Risk Management for DoD Security Programs
Student Guide

Welcome to Risk Management for DoD Security Programs. The goal of this course is to provide security professionals with a risk management process that incorporates five steps: asset assessment, threat assessment, vulnerability assessment, risk assessment, and countermeasure determination.

Practical Application

A corresponding job aid **(Risk Management – Tables, Charts & Worksheets)** is available in the course resources link which provides examples of each of the tables, charts and worksheets that are referenced in the courseware and are an integral part of the risk management process. This job aid can be used as quick reference material or as a starting point in your own risk management analysis.

Introduction

Rapid changes in the political, social, economic, and technological arenas have caused protection to become more complex, while resources for security have become more restricted. The risk management process provides a systematic approach for acquiring and analyzing the information necessary to protect assets and allocate security resources.

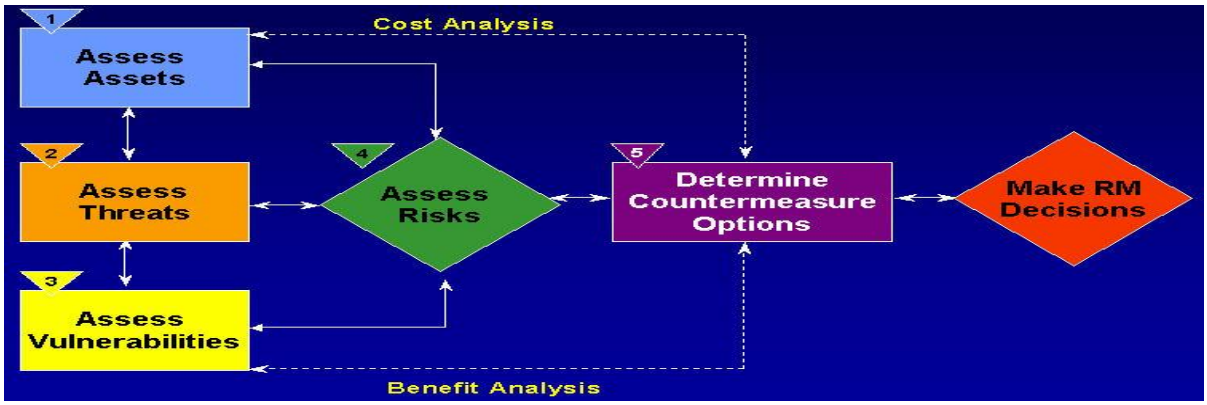
To meet today's security challenges; the national-level security policy initiatives endorse a holistic risk management approach which provides a level of balance that will accomplish the following:

- Realistically match security to the threat
- Effectively allocate limited resources
- Provide necessary security at an affordable price

The Risk Management Process

Risk management is a five-step process that provides a framework for collecting and evaluating information to:

- Assess assets (identify value of asset and degree of impact if asset is damaged or lost)
- Assess threats (type and degree of threat)
- Assess vulnerabilities (identification and extent of vulnerabilities)
- Assess risks (calculation of risks)
- Determine countermeasures (security countermeasure options that can reduce or mitigate risks cost effectively



During the analysis process values are assigned corresponding to the impact of asset loss, threats, and vulnerabilities, and then a resulting risk value is calculated.

The final step in the process is to make a risk management decision. This decision involves analyzing the outcomes from each step (typically using a numerical rating and/or linguistic value) and analyzing the information as a whole to determine the most appropriate countermeasure options for each asset.

Impact and Risk Scale				
	Low	**Medium**	**High**	**Critical**
Range	0-3	4-13	14-50	51-100
Mid-point	2	8	31	75

Threat and Vulnerability Scale				
Degree of Threat	**Low**	**Medium**	**High**	**Critical**
Range	.01-.24	.25-.49	.50-.74	.75-1.00
Mid-point	.12	.37	.62	.87

The Risk Management Process

Step 1 – Assess Assets

The first step in the risk management process is to identify and assess your organization's assets. An ***asset*** is anything of value or importance to the organization or an adversary, such as people, computers, buildings or strategic advantages. This first step determines the value of each asset and prioritizes the asset based upon the consequence of loss. During this step, focus only on assets that are worthy of protection and are most important to your organization and the national security of the United States.

Assets can be assigned to one of five categories:

- People
- Information
- Equipment
- Facilities
- Activities & Operations

Each category is broken into multiple levels to assist with capturing details about each asset. Each level within the categories is then used during the asset analysis. Asset analysis studies are done at a Level I, II, III, and IV, or deeper as necessary. (See job aid for an example of the Asset Category Table.)

NOTE: Categories can be adjusted to meet your organizational needs.

Identify Assets
A variety of resources, including reports, databases and equipment documentation, assist in determining significant assets. However, the best information is attained through a series of interviews with knowledgeable personnel or subject matter experts (SMEs), including the following:

- Customer
- Program/Facility Manager
- Chief of Operations
- Chief of Security

When interviewing SMEs, use a structured asset survey questionnaire to determine asset criticality. Questions should include, but not be limited to the following:

- What critical mission activities take place at this site? Describe.
- What critical/sensitive information (both classified & unclassified) is located at this site?
- What critical/valuable equipment is located at this site? Why is it critical/valuable? What assets would be viewed as critical to an adversary?
- Where are the assets located?
- Who are the facility personnel, tenants, customers, and visitors? What relationship do they have to the critical mission activities/operations?
- What do you view as undesirable events to your assets? Describe the expected impact if the event were to occur.

Identify Undesirable Events
Once you have identified the significant assets, the next step is to identify potential undesirable events. The occurrence of an undesirable event is the focal point of the risk management process. Document and assign a rating to each potential undesirable event that could adversely affect a specific asset.

Research available resources or use the SME interview technique to identify undesirable events. The following questions can help guide you:

- What undesirable events have happened in the past?
- What undesirable events regarding a particular asset concern the asset owner?
- What undesirable events have happened to similar assets?

Measure Impacts
Once undesirable events for each asset are identified, the next step is to measure the impact of such an occurrence. Consider the consequences for each asset that is lost, harmed, or otherwise adversely affected. Again research resources and interview SMEs to gain the needed information. Use the following questions as a guide:

- Could significant damage to national security or loss/injury to human life occur as a result of this event?
- Could ongoing operations be seriously impaired or halted?

- Could costly equipment or facilities be damaged or lost?

Create Risk Assessment Worksheet
Once the impact of an undesirable event is defined, create a ***Risk Assessment Worksheet*** for organizing and later analyzing the information to assist with the analysis.

At this stage of the risk management process, populate the first two columns of the worksheet with the following elements:

- Asset name
- Undesirable event description and impact or potential loss from the undesirable event

Notice that the worksheet contains empty columns. These columns will be completed as you progress through the remaining steps of the risk management process. (Upon completion of the asset assessment step, the first four columns of the worksheet will be completed.) (See job aid for a Risk Assessment Worksheet)

Risk Assessment Worksheet

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP									
	Criminal activity -> employee kidnapping									
Information	Loss -> mission failure									
	Unauthorized release-> capability disclosures									
Equipment	Theft->loss of computers									
	Implant -> compromise information									
Facilities	Mail bomb -> destruction of property									
	Technical attack -> loss of information									
Activities & Operations	Disrupt R&D -> schedule attack									
	Poor OPSEC-> operational disclosure									

Assign Asset Value
Now that you have identified assets and compiled a list of undesirable events, the next step is to assign a linguistic value of the impact:

- **Critical** (C) - A critical rating indicates that compromise to the targeted assets would have grave consequences resulting in loss of life, serious injury, or mission failure.
- **High** (H) - A high rating indicates that a compromise to assets would have serious consequences resulting in loss of classified or highly sensitive data or equipment/facilities that could impair operations affecting national interest for an indefinite period of time.
- **Medium** (M) - A medium rating indicates that a compromise to the assets would have moderate consequences resulting in loss of sensitive information, sensitive

data or costly equipment/property that would impair operations affecting national interests for a limited time period.

- **Low** (L) - A low rating indicates that little or no impact on human life or the continuation of operations affecting national security or national interests would result.

Further differentiate each asset by indicating high, medium, and low within each assigned value.

For a critical value, designate an asset as a high/critical or a low/critical. Doing so provides the ability to weigh a value between assets. For example, the compromise of Top Secret information may be more detrimental than the loss of Confidential information.

Linguistic values, or verbal terms, are less precise than numerical ratings. In addition, it will be more difficult later on in the risk management process to determine which combinations of ratings equal various risk ratings. Therefore, linguistic values are assigned a numerical rating to determine the degree of an asset within each linguistic category. The numerical rating scale ranges from 1 to 100. Additionally, the numeric scale allows for more effective ranking of valued assets within a given range.

For example, all personnel are important, but key project scientists may be ranked higher than a security guard. Thus, a scientist may be valued as critical and assigned a value of 90 yet a security guard may also be valued as critical but assigned a lower value of 60.

After each asset and corresponding undesirable event/impact is assigned a numerical rating representing asset loss, rank each asset in the numerical rating (impact) column by the value of the loss (rating).

When assigning ratings, be sure that the value assigned is based on the asset owner's perspective. In many cases an asset may be important to an asset manager, agency, or department, but may only have minor importance to the U.S. Government, which ultimately owns the asset and pays for its security. Basing ratings on the asset manager's perspective could result in asset overprotection at the expense of other more critical assets.

Risk Assessment Worksheet

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP	H/C	97							
	Criminal activity -> employee kidnapping	L/C	51							
Information	Loss -> mission failure	H/C	97							
	Unauthorized release-> capability disclosures	H/M	13							
Equipment	Theft->loss of computers	H/H	48							
	Implant -> compromise information	L/M	4							
Facilities	Mail bomb -> destruction of property	M/H	25							
	Technical attack -> loss of information	L	3							
Activities & Operations	Disrupt R&D -> schedule attack	M/M	10							
	Poor OPSEC-> operational disclosure	L/H	15							

Step 2 - Threat Assessment

The second step in the risk management process is to assess threats. The goal of this step is to assess the current threat level for the identified assets.

The first step in assessing threats is identifying an asset's adversaries and threats. There are many types of threats, some which are perpetrated by people or organizations, which are usually referred to as adversaries, while others are accidents or due to natural phenomenon and are not considered adversaries.

An ***adversary*** is any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to assets. Common examples of adversaries are terrorists, criminals, and foreign intelligence entities.

A ***threat*** is any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat may also be defined as the intention and capability of an adversary to undertake detrimental actions against an asset owner's interests.

Threats are assigned to one of the following categories:

- **Criminal:** A criminal is an adversary who violates the law causing the loss of or damage to assets. Examples include: violent acts against people, theft, hacking, etc.
- **Terrorist**: A terrorist is an adversary who uses violence or the threat of violence to inculcate fear, with the intent to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Examples include Al Qaeda, HAMAS, etc.
- **Insider**: An insider is an adversary who has special access or privileges, e.g., employees, contractors, customers, etc.
- **Economic espionage**: Economic espionage is the theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents. Both traditionally friendly nations and recognized adversaries conduct economic espionage.

- **Foreign Industrial Espionage**: Foreign industrial espionage is espionage conducted by a foreign government or a foreign company with direct assistance of a foreign government against a private U.S. company for the purpose of obtaining commercial secrets.
- **Foreign Intelligence Entity:** Foreign Intelligence Entities are organizations that are part of a foreign government and engage in intelligence activities.
- **Natural disaster**: Natural disasters are phenomena that occur in nature that have the potential to damage assets or interrupt activities and operations. Examples include: floods, lightning, tornadoes, volcanic eruptions, etc.

After identifying the adversaries, the next step is to analyze threat data to understand the adversaries' profile, specifically their intent.

Analyze Intent
Intent refers to an adversary's intended plans that may pose a threat to an asset. Analyzing intent requires an understanding of the adversary's perspective. Research resources, or use the SME interview technique to identify intent. The following questions can help guide you:

- What are the adversaries' goals?
- To what degree are the adversaries motivated to achieve those goals?
- How will exploiting or harming U.S. assets bring the adversaries closer to their goals?
- What level of risk are the adversaries likely to accept?
- Are the adversaries willing to risk getting caught?
- What might the adversaries lose if caught exploiting or harming U.S. assets?
- Are there other methods for adversaries to obtain their goals?
- Will the adversaries choose one of those methods?

Group the identified adversaries into categories to help in the analysis and organization of your assessment. The following categories are examples:

- **Individuals** - common criminals, insiders, and disturbed individuals
- **Groups & Organizations** - terrorists, corporate competitors, narco-traffickers
- **Governments** - foreign intelligence entities, foreign militaries, state-sponsored entities

After you have grouped the adversaries, create an ***Intent Assessment Chart*** to analyze and summarize the data. A "yes" or "no" response is required for the following:

- Knowledge of an asset
- Need
- Each adversary's demonstrated interest level

Some of this information can be obtained from intelligence and counterintelligence organizations. This is generally the weakest link in the overall risk management process because access to this type of information is often limited.

Based on the number of "yes" responses, assign a high, medium, or low intent level for each adversary. Typically, three "yes" responses equate to a high intent level, two "yes" responses translate to a medium, and one "yes" response indicates a low overall intent level.

Intent Assessment Chart				
Adversary Insider, Terrorist, FIE, Criminal	**Intent**			
	Knowledge of Asset	**Need**	**Demonstrated Interest**	**Overall Intent Level**
Adversary 1	Yes	Yes	Yes	High
Adversary 2	Yes	Yes	No	Medium
Adversary 3	Yes	No	No	Low

Determine Capability
After assessing an adversary's intent, determine the capability level to carry out an undesirable event.

Capability refers to an adversary's ability or capacity to act as a potential threat to an asset. Analyzing capability requires an understanding of the necessary skills and resources required to:

- Determine if an adversary possesses the resources to pose a threat to an asset

To gather information on an adversary's capabilities, research resources or interview SMEs to answer the question:

- Does the adversary have the following components for exploiting or attacking an asset?
  - ✓ Knowledge of specific locations and their vulnerabilities
  - ✓ Requisite technology and skills
  - ✓ Weapons or tools
  - ✓ Requisite special knowledge
  - ✓ Support structure

When researching an adversary's capabilities, remember that the adversary may use a combination of ***overt*** or ***covert*** methods/activities to collect information to target an asset. These methods/activities include the following:

- **SIGINT** (Signals Intelligence) is comprised of communications and the electronic and telemetry collection of information in the non-visible portion of the electromagnetic spectrum.
- **HUMINT** (Human Intelligence) is intelligence derived from people through interviews, elicitation, or reports originating from people.

  HUMINT insider – information collection techniques:
  - Attempting to obtain information without need to know
  - Making unusual use of or requests for classified publications
  - Attempting to access classified databases
  - Removing information without approval
  - Placing classified material in a desk or briefcase
  - Copying classified material in other offices
  - Borrowing or making notes of classified material
  - Bringing cameras or recording devices into cleared facilities
  - Obtaining or attempting to obtain witness signatures on classified destruction records

- Stockpiling classified or proprietary documents outside cleared area

HUMINIT insider indicators - personnel who:

- Are disgruntled with management
- Are disgruntled with the U.S. Government
- Are fascinated with and have a strong desire to engage in spy work
- Suddenly purchase high value items
- Suddenly settle large outstanding debts
- Travel to foreign countries repeatedly
- Make short trips overseas
- Have contact with foreign officials and representatives
- Attempt to conceal contacts with foreigners
- Have relatives or friends residing abroad
- Avoid or decline assignments requiring a counterintelligence-oriented polygraph
- Work an unusual amount of overtime
- Sudden decline in work quality

- **IMINT** (Imagery Intelligence) involves using various sources, such as satellites, photos, infrared, imaging radar, and electro-optical for collecting image data.
- **MASINT** (Measurement and Signatures Intelligence) It excludes signals intelligence and traditional imagery intelligence. When collected, processed, and analyzed, MASINT locates, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources. It includes the advanced data processing and exploitation of data from overhead and airborne imagery collection systems. MASINT data can be acquired from a variety of satellite, airborne, or ship borne platforms; remotely piloted vehicles; or from mobile or fixed ground-based collection sites.
- **OSINT** (Open Source Intelligence) includes resources such as newspapers, internet, magazines, international conventions, Freedom of Information Act (FOIA) requests, seminars, and exhibits (e.g., CNN.com, *The New York Times*, *Aviation Week*, and *Space & Technology)*.

Once each adversary's capabilities are determined, create a ***Collection Capability Assessment Chart*** to record the data. Assign a rating of high, medium, or low for each adversary's capabilities.

Collection Capability Assessment Chart						
Adversary Insider, Terrorist, FIE, Criminal	**Collection Capabilities**					
	HUMINT	**SIGINT**	**IMINT**	**MASINT**	**OSINT**	**Overall Capability Level**
Adversary 1	High	High	Medium	Medium	High	High
Adversary 2	High	Medium	Low	Medium	High	Medium
Adversary 3	Medium	Medium	Low	Low	Medium	Medium

Determine History
After assessing an adversary's intent and capability, determine an adversary's history of carrying out undesirable events.

An adversary's ***history*** is an account of past actions taken against assets. Analyzing an adversary's history requires both an understanding of an adversary's past attempts to attack assets as well as any successful attacks on assets. Conduct SME interviews and research resources to answer the following questions:

- Has the adversary attacked or exploited assets and personnel before?
- Has the adversary attempted to attack or exploit assets? If not, why not?
- Has the adversary been suspected of attacking or exploiting assets?
- Might some foreseeable event cause the adversary to attempt an attack in the future?

After identifying an adversary's history, document this information by creating a ***History Assessment Chart***. This chart requires completing information regarding an adversary's suspected, attempted, or successful incidents.

History Assessment Chart			
Adversary Insider, Terrorist, FIE, Criminal	**History**		
	Suspected Incidents	**Attempted Incidents**	**Successful Incidents**
Adversary 1	2 technical devices found	2 attempted forced entries	Unknown
Adversary 2	5 alarm activations; adversary sighted in area	2 attempted forced entries	Unknown
Adversary 3	None	None	None

Research resources and conduct SME interviews to gain knowledge regarding an adversary's intent, capability, and history. Depending on the threat topic at hand, the best sources for a given threat range from unclassified sources, such as the Internet, to classified sources, such as Top Secret intelligence or documentation. Some of the resources/SMEs that should be consulted include the following:

- Classified sources
  - ✓ Files
  - ✓ Counterintelligence support activity
  - ✓ Federal Bureau of Investigation (FBI)
  - ✓ Central Intelligence Agency (CIA)
- Unclassified sources
  - ✓ Local law enforcement
  - ✓ The news
  - ✓ Government publications/websites
  - ✓ Training and awareness organizations

Assign Threat Rating
Once the intent, capability, and history of an adversary are identified, determine a threat assessment rating.

You have made a chart for each of the steps in the threat assessment process (intent, capability, and history). Using those three charts, create a new chart, the ***Threat Assessment Summary Chart*** to summarize and analyze all the information.

The Threat Assessment Summary Chart contains a column to list the adversary and a rating of the adversary's intent, capability, and history. The intent and capability columns are populated with a high, medium, or low rating and the history column is populated with a "yes" or "no" response (whether there is a history or not of attacking an asset). This chart assists with keeping track of individual adversaries.

Putting it all together:

- The intent column is a summary of the ***Intent Assessment Chart***
- The capability column is a summary of the ***Collection Capability Assessment Chart***
- The history column is a summary of the ***History Assessment Chart***

Threat Assessment Summary Chart				
Adversary Insider, Terrorist, FIE, Criminal	**Intent (Interest/Need)**	**Capability (Methods)**	**History (Incidents/Indicators)**	**Overall Threat Level**
Adversary 1	High	High	Yes	High
Adversary 2	Medium	Medium	Yes	Medium
Adversary 3	Low	Medium	No	Low

After determining the overall threat level, create a second chart, the ***Threat Level Decision Matrix***. This chart assigns a "yes" or "no" rating for each adversary's intent, capability, and history.

Once completed, a threat level is assigned based on the number of "yes" ratings. The greater the number of "yes" ratings, the higher the threat level. The threat level is the relative rating based on the best available information. To determine the relative degree of threat, rating criteria has been developed to ensure consistent threat rating levels.

The Threat Level Decision Matrix requires assigning a level of critical (C), high (H), medium (M), or low (L) for each asset's threat/adversary(s).

For example,

"yes + yes + yes" = critical

"no + no + no" = low

Threat Level Decision Matrix			
Intent (Interest/Need)	**Capability (Methods)**	**History (Incidents/Indicators)**	**Threat Level**
Yes	Yes	Yes	Critical
Yes	Yes	No	High
Yes	No	Yes/No	Medium
No	Yes	No	Medium
No	No	No	Low

After determining the threat levels, map them back to the assets and their associated impacts. For example, hackers may be identified as being adversaries with a specific threat level. The adversary is then mapped to computer assets but probably not to other assets.

The last step is to assign a numerical rating to determine the degree of each threat or the likelihood that an adversary will launch an attack. The numerical rating scale ranges between .01 and 1.00. This range provides the opportunity to weigh the threats with some being assigned a higher numerical value than others even though they are within the same degree of threat category.

The ***Threat Assessment Rating Table*** represents likelihoods or probabilities. The percentages in this table assist with understanding the threat assessment rating BUT the numerical table facilitates the risk analysis process in step four of the risk management process.

Risk Assessment Worksheet

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP	H/C	97	Terrorist	H/C	.97				
	Criminal activity -> employee kidnapping	L/C	51	Terrorist	L/H	.50				
Information	Loss -> mission failure	H/C	97	FIE/Insider	H/H	.73				
	Unauthorized release-> capability disclosures	H/M	13	Insider	M/M	.37				
Equipment	Theft->loss of computers	H/H	48	Criminal	L/M	.30				
	Implant -> compromise information	L/M	4	FIE	H/H	.70				
Facilities	Mail bomb -> destruction of property	M/H	25	Terrorist	L/M	.25				
	Technical attack -> loss of information	L	3	Terrorist	H/H	.74				
Activities & Operations	Disrupt R&D -> schedule attack	M/M	10	FIE/Insider	L	.12				
	Poor OPSEC-> operational disclosure	L/H	15	Militant	M/M	.37				

Step 3 - Assess Vulnerabilities

The third step in the risk management process is to assess vulnerabilities. The goal of this step is to identify the current vulnerability level or any weakness that can be exploited by an adversary to gain access to an asset.

Perform a three-step vulnerability assessment to identify the following:

- Potential vulnerabilities related to specific assets and their undesirable events
- The degree of each asset's vulnerability to a threat.
- Existing countermeasures and their level of effectiveness in reducing vulnerabilities.

The process of identifying vulnerabilities may sound familiar because it encompasses a traditional security survey. Look for exploitable situations resulting from inadequate security, personal behavior, commercial construction techniques, or insufficient security procedures. Typical vulnerabilities include weak door locks, the absence of guards, poor password controls, and insufficient distance between a building and a street.

Vulnerability Areas
Five general areas are open to potential asset vulnerabilities:

- Human
- Operational
- Information
- Facility
- Equipment

Human Vulnerability Areas
Human vulnerability areas include persons who exhibit the following traits/issues:

- **A big ego**: Persons with a big ego may mishandle or improperly protect critical assets.
- **Anger management problems**: Persons with anger management problems may damage or destroy critical assets out of anger.
- **Are ignorant of technology**: Persons who are ignorant of technology fail to learn how to properly operate computers, secure telephones, etc. This may place sensitive information at risk.
- **Behavioral issues**: Behavioral issues apply to disgruntled personnel, persons with personality disorders, etc. These persons may represent either a direct or indirect threat to assets.
- **Boredom**: Persons suffering from boredom may become careless.
- **Greedy**: Persons who are greedy may compromise or steal critical assets for personal gain.
- **Loose lips**: Persons with loose lips may compromise sensitive information.
- **Mental illness**: Persons with mental illness may represent a threat to critical assets or place critical assets in jeopardy either knowingly or unknowingly.
- **Overworked**: Persons who are overworked may become careless.
- **Practice poor security**: Persons practicing poor security fail to comply with security requirements and may place critical assets in jeopardy.
- **Seek revenge**: Persons who seek revenge may attack critical assets to get even for a perceived wrong.
- **Substance abusers**: Persons who are substance abusers may pose a threat to critical assets by selling them for cash or being careless while under the influence.

Operational Vulnerability Areas
Operational vulnerability areas include the following:

- **Poor tradecraft practices** that potentially place critical assets at risk. For example, failure to develop and operate a property control system places critical assets at risk
- **Observables** are practices, activities, or assets that can be surveilled. The information gained could be utilized to threaten critical assets. An example is an activity that uses roving security guard patrols at exact intervals. An adversary may be able to observe this fact and estimate a timeframe within which to infiltrate a facility.
- **Other Operations Security (OPSEC) issues** – OPSEC is an analytical process used to deny an adversary information, generally unclassified, concerning an organization's intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other security disciplines - it supplements them.

- **Press exposure** of sensitive information represents a potential vulnerability. For example, an activity with poor entry control procedures may be susceptible to loss/theft of property and may have implanted listening devices.

Information Vulnerability Areas
Information vulnerability areas include the following:
- **Information unnecessarily disseminated to a wide audience** – the wider the dissemination the more difficult it is to protect.
- **Failure to practice need-to-know** - "Need-to-know" refers to the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform an authorized governmental function.
- **Poor program administration** includes failure to properly safeguard sensitive information, improperly classifying information and failure to mark classified information.
- **Failure to follow Freedom of Information Act (FOIA) requirements** - Adversaries routinely request information through FOIA. Failure to properly evaluate information that has been requested for public release may pose a threat to critical assets

Facility Vulnerability Areas
Facility vulnerability areas leave assets in jeopardy. These are some potential issues:
- **Location** – Areas designated as high crime areas or with a significant potential for natural disasters could be a concern.
- **Poor perimeter fencing** with holes, gaps, vegetation overgrowth, etc.
- **Building design characteristics** with floor plans that inhibit access control measures, ground floor windows along a heavy pedestrian route, etc.
- **Tunnels and drains** that permit an avenue of approach by an adversary
- **Unsecured doors** that allow adversary access.
- **Parking lots** provide adversaries with a venue for observing a facility, perpetrating a crime, detonating mobile explosive devices, etc.
- **Vehicle barriers** – They must be reinforced and security personnel must be trained to be effective.
- **Untrained guard forces** may be ineffective in observing, preventing, or responding to an adversary attack. Guard forces must understand their duties and be trained to carry them out.
- **Unsecured windows** provide adversaries with a potential avenue of approach.
- **Insufficient access control** allows adversaries a potential means of entry either detected or undetected.
- **Gates** must be properly operated when in use, locked when not in use, and regularly evaluated to ensure they do not provide adversaries with a potential avenue of approach.

Equipment Vulnerability Areas
Equipment vulnerability areas include the following:
- **Signal interceptions** that can occur when using devices like cell phones, wireless networked computers, and personal digital assistants (PDAs).
- **TEMPEST emanations** - TEMPEST is the short name referring to the investigation, study, and control of compromising emanations from telecommunications and information systems equipment. Computer equipment, typewriters, etc. emanate electronic signals that can be collected by an adversary. They can then interpret the

signals and obtain the information that was being processed on the electronic equipment.
- **Equipment tampering** in which equipment is modified to permit collection of information by an adversary. For example, modifications to a reproduction machine might enable image storage of everything copied.
- **Remote activation/operation** that allows modifications or programming permitting an adversary to remotely activate and/or operate equipment.

Vulnerability Assessment
View each asset as if you were the adversary. Study the asset and ask the questions:
- "If I were adversary "x", I would break into this facility by…"
- "If I wanted to physically harm person "x" in this facility, I would…"

This questioning process should be used on each asset for every adversary.

Common vulnerabilities that adversaries may exploit include the following:
- Information leaks
- Physically stored equipment and information
- Electronically stored and transmitted information
- Assets at risk of visual observation
- Vulnerability data

Gather Vulnerability Data
Vulnerability data can be obtained from a variety of subject matter experts (SMEs). Utilize the SME interview technique and question those who work most closely with protecting the asset.

For example, security guards almost always recognize vulnerabilities from past experiences or careful evaluation of their surroundings. Likewise, computer system administrators and program managers are likely to be aware of vulnerabilities in their systems through a variety of experiences, professional publications, conferences, and contacts.

Additional sources that can assist with gathering vulnerability information include the following:
- Personnel who work at the "site"
- Existing site surveys
- Engineering drawings and blueprints
- Maps
- Security planning documents
- Surveys and audits
- Incident reports

Regressive Analysis
Asset vulnerabilities may already have some type of security countermeasure in place. The best method to analyze these asset vulnerabilities is through ***regressive analysis***. Regressive analysis requires analyzing the asset in an unprotected state first and then analyzing the asset in conjunction with current countermeasures.

Regressive analysis is a five-step process:
1. Assess the asset's vulnerabilities in a pure, unprotected state.

2. Reevaluate the asset's vulnerabilities taking into consideration the efficacy of the existing countermeasures.
3. Identify the asset's vulnerability differences between the unprotected and protected assessments.
4. Identify the ineffective countermeasures.
5. Identify and characterize the specific vulnerabilities that still exist, given the current countermeasures.

Classify Countermeasures
Countermeasures are classified according to their implementation requirements. Some countermeasures are procedural in nature, others involve equipment/devices, and still others involve personnel usage.

Procedures	Equipment (Physical/Technical)	Manpower
• Security Policies • Security Procedures • Training • Awareness Programs • Legal Prosecution • Security Investigations • Polygraph • Disclosure Statements • Personnel Transfer • Contingency/Emergency Response Planning • OPSEC Procedures • Cover Procedures	• Locking Mechanism • Window Bars • Doors • Fences • Alarms/Sensors • Hardware/Software • Badges • Lighting • TEMPEST Devices • Paper Shredder • Weapons • Closed-circuit TV • Safe Haven • Vault	• Contractor Guard Force • Special Police Officers • Local Guards • Military Guards

Assign Vulnerability Level and Rating
After completing the regressive analysis, it is important to assign an asset a vulnerability level. Asset vulnerability is determined using a number of criteria including the following:
- **Quality**: The degree of difficulty required to exploit a single vulnerability. In other words, how hard is it to exploit a given asset?
- **Quantity**: The number of complementary vulnerabilities that can be exploited.
- **Efficacy of Countermeasures:** The ability of each existing countermeasure to effectively prevent or minimize a specific type of attack.

To determine the vulnerability level for a given asset, each of the following questions must be answered with a "yes" or "no":
- Is the asset made vulnerable by a single (as opposed to multiple) weakness in the security system?
- Does the nature of the vulnerability make it difficult to exploit?
- Do multiple effective layers of security countermeasures lessen an asset's vulnerability?

Once an asset's vulnerabilities are determined, assign and chart a vulnerability rating of critical (C), high (H), medium (M), or low (L) for each asset.

Finally, assign and chart a numerical rating to determine the degree of each asset's vulnerability. The numerical rating scale ranges between .01 and 1.00. This range provides the opportunity to allow a weighted evaluation of the threats within the same degree of threat category. After assigning the vulnerability rating, enter it into the numerical rating (vulnerability) column of the worksheet.

Risk Assessment Worksheet

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP	H/C	97	Terrorist	H/C	.97	Cars not inspected	C	.80	
	Criminal activity -> employee kidnapping	L/C	51	Terrorist	L/H	.50				
Information	Loss -> mission failure	H/C	97	FIE/Insider	H/H	.73	Ineffective document control	H	.65	
	Unauthorized release-> capability disclosures	H/M	13	Insider	M/M	.37				
Equipment	Theft->loss of computers	H/H	48	Criminal	L/M	.30	No IDS System	H	.55	
	Implant -> compromise information	L/M	4	FIE	H/H	.70				
Facilities	Mail bomb -> destruction of property	M/H	25	Terrorist	L/M	.25	No patrols at building	M	.35	
	Technical attack -> loss of information	L	3	Terrorist	H/H	.74				
Activities & Operations	Disrupt R&D -> schedule attack	M/M	10	FIE/Insider	L	.12	No backup power supply	M	.40	
	Poor OPSEC-> operational disclosure	L/H	15	Militant	M/M	.37				

Step 4 - Assess Risks

The fourth step in the risk management process is to assess risks. The goal of this step is to analyze the data collected and develop a risk rating.

Risk assessment combines and analyzes the first three assessments (asset, threat, and vulnerability) to provide an overall picture of potential risks to an asset or group of assets. Using this information, you will be able to calculate an asset's risk rating and assign the asset a risk level.

Risk Factors

Generally, the extent of an asset's risk is determined by how much the following risk factors overlap: assets, threats and vulnerabilities. For example, if the rating level for all factors is critical, then the risk level would be at its highest. However, if any of the factors have a lower rating level, then the level of risk would diminish based on the lower rating of each factor.

The assets/impacts must be measured against the probability of threats and vulnerabilities. The overall risk level varies with relation to the values of each item. The larger the risk area shared by assets, threats, and vulnerabilities, the higher the risk level.

The three risk factors are incorporated into a formula to determine and assign a more precise risk rating:

Risk = Impact x (Threat x Vulnerability) or (R = I [T x V])

"Impact" represents the consequence of the asset loss to the asset owner.
The "Threat x Vulnerability" value represents the probability of the undesirable event occurring.

Information in the impact, threat, and vulnerability assessment columns from the ***Risk Assessment Worksheet*** is used in the risk formula to calculate the risk rating.

Convert the numerical risk rating back to a linguistic scale using critical (C), high (H), medium (M), or low (L) and record the information. This linguistic conversion allows for categorizing the risk rating into layman's terms for briefing to management/command.

Risk Assessment Worksheet

Risk Assessment Worksheet										
Asset	**Undesirable Event/Impact**	**Ling. Value (Impact)**	**Num. Rating (Impact)**	**Threat Category**	**Ling. Value (Threat)**	**Num. Rating (Threat)**	**Vulnerability Category**	**Ling. Value (Vuln)**	**Num. Rating (Vuln)**	**Risk Rating**
People	Motorcade attack -> assassination of VIP	H/C	97	Terrorist	H/C	.97	Cars not inspected	C	.80	
	Criminal activity -> employee kidnapping	L/C	51	Terrorist	L/H	.50				
Information	Loss -> mission failure	H/C	97	FIE/Insider	H/H	.73	Ineffective document control	H	.65	
	Unauthorized release-> capability disclosures	H/M	13	Insider	M/M	.37				
Equipment	Theft->loss of computers	H/H	48	Criminal	L/M	.30	No IDS System	H	.55	
	Implant -> compromise information	L/M	4	FIE	H/H	.70				
Facilities	Mail bomb -> destruction of property	M/H	25	Terrorist	L/M	.25	No patrols at building	M	.35	
	Technical attack -> loss of information	L	3	Terrorist	H/H	.74				
Activities & Operations	Disrupt R&D -> schedule attack	M/M	10	FIE/Insider	L	.12	No backup power supply	M	.40	
	Poor OPSEC-> operational disclosure	L/H	15	Militant	M/M	.37				

What is Acceptable Risk?
An asset's acceptable risk cannot be determined by a formula. Acceptable risk varies with time, circumstances, and management's attitude toward risk in the organizational environment. The asset sponsors or owners have the responsibility of deciding what constitutes an acceptable level of risk for their assets.

Step 5 - Determine Countermeasures
The fifth and final step in the risk management process is to determine countermeasure options. The goal of this step is to identify potential countermeasures for reducing an asset's vulnerabilities, in turn reducing the overall risk to that asset.

Countermeasure Analysis
The ***Countermeasure Analysis Chart*** is an important tool in determining appropriate countermeasures for mitigating an asset's vulnerabilities. All the information acquired to this point in the risk management process will be used in conducting a countermeasure analysis and completing the chart.

Countermeasure Analysis Chart

Undesirable Events (1)	Existing Risk (2)	Related Vulnerability Level & Vulnerabiltiy (3)	Countermeasure (4)	Cost (5)	New Vulnerability Level (6)	New Risk Level (7)
Existing Risk →		Total Cost →			New Risk Level →	

To identify potential countermeasures, answer the following three questions:

- What are the possible protection solutions?
- What are the best solutions with no financial constraints?
- What are other possible solutions when the best is too expensive?

Countermeasure Cost Determination

The costs of implementing countermeasures must be considered relative to the following:

- **Dollars** - Consider the purchase price and the life-cycle maintenance costs (e.g. installation, preventive maintenance, repair/warranty, replacement, and training).
- **Inconvenience** - Consider whether the inconvenience caused is offset by the measure of risk reduction gained. If a countermeasure is inconvenient, people will find a way to circumvent it.
- **Time** - Include the time to implement and oversee the countermeasure and the time to prepare for its implementation, as well as any time required for follow-up and evaluation.
- **Personnel** - Consider the number of personnel needed to manage the countermeasure as well as the skills, knowledge, and abilities of the personnel involved. Also consider personnel training needs and costs.
- **Other** - Consider the adverse publicity, political repercussions, reduced operational efficiency, and unfavorable working conditions resulting from countermeasure implementation.

Categorize countermeasures according to their function:

- Procedures
- Equipment
- Manpower

Written procedures are the least expensive to implement with the costs rising for equipment and manpower.

Cost Benefit Analysis
Once you identify countermeasures and associated costs, compare the costs of each option with the benefits by answering the following questions:

- How does asset value compare to proposed cost of protection?
- How does the option mitigate the risk?
- To what degree does the option delay, deter, detect, defend, or destroy?
- Which option provides the best protection at the lowest cost?

Countermeasure Options
Upon completion of the cost benefit analysis, prioritize the countermeasure options by:

- Identifying countermeasures
- Selecting a reasonable number of countermeasure options
- Determining how each option affects the overall risk level
- Calculating the cost of each option
- Ensuring you address the maximum number of undesirable events with the various options you recommend

Countermeasure Analysis
Summarize and record all the information onto the ***Countermeasure Analysis Chart*** for each option chosen. The chart requires that you do the following:

- Specify each event (column 1)
- Enter the rating from the Risk Assessment Worksheet (column 2)
- Enter the rating and identify the specific vulnerability from the Risk Assessment Worksheet (column 3)
- Identify the countermeasure selected on the Countermeasure Worksheet #1 (column 4)
- Enter the cost (column 5)
- Enter the new vulnerability level rating resulting from the new countermeasure implementation (column 6)
- Calculate and enter the new risk level (R = I x [T x V]) resulting from the new vulnerability level of column 6 (column 7)
- Total the cost of the proposed countermeasure

The bottom row provides the total cost for all countermeasures and shows from/to risk data.

Countermeasure Analysis Chart

(1) Specify each event (2) Enter the rating from your Risk Assessment Worksheet (3) Enter Rating and Identify the specific vulnerability from your Risk Assessment Worksheet (4) identify your selected countermeasure from Countermeasure Worksheet #1 (5) Enter the cost (6) Enter the new Vulnerability Level Rating that results when you use the new Countermeasure (7) Calculate and enter the new Risk Level (R = I x [T x V]) when you use the new Vulnerability Level of column (6). The bottom row provides the total cost for all countermeasures and shows from/to risk data.

Undesirable Events (1)	Existing Risk (2)	Related Vulnerability Level & Vulnerabiltiy (3)	Countermeasure (4)	Cost (5)	New Vulnerability Level (6)	New Risk Level (7)
Motorcade attack –assassination of VIP	75.27 (Critical)	.80 –Cars not inspected	Car inspection program	$5,000	.40 (Medium)	37.6 (High)
Information loss – mission failure	46.03 (High)	.65 – Ineffective document control	Document control system	$8,000	.15 (Low)	10.6 (Medium)
Existing Risk	60.7 Critical		Total Cost	$13,000	New Risk Level	24.1 High

Countermeasure Options

Many security professionals are not in a position to obligate funds for countermeasures and must receive approval from a decision maker. In most situations, they will be asked to provide comparison information for several different options. Factors influencing decision makers are the following:

- Asset value
- Current exposure to loss/harm
- Protective measure availability
- Fund availability
- Mandatory security requirements

Normally, the security professional would make three recommendations to the decision maker:

- Best possible case, money no object
- Sensible recommendation, good security for the money
- Minimum need to meet the requirements

Now that you have completed this course, you should have the tools and knowledge necessary to identify and apply the five steps of the risk management process in the development of a risk assessment.