Student Guide

Course: Introduction to Risk Management

Introduction

Welcome to the Introduction to Risk Management. This course will provide security professionals with an introduction to the five-step process for acquiring and analyzing the information necessary for protecting assets and allocating security resources. Protection has become more complex and security resources more restricted, thereby requiring a holistic risk management approach, balancing the cost of security with the possible risk.

Course Objectives

At the end of this course you should be able to:

- Identify the steps of the Risk Management process.
- State the three analytical activities involved in the Risk Management process.

What is Risk Management?

To meet today's challenges, the security policies and services must realistically match the threats. These policies must be flexible and the standards and procedures in place must be consistent and allow for the effective allocation of resources. All policies, practices and procedures must provide the necessary security at an affordable price.

Risk Management is the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

What is the difference between Risk Avoidance and Risk Management?

It is important to understand that there is a difference between Risk Avoidance and Risk Management. Risk Avoidance assumes all opponents are aggressive threats, counters ALL vulnerabilities, and plans for worst-case scenarios.

Risk Management on the other hand is a process that integrates the assessment of assets, threats and vulnerabilities and weighs the calculated risk against the projected cost of security.

The Risk Management Model incorporates a five-step process that will:

- Identify the critical assets that require protection
- Identify undesirable events and expected impacts

- Value and prioritize assets based on the consequence of loss
- Assess the risks and
- Determine countermeasures

Case Study

Let's apply the concept of Risk Management by looking at an example of a real-life situation.

You are going away on a two-week trip and recently there have been thefts in your neighborhood. Car stereos, TV's, jewelry and even lawn furniture have been stolen. There have also been incidents of vandalism at the park two blocks away and at the local elementary school. There was even an attempted break-in at your neighbor's house last weekend.

What should you do?

Following the Risk Management process ask yourself the following questions:

- What assets are of value to you?
  Your answers would probably include your house, car, jewelry, furniture, clothes, and more. What would be the consequence of the loss? You might need to rebuild your house, replace costly items, and experience losses that cannot be replaced.

- What threats or dangers could cause harm to your assets?
  Your assets are susceptible to fire, theft, and natural disasters.

- How is your house vulnerable as a result of your absence?
  An empty house is attractive to burglars; also there is no one home to monitor the inside and outside environment.

- What countermeasures are currently in place to help mitigate these risks?
  You might have an alarm system, smoke detectors, or a neighbor watching the house. Most likely you have insurance.

- What assets are most at risk?
  Foremost would be your house, then all the contents of your house and your vehicles.

- What countermeasures can you utilize to reduce or eliminate the risks?
  If you don't already have one, you might want to consider installing an alarm system. You would most likely notify your neighbors that you will be away. You would stop the delivery of mail and newspapers. You might install timers for inside lights, and install outside motion lights.

The important point to remember is that before you leave you would carefully assess the answers to the questions and implement effective countermeasures and deterrents to reduce or eliminate the risks.

You should always use the same process when making decisions regarding the protection requirements for government resources and assets!

Risk Management Process – Step 1
Identify Assets

Let's take a look at each step of the Risk Management Process.

The first step in the process is to identify assets.

Assets fall into 5 categories:

- People
- Information
- Equipment
- Facilities and
- Activities and Operations

The goal of the first step is to determine the value of each asset and prioritize the assets based on the consequence of the loss. During this step you want to focus only on those assets that are worthy of protection and are most important to the national security of the United States. The impact of the loss of these assets would be categorized as Critical, High, Medium or Low.

Once you have identified the assets and undesirable events, you must assign an asset value.

Critical indicates that compromise to the assets targeted would have grave consequences leading to loss of life, serious injury, or mission failure. The rating scale is from 50-100.

A ***High*** value indicates that a compromise to assets would have serious consequences resulting in the loss of classified or highly sensitive data that could impair operations affecting national interests for a limited period of time. The rating scale is from 13-50.

An asset value of ***Medium*** indicates that a compromise to the assets would have moderate consequences resulting in the loss of confidential, sensitive data or costly equipment/property that would impair operations affecting national interests for a limited period of time. The rating scale is from 3-13.

A ***Low*** value indicates that there is little or no impact on human life or the continuation of operations affecting national security or national interests. The rating scale is from 1-3.

Risk Management Process – Step 2
Identify Threats

The second step of the Risk Management Process is to identify threats. The goal of this step is to assess the current threat level for the identified assets. Threat assessment is identifying an asset's adversaries and threats.

Threats could include:

- Foreign Intelligence Services, which are organizations that are part of a foreign government and engage in intelligence activities.
- Terrorists who use violence to instill fear and coerce or intimidate governments in their pursuit of political, religious or ideological goals.
- Criminals who violate the law causing loss or damage to assets.
- Insiders with special access or privileges and,
- Natural Disasters, which are phenomena that occur in nature and have the potential to damage assets.

Threats are rated using the same four criteria of ***Critical***, ***High***, ***Medium*** and ***Low***.

A ***Critical*** rating indicates that a definite threat exists against the assets and that the adversary has both the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequent or recurring basis. The rating scale is set at 75-100%.

A ***High*** rating indicates that a credible threat against the assets exists, based on our knowledge of the adversary's capability and intent to attack the assets and based on related incidents having taken place at similar facilities. The rating scale is 50-74%.

A rating of ***Medium*** indicates that there is a potential threat to the 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. The rating scale is set from 25-49%.

A ***Low*** rating indicates little or no credible evidence of capability or intent, with no history of actual or planned threats against the assets. The rating scale is set at 0-24%.

Risk Management Process – Step 3
Identify Vulnerabilities

The third step in the Risk Management Process is to identify 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.

There are five general areas of vulnerability.

- Human, includes persons who exhibit traits of anger, boredom, greed, and revenge.
- Operational would include insufficient security procedures.
- Information vulnerabilities include the failure to follow the Freedom of Information Act requirements and failure to practice need-to-know.
- Facility issues include weak door locks, the geographic location, and the absence of guards and,
- Equipment vulnerabilities could include equipment tampering, TEMPEST emanations and signal interceptions.

After identifying the vulnerabilities you must then assign a rating.

A ***Critical*** rating indicates that there are no effective countermeasures currently in place and all known adversaries would be capable of exploiting the asset. Critical is assigned a rating scale of 75-100%.

Assigning a ***High*** rating indicates that although there are some countermeasures in place, there are still multiple weaknesses through which many adversaries would be capable of exploiting the asset. The rating scale is set at 50-74%.

A ***Medium*** rating indicates that there are effective countermeasures in place, however one weakness does exist which some known adversaries would be capable of exploiting. The rating scale is set at 25-49%.

Assigning a ***Low*** rating indicates that multiple layers of effective countermeasures exist and few or no known adversaries would be capable of exploiting the asset. The low rating scale is set at 0-24%.

Risk Management Process – Step 4
Assess Risks

The fourth step in the Risk Management Process is Risk Assessment. The goal of this step is to integrate the data collected during the first three steps to obtain a risk rating that will establish priorities for the mitigation of risk.

The risk formula ***RISK = IMPACT x (THREAT x VULNERABILITY)*** incorporates the three risk factors for determining and assigning a more precise risk rating.

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

In general, the extent of an asset's risk is determined by how much the following risk factors overlap: assets, vulnerabilities and threats.

Use the formula ***RISK = IMPACT x (THREAT x VULNERABILITY)*** to calculate the risk to the asset.

When you are assigning an asset value - use the charts given to you and make your decision according to the definitions given.

For example:
If compromise to your assets would cause grave consequences or mission failure, you know based on completed charts, that those assets will be assigned a "***Critical Value."***.

If compromise to your assets would have serious consequences resulting in the loss of classified or controlled unclassified information that would impair operations affecting national interests then you know you would assign a "***High Value."***

Assigning a ***Medium*** value indicates that a compromise to the assets would have moderate consequences resulting in loss of confidential, sensitive data or costly equipment/property.

Little or no impact on human life or the continuation of operations would constitute the assignment of a ***Low*** value.

Risk Management Process – Step 5
Determine Countermeasures

The fifth and final step in the Risk Management Process is to Determine Countermeasures. The goal of this step is to identify potential countermeasures for reducing an asset's vulnerabilities in turn reducing overall risk.

Countermeasures include:

- Manpower
- Equipment and
- Procedures

The costs of implementing countermeasures must be considered relative to the risk. Written procedures are the least expensive to implement with the costs rising for equipment and manpower.

Summary

There are no simple answers. Risk Managers must balance the benefits of risk reduction against the cost of reducing risk.

Now that you have completed the Introduction to Risk Management course you should be able to:

- Identify the steps of the Risk Management process.
- State the three analytical activities involved in the Risk Management process