Date	Time	Team	Interviewee Name & Title	Location
	18h00	Out of town members	Coordination meeting	
	07h30-08h00	ALL	Pre-assessment team coordination meeting	
	08h00-12h00	ALL	Travel to Abuja	
	12h00-13h00	ALL	Lunch	
	13h00-15h00	ALL	Tour of	
	15h00 15h30	Team 1	Interview 1	
	15h00 15h30	Team 2	Interview 2	
	15h30 16h00	Team 1	Interview 3	
	15h30 16h00	Team 2	Interview 4	
	16h00-18h00	ALL	Tours of _____________	
	18h00-18h30	ALL	Data reviews	
	18h30-19h00	ALL	Team exchange of information	
	19h00-		Dinner	
	07h30-08h00	ALL	Team coordination meeting	
	08h00-08h30	Team 1	Interview 5:	
	08h00-08h30	Team 2	Interview 6:	
	08h30-09h00	Team 1	Interview 7:	
	08h30-09h00	Team 2	Interview 8:	
	09h00-09h30	Team 1	Interview 9:	
	09h00-09h30	Team 2	Interview 10:	
	09h30-10h30	ALL	Team exchange of information	
	18h00-	ALL	Dinner	
	07h30-08h00	ALL	Team coordination meeting	

Date	Time	Team	Interviewee Name & Title	Location
	11h30- 12h30	ALL	Lunch	
	12h30- 15h00	ALL	Tour facilities and project locations	
	15h00 15h30	Team 1	Interview 11	
	15h00 15h30	Team 2	Interview 12	
	15h30 16h00	Team 1	Interview 13	
	15h30 16h00	Team 2	Interview 14	
	16h00 16h30	Team 1	Interview 15	
	16h00 16h30	Team 2	Interview 16	
	16h30- 17h30	ALL	Team exchange of information	
	17h30			

Threat Characterization Statement

(Classified - to be distributed with final draft of execution plan**)**

See Element 2 of the ISMS

3.9 Risk Assessment Methodology

3.9.1 System Concept

Security is the application of special technical and managerial skills to the systematic, forward-looking identification and control of risks throughout the life cycle of a project, program, or activity. The concept calls for vulnerability analyses and vulnerability-control actions. The emphasis is on preventing threats by systematically identifying vulnerabilities and eliminating or controlling the associated risks. To ensure that the security program is designed and implemented in a manner that attains the desired high level of protection, it is necessary to conduct vulnerability analysis and resolution. This approach reduces loss to the lowest practical levels. In addition, it provides guidance by identifying the most critical assets. The vulnerability resolution process depicted in Figure 15 and Figure 20. presents the process that should be followed to ensure the highest practical degree of security support.

3.9.2 Vulnerability Resolution Process

3.9.2.1 System Definition

The first step in the vulnerability resolution process is to define the system to be analyzed. This definition is presented in terms of the major elements that make up the system: equipment, procedures, people, and environment. Knowledge and understanding of the relationship between the individual system elements, asset priorities and threat elements are essential to the analysis process.

3.9.2.2 Identification of Vulnerabilities

The second step in the vulnerability resolution process involves the identification of vulnerabilities and the determination of their nature and source. In this process, only a portion of the total number of vulnerabilities present in a system or subsystem will be identified. The extent and quality of the vulnerability analysis will influence the total number of vulnerabilities identified.

Define the Safeguards and Security System

- Define future physical and functional characteristics (assets) and understand and evaluate the people, procedures, facilities and equipment, and the environment (threat assessment).

Identify Vulnerabilities

- Pair the assets to the threats
- Identify vulnerabilities and undesired events — develop scenarios
- Determine the causes of vulnerabilities

Assess Vulnerabilities

- Determine severity
- Determine probability
- Decide to accept, eliminate, or control associated risk

Resolve Vulnerabilities

- Make countermeasure recommendations to:
    - Eliminate Risk
    - Control Risk
- Or assume the associated risk

Follow Up

- Monitor for effectiveness
- Monitor for unexpected vulnerabilities

Figure 15: Summary of the Vulnerability Resolution Process

There are five basic methods used to identify vulnerabilities:

1. Evaluation of data developed during direct surveys and evaluations;
2. Evaluation of historical data from related incidents and/or system operating experience;
3. Scenario development and judgment by knowledgeable individuals;
4. Examination of previous risk assessment reports; and
5. Formal vulnerability analysis techniques.

3.9.2.3 Assess Vulnerabilities

The third step in the vulnerability resolution process is to assess the identified vulnerabilities in terms of their severity or consequence and their probability of occurrence. Figure 16 .and Figure 17 show ranking criteria endorsed by the U.S. Government Accountability Office (GAO) and the U.S. Department of Energy (DOE). Figure16 contains four severity categories and provides a general description of the characteristics that define the "worst case" event. Figure 17 lists the qualitative ranking of probability categories and describes the characteristics of each level.

The Risk Index (RI) presented in Figure 18 is a value derived by considering both the severity and probability of a compromise. The RI presents vulnerability analysis data in a format that assists the decision-maker in determining whether the vulnerabilities should be eliminated, controlled, or accepted. The RI also provides a basis for logical management decisions that consider both the probability of occurrence and the severity of consequences. This approach can maximize the effective use of available resources.

It should be noted that the potential severity of a compromise could not be reduced unless the vulnerability is completely eliminated through a major redesign.

However, the probability, and therefore the associated risk, can be greatly reduced by the incorporation of controls, prophylaxis, evaluation systems, procedures, training or a combination thereof. Reducing the probability was the primary goal of the risk assessment team.

3.9.2.4 Vulnerability Resolution

After the vulnerability analysis is complete, the vulnerabilities can be resolved by deciding either to accept the risk associated with the vulnerability, or to eliminate or control the source of the vulnerability.

Reference: Adapted from the Risk Assessment matrix of MIL-STD 882C

Severity	Characteristics
I Critical	• Loss of critical proprietary information • Loss of essential assets • Significant impairment of mission • Loss of system • Extended national or world-wide news coverage • Loss of more than $10M USD
II Serious	• Serious loss of proprietary information and physical equipment • Unacceptable mission delays • Extended local news coverage or one national / international mention • Unacceptable system and operations disruption • Loss of $1M to $10M USD
III Moderate	• Undetected or delay in the detection of unauthorized entry resulting in moderate loss of assets or sensitive materials • Moderate mission impairment • One time mention on local news • Moderate system and operations disruption • Loss of $100K-$1M USD
IV Minor	• Undetected or delay in the detection of unauthorized entry with access to sensitive materials • Minor system or operations disruption • Loss of $10K to $100K USD

Figure 16: Undesired Event Severity Categories

Reference: Adapted from the Risk Assessment matrix of MIL-STD 82C

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)

Figure 17: Undesired Event Probability Categories

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**	**IIE**
III	**IIIA**	**IIIB**	**IIIC**	**IIID**	**IIIE**
IV	**IVA**	**IVB**	**IVC**	**IVD**	**IVE**

Risk Category (RC)		Risk Index (RI)	Risk Number
IA, IB, IC, IIA, IIB, & IIIA	🟥	Implement countermeasures that reduce risk to an SSRI of a level 2, at a minimum.	1
ID, IIC, IID, IIIB, & IIIC	🟫	Not acceptable without management re-evaluation.	2
IE, IIE, IIID, IIIE, IVA, & IVB	🟨	Acceptable with Review by Management.	3
IVC, IVD, & IVE	🟩	Acceptable Without Review.	4

Figure 18: LSSQRA Risk Assessment matrix

Various methods can be used to reduce the risk to an acceptable level. Figure 5 presents a vulnerability reduction precedence process that can be used to determine the extent and nature of preventive actions that can be taken to reduce the risk to an acceptable level. Resolution strategies (or countermeasures[2]) are listed below in order of preference.

Design to Eliminate Vulnerabilities

This strategy generally applies to the design and acquisition of new subsystems and equipment or the expansion of existing subsystems; however, it can also be applied to any change in equipment or individual components.

Design to Minimize Vulnerabilities

A major goal during the subsystem design process is to include features that are fail-safe or have capabilities to handle contingencies through redundancies of critical elements. Complex features that could increase the likelihood of a loss should be avoided.

Safeguards Devices

Known vulnerabilities that cannot be eliminated or minimized through design may be controlled through the use of appropriate safeguards devices. The use of such countermeasures can help reduce risk to an acceptable level. Safeguards devices must be integrated into a part of the safeguards and security system.

Access Control and Warning Devices

Warning devices and access control measures for timely detection of conditions that precede the actual occurrence of the event.

Procedures and Training

Where it is not possible to totally eliminate or control safeguards or security-related vulnerabilities using one of the above methods, detailed procedures for responding to the resulting undesired event should be developed and formally implemented. These procedures should be standardized and used in all protective system tests, operations, and maintenance activities. Personnel should receive proper training to enable them to carry out these procedures.

Vulnerability Acceptance

Where it is not possible to reduce the probability of safeguards or security vulnerabilities by any means, a decision must be made to either accept the risk associated with the vulnerability or reevaluate the requirements for the particular asset being protected.

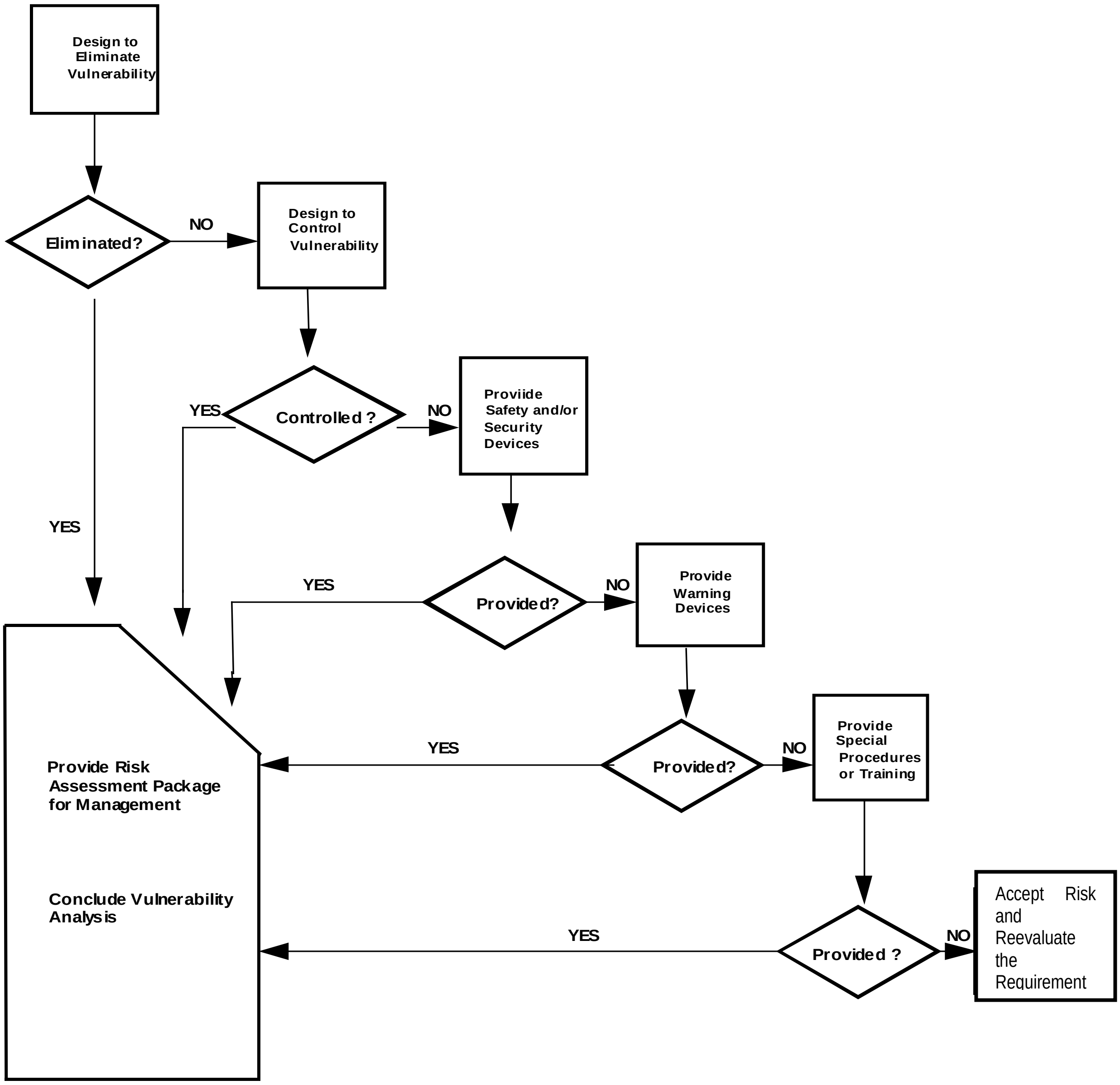
3.9.2.5 Risk Assessment Worksheet

The flowchart in FIgure depicts the process to be used by the Risk Assessment Team to assess and evaluate risk. The Team first develops scenarios and then in the assessment phase evaluates existing safeguards, conducts a cause-effect analysis, and calculates risk using the above probability/severity tables and the risk matrix. In the evaluation phase the team evaluates countermeasures to mitigate the risks and then recalculates risk assuming implementation of the countermeasures.

[2] A "countermeasure" is defined as any action or series of actions that may be taken to reduce the risk of an undesired event and/or the frequency of its occurrence.

3.9.2.6 Follow-up

The last step in the vulnerability resolution process is follow up. It is necessary to monitor and audit the effectiveness of recommended countermeasures and ensure that they do not introduce any new vulnerability. A vulnerability analysis should be conducted to identify and resolve any new vulnerability that may occur whenever changes are made to any of the system elements (equipment, procedures, people, or environment).


Design to Eliminate Vulnerability
Eliminated?
NO
Design to Control Vulnerability
YES
Controlled ?
YES
NO
Proviide Safety and/or Security Devices
YES
Provided?
NO
Provide Warning Devices
YES
Provided?
NO
Provide Special Procedures or Training
YES
Provided ?
NO
Accept Risk and Reevaluate the Requirement
Provide Risk Assessment Package for Management
Conclude Vulnerability Analysis

Source: Roland & Moriarty, *System Safety Engineering and Management*, 1983.

Figure 19: Vulnerability Reduction Precedence Process

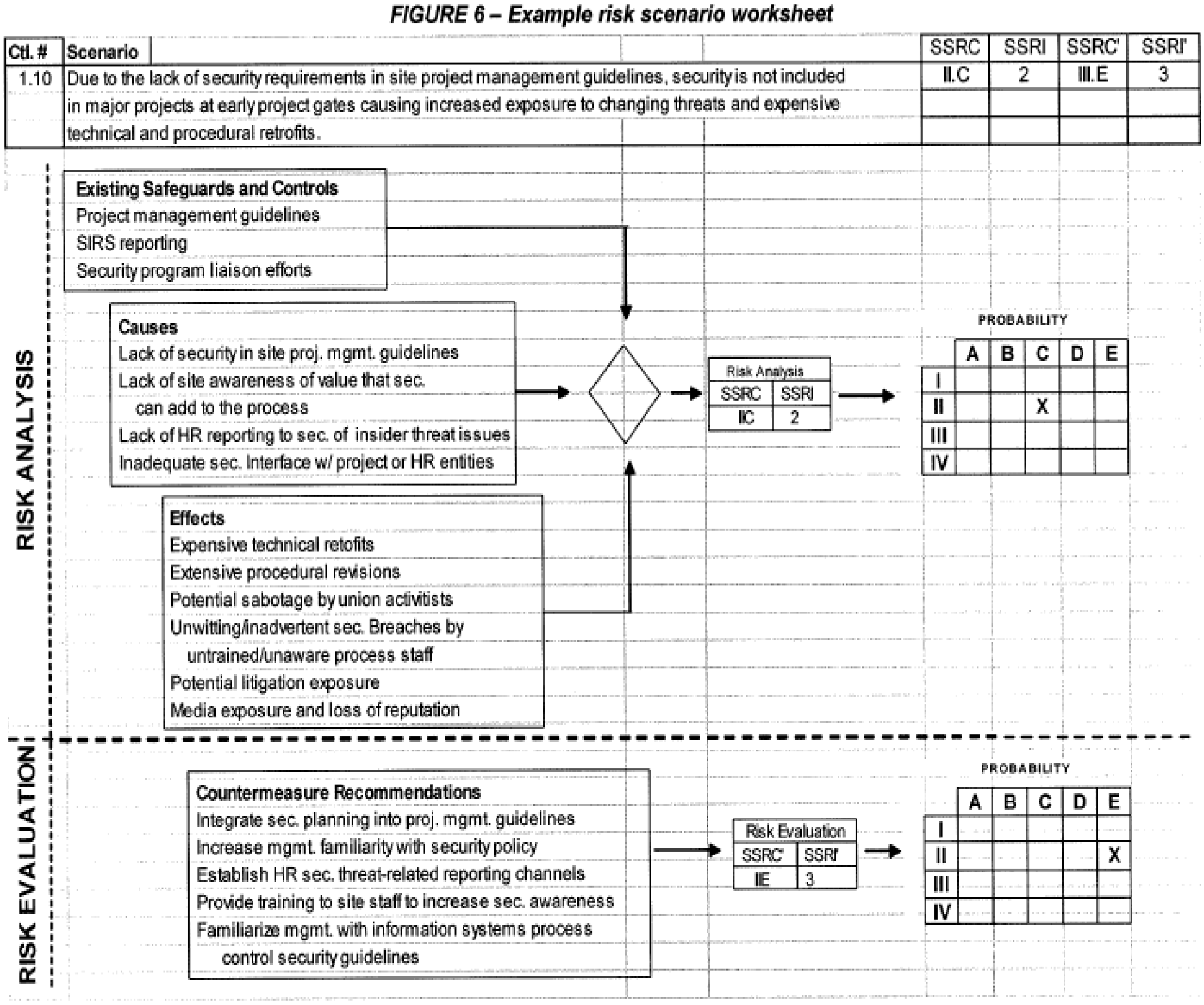


FIGURE 6 – Example risk scenario worksheet

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

RISK ANALYSIS

Existing Safeguards and Controls
Project management guidelines
SIRS reporting
Security program liaison efforts

Causes
Lack of security in site proj. mgmt. guidelines
Lack of site awareness of value that sec. can add to the process
Lack of HR reporting to sec. of insider threat issues
Inadequate sec. Interface w/ project or HR entities

Effects
Expensive technical retofits
Extensive procedural revisions
Potential sabotage by union activitists
Unwitting/inadvertent sec. Breaches by untrained/unaware process staff
Potential litigation exposure
Media exposure and loss of reputation

Risk Analysis

SSRC	SSRI
IIC	2

PROBABILITY

	A	B	C	D	E
I					
II			X		
III					
IV					

RISK EVALUATION

Countermeasure Recommendations
Integrate sec. planning into proj. mgmt. guidelines
Increase mgmt. familiarity with security policy
Establish HR sec. threat-related reporting channels
Provide training to site staff to increase sec. awareness
Familiarize mgmt. with information systems process control security guidelines

Risk Evaluation

SSRC'	SSRI'
IIE	3

PROBABILITY

	A	B	C	D	E
I					
II					X
III					
IV					

Figure 20: Example risk scenario worksheet