010914 Webinar

Risk Management-Assessing Risks

Thank you for standing by. At this time all lines are in a "listen only" mode. Today's call is being recorded; if you have any objections you may disconnect. I would now like to turn the call over to Danny Jennings. Thank you sir you may begin.

Danny: Alright thank you ma'am.

Before we get started, please be aware that the video portion of this webinar is being recorded. Once we receive the red light to begin, we will. And they're telling me that we can go ahead and get started right now.

Good Afternoon! My name is Danny Jennings; I am the Physical & General Security Curriculum Manager here at CDSE and I will be your host for today's webinar.

First, I want to thank you for taking time out of your busy schedules to join us today. As a Curriculum Manager, some of my responsibilities include Curriculum Development, Course Instruction, and Course Review.

The topic for today's webinar is Risk Management-Assessing Risks. My producers for today are Rachel Mojo and Roy Ringrose. At this time, Rachel will provide you some instructions on how to navigate the webinar room. Rachel!

Rachel: Thank you Danny!

If you take a look at your screen in the lower left hand corner, you will find a notes box. This gives you the call-in number and other announcements as necessary. It will be on the screen for the duration of the webinar.

Over on the right, there's a Q&A box. If you have any questions or comments please enter them in this box. Your phones are muted, so this is the only way you can communicate with us.

You'll also see a file-share box, there are two files in this box. One is a Risk Management guide which Danny will be referencing during the webinar, and there are also our webinar slides. Feel free to download those, print them, and take notes as we go.

Also, Danny will be referring to some detailed tables during the webinar, and it helps to be in “full screen” mode to really see them. So just select the “full screen” button at the gray banner on the top of your screen.

Remember to select it again so that you can respond to poll questions or chat questions. At the end of the webinar we will have a poll question. This is what one looks like; just select the response and we’ll provide some feedback.

We also have several chat questions, and these boxes will sort of float in on top of the Q&A box you just insert your response and we’ll discuss. Well that concludes our tour, back to you Danny!

Danny: Alright, thank you Rachel! Let’s look at our webinar objectives. By the end of this webinar you should be able to:

- Define Risk Management
- Identify the steps in the Risk Management Process, and
- Assess Assets

But I want to bring to your attention: one of your biggest take a ways is going to be that downloadable Risk Management job aide that Rachel mentioned earlier, and it’s going to help assist in your understanding the Risk Management Process.

We’re going to start off with a chat question: In your own words, what is Risk Management? Give me some key words that you think Risk Management means to you.

Okay, assessing risks, identifying assessing risks, controlling risks, someone said balancing, assessing situations, identifying controlling risks, minimizing risks, protection of assets, vulnerability control, assessing assets, and threats.

These are all good responses. Understand that Risk Management includes several different things. It is the overarching process that encompasses identification, analysis, mitigation and implementation, tracking, and monitoring risks.

Understand that Risk Management is a systematic, documented process that identifies, assesses, and controls risks. Key word is documentation and you each have to ask yourself, how are you documenting your Risk Management process of your programs? Which leads us to our next question:

Why implement Risk Management? Why do you think we implement Risk Management?

Required to be proactive. I like being proactive, absolutely, help prevent loss and mitigate liability. Good answers! To minimize risk, safety first. I'm going to tell you that a lot of those answers encompass Risk Management.

Understand, Risk Management provides commanders with the information to make Risk Management decisions in protection of DoD assets. Those decisions involve protection requirements, resource allocations, and cost and benefit analysis.

Also, DoD policy states that commanders or directors are required to identify critical assets and their subsequent protection requirements. This includes future expenditures. Due to Risk Management process, your commanders are able to match security and protection with existing threats, therefore minimizing the waste of time, money, and effort.

It provides commanders with a tool to allocate limited resources by helping them prioritize your protection requirements. Now, you cannot establish a Risk Management program that is going to alleviate all risks, or remove all risks, but the goal is to minimize the risk to an acceptable level.

Next chat question: When should you implement Risk Management?

- Before the program is established?
- After a program is established?
- During a program existed?

Someone says always; before; before, during, and after; soon as possible in the acquisition process; which is a different form of Risk Management absolutely. It's initial and it's ongoing. These are all very good responses and I would say really for the most part all of the above.

Risk management should be implemented before, during, and after program establishment. Understand that, Risk Management is an intricate part of program management and should be incorporated in the earliest stages and throughout the planning process.

Understand that your operational environment is subject to change, meaning that your asset is going to change, your vulnerabilities, and your threats duties are going to change. Therefore Risk Management should be contingent throughout the life cycle of the program management.

There are several different Risk Management models that agencies may use to conduct risk assessments. But on it you got I think OPSEC has a Risk Management model that is out there, I think we had some questions from the last webinar.

AT has an AT Risk Management process but I'm going to tell you they all basically do some of the same things where they're going to: assess your assets, assess your threats, vulnerabilities, and give you an overall risk assessment.

Here at CDSE we use a five step model where we're going to do step 1:

1. Assess our Assets
2. Assess our Threats
3. Assess our Vulnerabilities
4. Assess Risks
5. Determine countermeasures

Providing that commander with information to make Risk Management decisions. But I want you to note that this particular specific process is not policy directed.

However, policy states that you will have a Risk Management process in place, but it does not tell you which process that you need to use.

They give that commander the flexibility to manage risk that fits his organization or unit. But once again if you do not have a Risk Management process in place, please use Risk Management job aid that CDSE has offered. This is a great tool to get you started.

We also offer Risk Management eLearning courses; I think the title of the course is Risk Management for DoD programs.

During this webinar, we will be focusing on Step 1 of this 5 step process, which is Assessing Assets. Please refer to the Risk Management job aid that will give you step by step instructions for conducting steps 2 through 5.

Step 1-assessing assets can be broken down into two parts. They are: Asset Identification and identifying the criticality of an asset.

Asset identification requires you to understand what it is you are responsible for protecting. What is on your installation or in your agency?

Understand an asset is anything of value or importance to the organization and or adversary, such as people, classified information, or strategic operations.

Use the acronym P.I.E.F.O to help you categorize your asset at a high level and curtail this to your specific agency mission. And P.I.E.F.O stands for:

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

Once again use this acronym to get you started and curtail it to your specific agency operations.

Now, a question for you. Would all these assets have the same level or protection? Absolutely not! It's impossible to protect assets at the same level.

What you want to do would be to prioritize your assets and our next chat question is: How do you prioritize your assets? Value and affect, importance, cost to replace, I see a lot of stuff that's involved in the Risk Management process. Importance and effect of loss, threat and admission, redundancy. That's a good question; I had a post question with that on there, good answer.

Understand, priority depends on the criticality of the asset. To determine criticality, you need to conduct a criticality assessment. We're going to talk about the next step to get started on that.

Asset criticality is based on three major factors:

- An assets importance to National Security
- The effect or the degree of impact of its partial or complete loss to the mission, and
- The identification of undesirable events and the impact of those undesirable events

A criticality assessment addresses the effect of temporary or permanent loss of key assets or infrastructures on the installation or the unit's ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability, and infrastructure support.

Please note, it's important that during this step to focus only on assets that are worthy of protection and are most important to your organization and the national security.

A variety of resources can be used to determine significant assets, such as, physical security plans, reports, and databases. However, the best information is attained by getting out and talking to knowledgeable personnel, or subject matter experts such as, program manager/facility managers, Chief of Operations, and Chief of Security. You want to get out and talk to those folks.

Knowing what to ask your stakeholders or subject matter experts is very important. They may or may not consider their program and or area is critical to the agency's mission. A lot of times they don't know how critical their program is, or you talk to some program managers who might think their operations are a lot more sensitive or critical than deemed appropriate.

So you want to get out there and kind of structure yourself and develop a questionnaire to help do your interview and ask these questions; get you kind of in the right direction in determining the criticality of an asset. So let's review some of these questions.

You want to ask: What critical mission activities take place at the site? You want to talk to your subject matter expert to determine what critical information in both classified and unclassified is located at the site?

What critical/valuable equipment is located at this site? And why is it critical? Why is it valuable?

What assets would be viewed as critical to an adversary? You want to look at it from an adversary's point of view as well, and not from the owner of the asset. Looking at the installation you might look at what critical infrastructure would need to be protected, kind of put a halt to that mission.

So you want to look at if you were an adversary, what you would attack. You want to find out who and what people are associated on the installation and or agency, and are they high risk personnel, contractor civilians, or are they working on special programs.

Once you have identified the significant assets, the next step is to identify potential undesirable events. Understand that the occurrence of an undesirable event is the focal point of determining asset criticality.

Here are some examples of undesirable events: Loss of life (whether through a mail bomb, assassination, or compromise of information, unauthorized disclosure, whether it's from an insider threat or foreign intelligence).

Once again assassination or loss of life, or the theft of equipment and another example would be the loss of asset through natural disaster such as hurricanes, floods, or fire.

Another note here is you have to do this process with each asset. You have to go through this process with each individual asset.

Once again you want to research, conduct interviews with your subject matter expert. Some of the questions to help guide you are:

- What undesirable events have happened in the past? You want to talk to the asset owner and find out what he or she deemed would be an undesirable event, what concerns they might have.
- What undesirable events have happened to similar assets?

Once you have identified undesirable events for each asset the next step is to determine the impact of such events. Understand when measuring impacts consider the consequences of each asset that is lost, harmed, or otherwise adversely affected. You want to use the following questions as a guide:

- Could significant damage to National Security or loss or 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?

Once you get this information, it is important that you establish a grading criteria to help you measure and evaluate it.

Here is an example of established criteria that has been placed in a table to help you evaluate and rate the criticality of an asset which is based on an undesirable event. Notice you have Linguistic Value and Numeric ratings.

Linguistic values are verbal terms that allow for categorizing the risk rating in layman's terms for briefing to commanders or management. Understand that Linguistic values are less precise than numerical ratings.

Numerical rating is used to determine the degree of criticality of an asset within each linguistic category. The numerical rating scale ranges from 1 to 100. The numeric scale allows for more effective ranking of valued assets within a given range.

If you look at the table, information that you gathered, you've got to have a grading criteria. You establish Linguistic value for low, medium, high, and critical. We also put the grading criteria in a definition to go along with the linguistic value.

We also added a numerical rating from 1-100. If you look at under the different columns the low is 1-3, medium will be 4-13, high would be 14-50, and critical would be 51-100. And this is very important: when you get to start multiplying and adding up your values to get your overall risk assessment.

An example would look like this. You would want to place it in an excel spreadsheet or a Risk Management worksheet where you will list your assets in the right hand column. For training purposes we put people, information, equipment, facility, activities, and operations. We linked that to an undesirable event. They had a category of linguistic value, and we added the numerical rating. And understand, you have to do this similar process when you're assessing threats, assessing vulnerabilities.

Let's look at the chart when it's filled in. After you do all the charts and assess your threat and assess your vulnerabilities we'll take you all the way up to step 3, where you would take that numerical rating to get your overall risk rating.

You have to do that with each individual asset. And understand, we've given you a high level overview of the process. Risk Management is not an easy task. It is very time consuming but it is important.

You have to go through this process. If you don't go through this process and you're making decisions that are not based on Risk Management. And once again, we've given you a high overview of this process, please refer to the job aid and it will give you step by step instructions on how to do each step where you evaluate your threat, evaluate your vulnerabilities and get your overall risk rating.

Once again this is the 5 step process: assessing assets, assessing threats, assessing vulnerabilities, get your numerical ratings after you do your assessments, once you get to step 4, you're going to multiply your numerical value to get your overall risk rating.

Risk equals impact, times threat, times vulnerability. You're going to have established a linguistic criteria low, medium, high, or critical for your overall risk rating.

The next step you would do is to determine countermeasures. Doing this process your countermeasures is you're going to do some cost benefit analysis. Meaning does the cost outweigh the benefits to protect this asset?

You're going to do countermeasures to help reduce the risks, your overall risk rating depending on how high that risk rating is. It is your job as a security professional to understand this Risk Management process.

Once you develop countermeasures, you're going to give the commander or the agency head, you want to give them options, so they can have information to make Risk Management decisions.

Which leads us up to our next poll question: Who determines the level of risk acceptance?

Is it you the Security Specialist?

Is it the Operations Manager?

Or is it the Commander of the Agency Head?

Somebody said Operations Manager, about 98% looking good, okay somebody else said operations manager. Most of you are saying Commander Agency Head and you would be absolutely correct. The owner of the asset would determine what is acceptable level of risk.

Now in summary we defined Risk Management, identified the steps in the Risk Management Process, and we Assess Assets. Once again we gave you a high level view, we talked through and walked through the assess asset portion of it, that was step 1.

Please utilize your Risk Management job aid to help issue steps 2 through 5. It's a great tool if you do not have a Risk Management process in place, it would help you get one started. Risk management is not an easy process, but it is a necessary one.

At this time we're going to address some of the pre questions, we may not have the chance to get to all of them but we have some pre webinar questions that were sent in and the first question was:

Question: Is DoD going to standardize the way it does Risk Management and give direction for all to follow published guidance?

Answer: I don't know the answer to that question but this is my take on it: Risk Management is Risk Management. There are different models out there to do this process, but when you really get into the weeds of it, it all kind of equates to the same thing.

I think it is designed to give commanders that flexibility to cost programs are different. DoD policy states they will have a Risk Management process in place, however, they do not tell them how to actually do that process. But if we get more information, we'll be sure to let you know.

Question: Does redundancy affect the criticality of an asset?

Answer: I would have to say you would have to go through the Risk Management process, but yes redundancy would have an effect on a criticality of an asset. Putting it in layman's terms, if you had only one asset that was very critical, then it would probably remain there, but if you had different assets or similar functions throughout, then if you loss one then you would still continue the mission. And that's my rationale on that.

At this time we would like you to let us know how we're doing. Your feedback is very important to us as we develop webinars and other types of training reaching out to our customers and our stakeholders. Want to let you know this training is actually meeting your needs, and really want a list of ideas from you to help us take care of you out in the field. So take a minute to fill out this feedback form, and we would greatly appreciate it.

Rachel: Okay, you should be able to see that survey now. Go ahead and fill that out. It may appear as a separate tab or it will show up right over top of the DCO screen. We thank you for joining us today. Handouts and frequently asked questions from this webinar will be posted on the CDSE website if you didn't have a chance to download them from the file share box, it will be online. You can also email general security

training related questions to DSS at GeneralSecurity.training@dss.mil. And we thank you for joining us today.

Danny: Absolutely guys we thank you again. We appreciate you taking time out of your busy schedule for joining us today, and appreciate your feedback on let us know how we are doing, and what training you're looking for in the future. Appreciate you joining us today. Thank you!