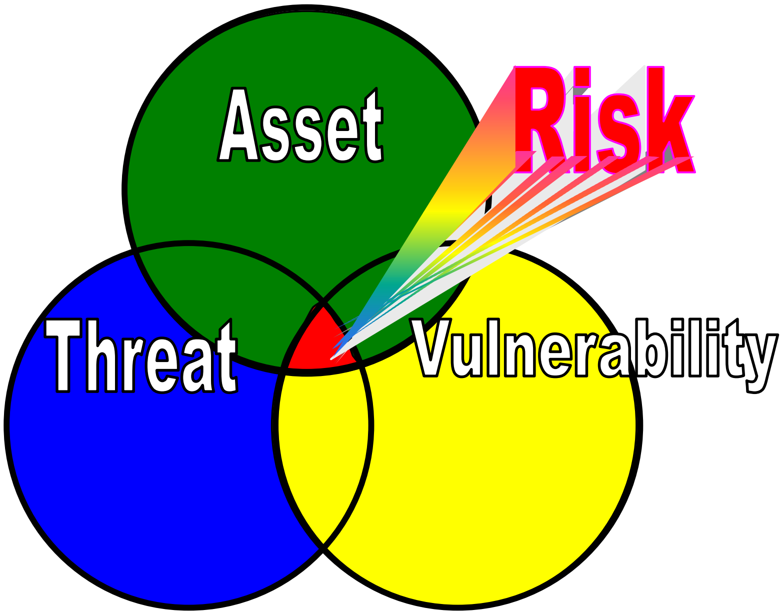
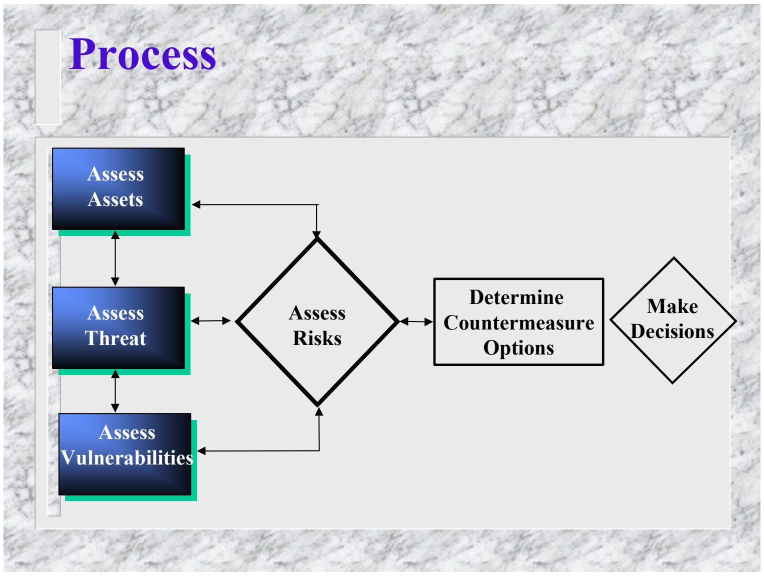
Risk Management Handbook

1999



Introduction

Risk management is "the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost." The analytical risk management (ARM) process outlined in the annex can be tailored and applied to any organization or assessment. The process includes the following activities:



"The process begins with an assessment of the value of the information, the degree of a specific threat, and extent of the vulnerability. These three factors determine risk. A decision is then made as to what level of risk can be accepted and which countermeasures should be applied. Such a decision involves a cost-benefit analysis, giving decision makers the ability to weigh varying risk levels against the cost of a specific countermeasure." - Quotation taken from: The Diplomatic Security Risk Management Policy

This appendix describes in detail the analytical risk management process utilized by the IOVAD. The process consists of five steps that result in the identification of risk associated with a vulnerability and effective countermeasures that a commander can apply to mitigate the risk.

Outline of Analytical Risk Management Steps

Determine critical information requiring protection.
Identify undesirable events and expected impacts
Value/prioritize information based on consequence of loss

Step 1. Identify assets and loss impacts

Step one starts in the planning phase and continues into the execution phase. Hopefully the critical information and undesirable events can be identified during planning most likely the commander and staff will identify them during the execution phase.

Step 2. Identify and characterize the threat

Identify threat categories and potential adversaries

Assess intent and motivation of adversary

Assess capability of adversary

Determine frequency of threat-related incidents

Estimate degree of threat relative to each item of critical information and undesirable event

Step 2 begins in the planning phase with the formal request for a threat assessment through the LIWA IT&S Division. Many times detailed threat information is not available and a generalized threat definition and rating has to be used.

Identify existing countermeasures and their level of effectiveness

Estimate the degree of vulnerability relative to each asset and threat

Step 3. Identify and analyze vulnerabilities

The data collected during the execution phase identifies the vulnerabilities associated with the units Information Operations.

Step 4. Assess risk

Estimate degree of impact relative to each critical asset
Estimate likelihood of attack by a potential adversary/threat
Estimate the likelihood that a specific vulnerability will be exploited.
Determine your relative degree of risk
Prioritize risks based in integrated assessment

A preliminary assessment is completed in the execution phase and included in the commanders out-briefing. The assessment is then reviewed and finalized ad included in the final written report submitted to the assessed unit.

Step 5. Identify countermeasure, costs, and tradeoffs

Identify potential countermeasures to reduce vulnerabilities
Identify countermeasure capability and effectiveness
Identify countermeasure cost
Conduct countermeasure cost-benefit and trade-off analysis
Prioritize options and prepare recommendations for the commander

The completed risk assessment submitted with the final report includes mitigation techniques for the unit to implement.

Definition of Key Terms

Assets

- Command & Control Systems
- Operational Activities

Undesirable Impact

Identifies the undesirable event and the expected impact to the information and overall operation. The narrative explanation clearly states what the undesirable event and defines the levels of impact.

Threat.

Threat can be defined as any indication, circumstance, or event with the potential to cause loss, or damage to an asset. It can also be defined as the intention or capability of an adversary to undertake actions that would be detrimental to critical assets. Threat is an attribute of an adversary. The threat may be specifically identified or categorized in general such as; Foreign Intelligence Service, Terrorist, Insider, Criminal, Foreign Military, Political, or other. Environmental condition (Natural Disaster) is an example of other. The definition identifies the threat's existence, capability, intent, and probability of action against the asset.

Adversary

Is an individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to critical assets. These include intelligence services of the host nation or third party nations, political or terrorist groups, criminal and hacker groups, and private interests.

Vulnerability**.**

Vulnerability ratings describe the severity of the vulnerability. The vulnerability can be specifically identified or stated in general terms, i.e., No firewall established between Command Router and PBX Switch or poor access control procedures.

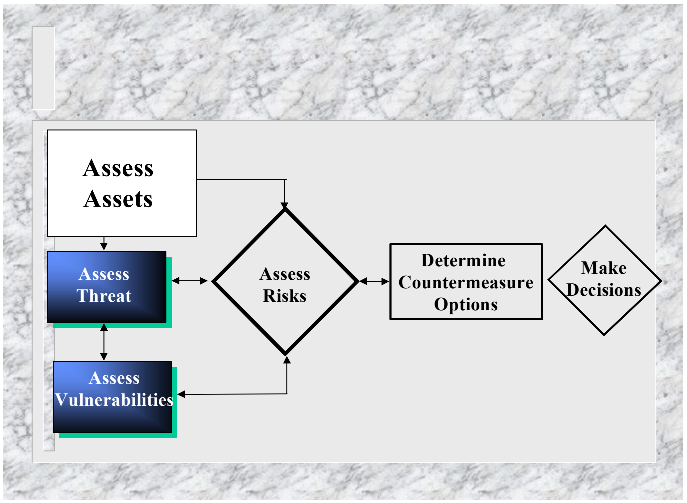
Risk.

Define the overall risk. The definition states in one sentence the overall risk to the asset with the identified threat and vulnerabilities.

Countermeasure

Is an action taken or a physical entity used to reduce or eliminate one or more vulnerabilities. The cost of a possible countermeasure may be monetary but may also include man-hours, or reduce operational efficiency.

Step 1. Identify Assets and Loss Impacts



Assets are identified during the initial coordination and are clearly identified by the supported commander's purpose, scope, and intent. IO assets are:

- Command & Control Systems**.** Automated Information and Communications systems that provide data for the commander that is available on demand, maintains integrity, and confidentiality during manipulation, transmission and storage.
- Operational Activities other than Automated Information and Communications system that comprise IO. These are the pillars of IO; PSYOP, Deception, OPSEC, Electronic Warfare, Physical Destruction and Civil and Public Affairs. All of these activities communicate information in one form or another. These systems release information, intentionally or as a function of the activity. The accuracy and availability of this information must be controlled**.**

Asset Survey

You can gather information about critical assets from a variety of sources:

☒ **Commander**

☒ **Senior Staff Officers**

☒ **IO Component Staff Officers, i.e. OPSEC Officer, PSYOP Planner, etc.**

☒ **Security Managers**

☒ **Information System Security Officers and System Administrators**

☒ **Existing Security Plans, SOPs, and Policies**

☒ **Open Source Information**

Ask the following questions to clarify the assets:

Clarification of Assets
What critical mission activities/operations take place at this unit at this time?
What units, other personnel, and visitors are involved in the activity/operation? What relationship do they have to the critical assets?
What critical/sensitive information (classified and unclassified) is located at the unit?
What critical/valuable equipment is located at the unit?
Where are the assets located?
Describe the expected impact if the event were to occur.

Table 19. Clarification of Assets

Identify specific undesirable events and the potential impacts if the events were to occur. For example, you need to protect the exact time and location of the main attack; the undesirable event would be the adversary obtaining this information. The impact could be mission failure. Answer the following questions to assess loss impacts for any asset:

Impact Assessment
How does obtaining this information help the adversary attain its goals?
What would we lose?
Is this asset still valuable to us once it has been compromised?
What did it cost us to develop the asset?
What is the impact on soldiers lives, the mission, and the National security?

Table 20. Impact Assessment

For every observation determine the impact of the undesirable event, the answers to the above questions should clarify the appropriate rating. The matrix below will assist in identifying the correct level.

Undesirable Events					
Mission Failure, Loss of Life, Mass Casualties	Loss Of Classified Data That Impairs Operations For An Indefinite Amount Of Time	Loss Of Data, Service, Or Systems That Impairs Operations For An Indefinite Amount Of Time	Compromise Or Corruption Of Data Or Lose Of Resources That Impairs Operations For A Limited Amount Of Time	Little To No Impact On Human Life Or Continued Operations	Overall Impact Level
YES	Yes/No	Yes/No	Yes/No	Yes/No	Critical
	YES	Yes/No	Yes/No	Yes/No	High
	YES/No	Yes/No	Yes/No	Yes/No	High
			YES	Yes/No	Medium
				YES	Low

Table 21 Impact Matrix

Impact Rating Criteria

The following definitions and numerical ratings have been established. There is a degree of subjectivity within the rating scales. If the data clearly indicates a grave consequence then a high critical rating is justified. If the data is in the gray area could be a low critical of in the upper side of a high rating, error on the high side and select the low side of critical. Determine the appropriate rating and enter the definition and numerical rating in the 'Impact Rating' column of worksheet 8 for every observation.

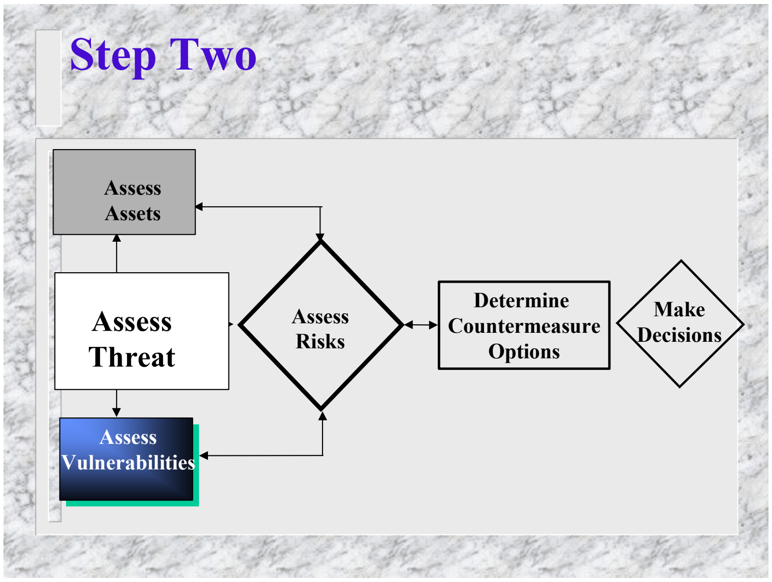
- Critical – Grave Consequence. The intrusion, disruption and or destruction of any system(s) or activity ultimately result in the failure to accomplish the assigned mission, loss of life or mass casualties. (50 - 100)

- High -- Serious consequence. The compromise or corruption of classified or sensitive data, denial or loss of service of one or more information systems, the manipulation of data or degradation of logistical support or facilities that could impair operations for an indefinite amount of time (13 - 50)

- Medium – Moderate Consequence. Actions resulting in the compromise or corruption of sensitive data, destruction or loss of costly equipment or degradation of any logistics capability that would impair operations for a limited period of time. (3 - 13)

- Low -- Indicates little or no impact on information operations, human life or the continuation of operations. (1 - 3)

Step 2. Assess Threats



Understanding threats requires an understanding of the adversaries' intentions and motives, as well as their capability to compromise critical assets. Because access to this type of information is often limited, this is generally the weakest link in the overall risk assessment process. During this step you identify and list the potential threats and any known or potential adversaries, that could put critical assets at risk.

Assess intent and motivation of the adversary.

Intent is determined for the most part by inference. You can infer intent through a set of questions regarding the adversary. For example:

Intent and Motivation
Does the adversary have a current or projected need for the asset?
Do they seek to deny us the use of the asset?
Have they demonstrated an interest by targeting similar types of assets?
Do they know that the asset exists and where it is located?
What are the specific goals and objectives of the adversary?
What does the adversary gain by achieving these goals?
Can the adversary achieve these goals by exploiting the asset?
Is the adversary's intent to obtain, damage, or destroy the asset?
Are there any other means for the adversary to obtain its goals?
Are the other means easier?
What specific events might provoke the adversary to act?
What might the adversary lose in attempting to exploit our asset?
To what degree is the adversary motivated to use its capability?

Table 22. Intent and Motivation

Write the answers to the questions from Table 22 in the note section of worksheet 1. List all of the adversaries in column one. Enter a yes or a no in columns 2, 3, and 4 based on the information you gathered using table 22. Enter the overall intent level in column 5 using one of the three combinations depicted below.

Intent Worksheet				
Adversary	Knowledge of Asset	Need	Demonstrated Interest	Overall Intent Level
# 1	Yes	Yes	Yes	High
# 2	Yes	Yes	No	Medium
# 3	Yes	No	No	Low

Worksheet 1. Intent

Determine the capability of the Adversary.

There are two distinct types of capability you will need to consider with respect to the adversary. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained. Consider the following:

Adversary Capabilities
Is the adversary aware that the asset exists?
Does he know where the asset is located?
What do we know about the adversary's HUMINT collection capabilities?
What do we know about the adversary's Technical (SIGINT, IMINT, MASINT) Capabilities?
What do we know about the adversary's Open Source (OSINT) capabilities?
What do we know about the adversary's methods of operation (Hacking networks, subversive activities, etc).

Table 23. Adversary Capabilities

Write the answers to the questions in Table 4 in the note section of worksheet 2. List the adversaries in column 1. Enter a high, medium, or low rating for each collection category based on the information gathered using Table 4. Assign an overall level rating based on the majority of the individual ratings, i.e. if three out of five answers are high then the overall rating is high.

Collection Capabilities						
Adversary	HUMINT	SIGINT	IMINT	MASINT	OSINT	Overall Level
#1	High	High	Med	Med	High	High
#2	High	Med	Low	Med	High	Med
#3	Med	Med	Low	Low	Med	Med
#4	Med.	Low	Low	Low	Med.	Low

Worksheet 2. Collection Capabilities

Determine the frequency of threat related incidents based on historical data.

A high frequency of threat-related incidents can indicate an increased likelihood that a similar incident may take place in the future, especially if capability and intent are high. Answer the following questions to determine history.

History
What do you know about the adversary's track records?
How many suspected incidents?
How may attempted incidents?
How many successful incidents?

Table 24. History

Write the answers to the questions in Table 24 in the note section of worksheet 3. List the adversaries in column 1. Enter the information gathered for each adversary in the appropriate columns, you do not need to put all of the data into these columns only enough to establish the bottom line history.

History			
Adversary	Suspected Incidents	Attempted Incidents	Successful Incidents
# 1	Hacking XYZ Network	Subversion of Government Employee	Interception of communications
# 2	Probe of ABC Network	Theft of Equipment	Imagery of facilities
# 3	Theft of Documents	Denial of Service attack	Purchase of classified documents

Worksheet 3. History

Assessing threats.

The threat level is a relative rating based on the best available information. Worksheet 4 is the compilation of the data entered in worksheets 1,2,and 3. List the adversaries in column 1 and enter the overall intent, Capability, and history for each adversary under the appropriate headings. Use the threat decision matrix to determine the correct level for the Rating column.

Intent	**Capability ****	**History**	**Level**
High	High/Medium/Low	Yes	Critical
High/Medium	High/Medium/Low	No	Critical
Medium	Medium	Yes	High
Medium/Low	Medium/Low	No	Medium
Low	Low	No	Low

Threat Decision Matrix

** Capability *can be obtained or provided by a third party*.

Threat Rating				
Adversary	Intent	Capability	History	Rating
# 1	High	High	Yes	Critical
# 2	Medium	Medium	Yes	High
# 3	Medium	Medium	No	Medium
# 4	Low	Low	No	Low

Worksheet 4. Threat Rating

Threat Rating Criteria

The following definitions and numerical ratings have been established. There is a degree of subjectivity within the rating scales. If the data clearly indicates a grave consequence then a high critical rating is justified. If the data is in the gray area could be a low critical of in the upper side of a high rating, error on the high side and select the low side of critical. Determine the appropriate rating and enter the definition and numerical rating in the 'Threat Rating' column of worksheet 8 for every observation.

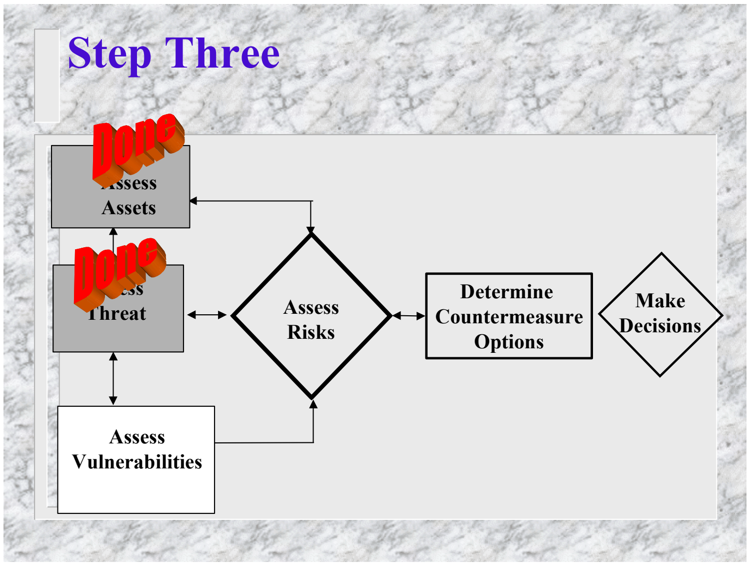
- Critical -- A definite threat exists against the assets and the adversary has both the capability and intent to launch an attack, and the subject or similar assets are targeted on a frequent and recurring basis. (75-100%)

- High -- A credible threat exists against the assets based on our knowledge of the adversary's capability and intent to attack the assets and based on related incidents having taken place. (50 - 74%)

- Medium -- There is a possible threat to assets based on the adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents. (25 – 49%)

- Low -- Little to no credible evidence of capability, intent, with any history of actual or planned threats against the assets. (0 – 24%)

Step 3 Assess Vulnerabilities



Vulnerability assessments help identify weaknesses that could be exploited to gain access to the asset. A vulnerability provides a pathway for creating an undesirable event and thus adverse impact. Using an adversary's perspective causes an analyst to develop attack scenarios that facilitate the identification of vulnerabilities. To determine where a vulnerability exists, first determine the possible paths the adversary may take. Next, determine what countermeasures are already in place and their relative degree of effectiveness in countering the assessed threats. Finally, identify and characterize the specific vulnerabilities that still exist given the current mix of countermeasures. Determining vulnerabilities also requires an understanding of adversary capabilities and their methods of operation.

Adversary Exploitation
What typically do adversaries exploit?
Intercept of unsecured telephone conversations and fax transmissions?
Faulty access control procedures?
Penetration of improperly secured information networks?
Trash collection?
Social engineering?
Co-opting an insider, or use of cleared host nation personnel?
Observation of activities and operations?

Table 25. Adversary Exploitation

There may be conditions that inhibit the effectiveness of existing countermeasures and the proper operation of the overall security. Some items to look for:

Existing Countermeasures
Obsolete, faulty, or improperly configured equipment.
Poor procedures or the lack of enforcement of good procedures.
Poor training of the end-user.
Human error.
Poor maintenance of equipment.
Insufficient manpower to effectively manage systems.
What type of protection do existing countermeasures provide (Deter, delay, detect, destroy, defend, defeat)?
What type of undesirable events do they guard against (Network penetration, surreptitious entry, technical implant, and unauthorized access to areas, or networks, theft of material)?
When are they effective – during which hours, activities, or phases of an operation?
Where are they effective? What areas do they cover?
What is the history of reported malfunctions?
What is the correlation of countermeasure effectiveness to security incident reports that may indicate that the countermeasure was defeated?

Table 26. Existing Countermeasures

The likelihood (probability) that a targeted vulnerability will be successfully exploited is a function of the number and effectiveness of the security countermeasures put into place.   The following worksheet can be used to track existing countermeasures and their effectiveness against undesirable events. A rating scale High, Medium, or Low is utilized to judge the effectiveness. Document the answers to Table 25 and 26 in the note section of worksheet 5, this will assist in determining the effectiveness of the existing countermeasures. List the existing countermeasures in column one if the countermeasure is designed to protect against the event, enter an effectiveness rating of the countermeasure for each undesirable event.

	Impact			
Exiting Counter-measure	Intrusion of, Disruption, or destruction of information systems	The compromise, corruption of classified or sensitive data, or the denial of service of an information system	Data manipulation, degradation of logistics support of facilities	Destruction or loss of expensive equipment
Doors, Lock, Bars		Medium	Medium0	Medium
Alarms, Sensors		Medium	Medium	
Guards			Medium	Low
Security Awareness	Low	Low	Low	Low
Passwords	Medium	Medium		
Firewalls, Intrusion Detection				

Worksheet 5. Countermeasure Effectiveness

Vulnerability data is linked directly to specific undesirable events. The following worksheet links vulnerabilities and their associated observations to undesirable events and the existing countermeasures. This is required to assess vulnerability levels associated with each undesirable event it will assist in the selection of countermeasures once the risk areas have been prioritized.

For every vulnerability/observation found, determine the appropriate impact column and list the existing countermeasures and their effectiveness in every cell.

Observation	Impact							
	Intrusion of, Disruption, or destruction of information systems		The compromise, corruption of classified or sensitive data, or the denial of service of an information system		Data manipulation, degradation of logistics support of facilities		Destruction or loss of expensive equipment	
Unauthorized Access to an information system								
Poor Physical Security							Locks Guards Awareness	Med . Low Low

Worksheet 6. Vulnerability-to-Event

Determine the vulnerability level.

The likelihood that a targeted vulnerability will be successfully exploited is a function of the number and effectiveness of the security countermeasures put into place. If few, ineffective, or no countermeasures are put into place, the likelihood that the exploitation will be successful is very high. To determine the vulnerability level for a given asset, you should answer the following three questions:

Vulnerability Level
Is the asset made vulnerable by a single weakness in the protective system?
Does the nature of the vulnerability make it difficult to exploit?
Is the vulnerability of the asset lessened by multiple, effective layers of security countermeasures?

Table 27. Vulnerability Level

Using the following decision worksheet to determine the relative vulnerability rating level. The data from Table 27 and Worksheets 5 & 6 support this matrix.

Vulnerable through Weakness?	Difficult to exploit weakness?	Multiple Layers of countermeasures?	Vulnerability Level
Single Weakness			
Vulnerable	Not Difficult		Critical
Vulnerable	Difficult		High
Not Vulnerable	Difficult		Medium
Multiple Weakness			
Vulnerable	Not Difficult	No Layers	Critical
Vulnerable	Difficult	Multiple Layers	High
Not Vulnerable	Not Difficult	Multiple Layers	Medium
Not Vulnerable	Difficult	Multiple Layers	Low

Worksheet 7. Vulnerability Rating Decision Matrix

Vulnerability Rating Criteria

The following definitions and numerical ratings have been established. There is a degree of subjectivity within the rating scales. If the data clearly indicates a grave consequence then a high critical rating is justified. If the data is in the gray area could be a low critical of in the upper side of a high rating, error on the high side and select the low side of critical. Determine the appropriate rating and enter the definition and numerical rating in the 'Vulnerability Rating' column of worksheet 8 for every observation.

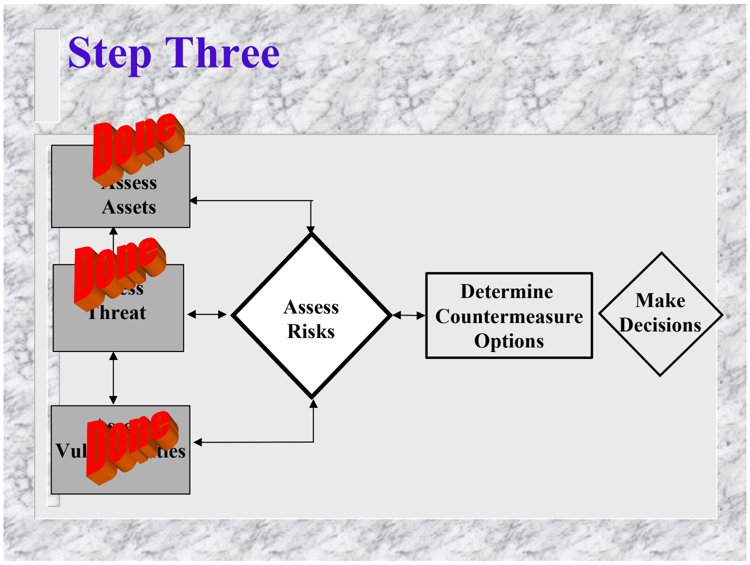
- **Critical** -- There are no effective countermeasures currently in place and all known adversaries would be capable of exploiting the asset. (75-100%)

- **High** -- Although there are some countermeasures in place, there are still multiple weaknesses through which many adversaries would be capable of exploiting the asset. (50-74%)

- **Medium** -- There are effective countermeasures in place, however some weakness does exist which a few known adversaries would be capable of exploiting. (25 - 49%)

- **Low** -- Multiple layers of effective countermeasures exist and few or no known adversaries would be capable of exploiting the asset. (1-24%)

Step 4 Assess the Risks



An undesirable event has an expected impact (I), while threat (T) and Vulnerability (V) are considered together to determine the probability of the undesirable event occurring. Risk Assessment (R) is the process of determining the likelihood (probability) of an adversary (T) successfully exploiting a vulnerability (V) and the resulting degree of damage or impact (I) on an asset. Thus the formula used is:

Risk = Impact x (Threat x Vulnerability)

Where vulnerabilities are great and the threat is evident the risk of exploitation is greater. This worksheet is filled in during the first three steps. Use the risk formula to calculate the overall risk and enter the number (Round to the nearest whole number) in the last column.

Impact Rating		**Threat Rating**		**Vulnerability Rating**		**Overall Risk**
(Definition)	#	(Definition)	#	(Definition)	#	#

Worksheet 8. Risk Calculation

The overall risk is defined with the following matrix. Locate the value calculated with the risk formula in the rating ranges, the resultant is the overall risk rating and definition.

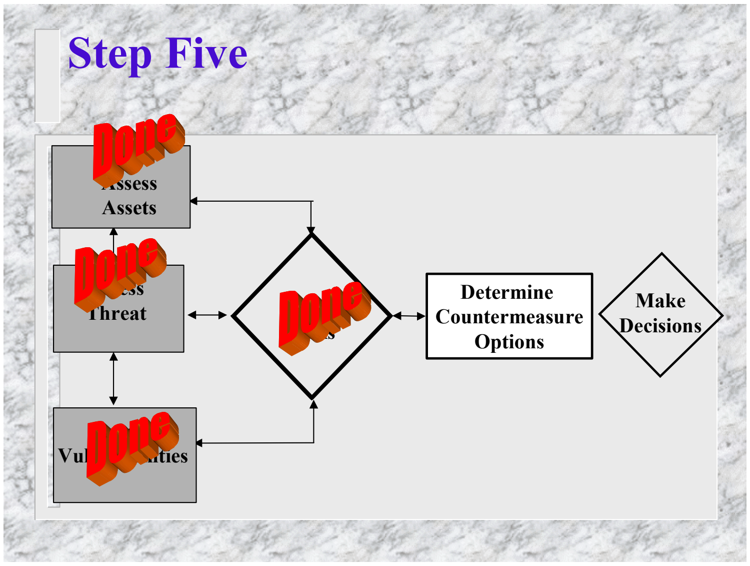
51-100 - Critical -- There is an exceptionally high risk of loss to the asset with resulting consequential impact.

11-50 - High -- There is a very high risk of loss to the asset with resulting serious impact.

2-10 - Medium -- There is some risk of loss to the asset with moderate impact

0-1 - Low -- There is little risk of loss to the asset with negligible impact.

Step 5. Identify Countermeasures



Based on the information obtained and analyzed in the previous steps, you can now identify countermeasures that reduce vulnerabilities linked to your unacceptable risks. You can choose to employ a single countermeasure or several countermeasures used in combination. Two or more countermeasures may work together in a compensating fashion to guard against a vulnerability that neither would adequately protect individually.

To identify potential countermeasures to reduce vulnerabilities consider the possible protection solutions for the risk scenarios. Identify the best solutions regardless of financial constraints. Countermeasures generally fit into one of the following three categories.

Procedures	Equipment	Personnel
OPSEC Procedures	Locking Mechanism	Appointed OPSEC Officer
Training Programs	Alarms/Sensors	System Administrators
Awareness Programs	Hardware/Software	ISSOs/ISSMs
Security Inspections/ Assessments	Access Control Devices, Badges	Guards
Contingency Planning	Shredders	Appointed Security Managers
Security SOP	Storage Containers	IO Officer
Network SOP	Operating Systems	

Table 29. Countermeasure Categories

Identify the cost of countermeasures.

Consider not only the cost of tangible materials, but also the on going operational costs. Keep in mind that written procedures are usually the least expensive type of security. Hardware is generally more expensive than written procedures, manpower costs are usually the most expensive, especially if the solution requires extensive training or contracting to obtain the skills. Every countermeasure has a cost associated with it that can be measured in terms of dollars, inconvenience, time, or personnel. The following chart will assist in identifying countermeasure packages.

When determining the dollar cost of a countermeasure, include the purchase price as well as life cycle maintenance. This may include installation, preventive maintenance, repair, warranty, and replacement costs.

When determining the cost of a countermeasure in terms of inconvenience consider whether the inconvenience caused is offset by the measure of risk reduction gained.

When determining the cost of a countermeasure in terms of time, include the time to implement or oversee the countermeasure and the time to prepare for implementation as well as any time required for training and follow-up.

When determining the cost of a countermeasure in terms of personnel required utilizing it, considering the number of staff needed as well as the skills, knowledge, and abilities of the personnel involved. Complete worksheet 9 to document improvements to existing countermeasures or the implementation of new countermeasures

Undesirable Event	Potential Countermeasures & Costs		
	Procedures	**Equipment**	**Personnel**
Intrusion of, Disruption, or destruction of information systems	Network Security SOP. Cost: Man-hours to develop the SOP, train operators and enforce policies	Network Firewall. Cost $20,000	Qualified Systems Administrator
	Procedures to secure the facility. Cost: Moderately Inconvenient	Photo Identification Badges for access control. Cost: $500	
The compromise, corruption of classified or sensitive data, or the denial of service of an information system	Security SOP for safeguarding classified information. Cost: Man-hours to develop the SOP, train operators and enforce policies		

Worksheet 9. Cost-Benefit Analysis

To complete worksheet 10 the process has to be repeated. Once a countermeasure is improved or implemented it has a three-fold effect. The impact of the undesirable event is reduced because the threat no longer has the capability to collect against the asset and the vulnerability is reduced due to multiple layers of effective countermeasures. Enter the vulnerability/observation in column one, the existing risk level in column two, the recommended countermeasure in column three. Complete a new worksheet 8 based on the new figures and recalculates the overall risk. Enter this new figure in the 'Mitigated Risk Level' column. Enter any clarifying comments in the last column.

Vulnerability/ Observation	Existing Risk Level	Recommended Mitigation Technique	Mitigated Risk Level	Comments
Failure to protect information				
Inadequate Perimeter Security	High	Develop and implement AISSP IAW AR 380-19	Medium	
Machines running vulnerable operating systems	Critical	Establish and enforce an approved list of software for all machines	High	

Worksheet 10. Risk Mitigation

Tab 1 (Intent Worksheet) to Risk Assessment Guide

Intent Worksheet				
Adversary	Knowledge of Asset	Need	Demonstrated Interest	Overall Intent Level

Notes:

Tab 2 (Collection Capability Worksheet) to Risk Assessment Guide

Collection Capabilities						
Adversary	HUMINT	SIGINT	IMINT	MASINT	OSINT	Overall Level

Notes:

Tab 3 (Adversary History Worksheet) to Risk Assessment Guide

History			
Adversary	Suspected Incidents	Attempted Incidents	Successful Incidents

Notes:

Tab 4 (Threat Rating Worksheet) to Risk Assessment Guide

Threat Rating				
Adversary	Intent	Capability	History	Rating

Notes:

Tab 5 (Countermeasure Effectiveness Worksheet) to Risk Assessment Guide

Exiting Counter-measure	Impact			
	Intrusion of, Disruption, or destruction of information systems	The compromise, corruption of classified or sensitive data, or the denial of service of an information system	Data manipulation, degradation of logistics support of facilities	Destruction or loss of expensive equipment

Notes:

Tab 6 (Vulnerability-to Event Worksheet) to Risk Assessment Guide

Vulnerability/ Observation	Impact							
	Intrusion of, Disruption, or destruction of information systems		The compromise, corruption of classified or sensitive data, or the denial of service of an information system		Data manipulation, degradation of logistics support of facilities		Destruction or loss of expensive equipment	
Unauthorized Access to an information system								
Poor Physical Security							Locks Guards Awareness	Med . Low Low

Notes:

Tab 7 (Vulnerability Rating Worksheet) to Risk Assessment Guide

Vulnerable through Weakness?	Difficult to exploit weakness?	Multiple Layers of countermeasures?	Vulnerability Level
Single Weakness			
Multiple Weakness			

Notes:

Tab 8 (Risk Calculation Worksheet) to Risk Assessment Guide

Impact Rating		Threat Rating		Vulnerability Rating		Overall Risk

Notes:

Tab 9 (Cost Benefit Analysis Worksheet) to Risk Assessment Guide

Undesirable Event	Potential Countermeasures & Costs		
	Procedures	**Equipment**	**Personnel**

Notes:

Tab 10 (Risk Mitigation Worksheet) to Risk Assessment Guide

Vulnerability/ Observation	Existing Risk Level	Recommended Mitigation Technique	Mitigated Risk Level	Comments

Notes: