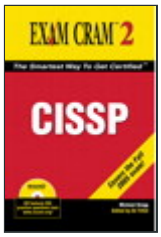
CISSP Security-Management Practices

By Michael Gregg

Oct 28, 2005

Risk

This chapter is from the book



CISSP Exam Cram 2

Learn More Buy

Assessment

A *risk assessment* is the process of identifying and prioritizing risks to the business. The assessment is crucial. Without an assessment, it is impossible to design good security policies and procedures that will defend your company's critical assets. Risk assessment requires individuals to take charge of the risk-management process. These can be either senior management or lower-level employees. If senior management is driving the process, it's considered top-down security, which is the preferred method. After all, senior management knows the goals and objectives of the company and are ultimately responsible. With senior management's support, security will gain added importance. Management can also set the tone and direction of the security program and can define what is most critical.

Bottom-up security refers to a process by which lower-ranking individuals or groups of individuals attempt to implement better security-management practices without the active support of senior management. Bottom-up security places these individuals in a situation that's unlikely to be successful. Without support from senior management, employees typically don't see risk management and good security practices as being that important. Even if these individuals can successfully determine risks and suggest good controls, they'll have a hard time procuring the needed funds for implementation.

Risk Management

Risk management is the act of determining what threats your organization faces, analyzing your vulnerabilities to assess the threat level, and determining how you will deal with the risk. Some of the major parts of risk management include developing the risk-management team, identifying threats and vulnerabilities, placing a value on the organization's assets, and determining how you will deal with the risk you uncover. The following definitions are important to know for risk management:

- **Threat**—A natural or man-made event that could have some type of negative impact on the organization.
- **Vulnerability**—A flaw, loophole, oversight, or error that can be exploited to violate system security policy.
- **Controls**—Mechanisms used to restrain, regulate, or reduce vulnerabilities. Controls can be corrective, detective, preventive, or deterrent.

Before you spend too much time struggling with all these concepts, take a moment to review Figure 3.2, which displays the relationship among threats, vulnerabilities, and controls. Notice that a threat by itself does not represent a danger and is not sufficient for a successful attack. A threat agent is required for an attack to be successful. A threat agent can be described as any circumstance or event that has the potential to cause harm to information assets through destruction, disclosure, or modification. Figure 3.2 uses an example threat of someone hacking a web server. Although it's true that anyone can attempt to attack a web server, the attacker needs a threat agent to be successful. The threat agent is described in Figure 3.2 as unpatched web server software that the attacker can access.

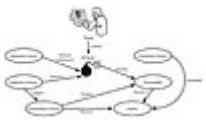


Figure 3.2 Threats, vulnerabilities, and controls.

Risk-Management Team

Don't start thinking that this is a job you are going to take on by yourself. Risk management is a big job. You'll need co-workers and employees from other departments to help. To do an effective job of risk-management analysis, you must involve individuals from all the different departments of the company. Otherwise, you run the risk of not seeing the big picture. It would be hard for any one person to understand the inner workings of all departments.

Sure, as an IT or security administrator, you understand the logical risk the IT infrastructure faces, but do you really have a grasp of the problems HR might have? These might include employee controls, effective termination practices, and control of confidentiality information. Bringing in key employees from other functional areas is required if you expect the risk management process to be successful. Consider employees from the following groups:

- Information system security
- IT and operations management
- System and network administration
- Internal audit
- Physical security
- Business process and information owners
- Human resources
- Legal
- Physical safety

Identifying the Threats and Vulnerabilities

Identifying threats and vulnerabilities is another important part of the risk-management process. Earlier we discussed how a natural or man-made threat can have some type of negative impact on the organization. Now let's look at where threats can come from. Threats can occur as a result of human or natural factors, and can be caused by internal or external events. Figure 3.3 details some common threats to security. This is not meant to be an all-inclusive list, but it should get you thinking about some of the ways in which the organization can be threatened. Threats can also occur because of many other reasons, such as errors in computer code, accidental buffer overflows, or the unintentional actions of employees.

Figure 3.3 Security threats.

Identifying threats, threat agents, and vulnerabilities is just one step of the process. Knowing the values of the assets that you are trying to protect is also important because it would be foolish to exceed the value of the asset by spending more on the countermeasure than the asset is worth. Organizations have only limited funds and resources, so countermeasures must be effectively deployed to guard what has been deemed most critical.

Without placing dollar values or using some other metric to assess these variables, how can you start to analyze the threats, vulnerabilities, and risks the organization faces? One approach is to develop a table such as the one shown in Table 3.1. This helps demonstrate the relationship among threats, vulnerabilities, and risk. For example, an intruder can represent a threat that exposes the organization to theft of equipment because there is no security guard or controlled entrance.

Table 3.1 Threat, Vulnerability, and Risk

Threat Type	Threat	Exploit/Vulnerability	Exposed Risk
Human factor internal threat	Intruder	No security guard or controlled entrance	Theft
Human factor external threat	Hacker	Misconfigured firewall	Stolen credit card information
Human factor internal threat	Current employee	Poor accountability; no audit policy	Loss of integrity; altered data
Natural	Fire	Insufficient fire	Damage or loss of

		control	life
Natural	Hurricane	Insufficient preparation	Damage or loss of life
Malicious external threat	Virus	Out-of-date antivirus software	Virus infection and loss of productivity
Technical internal threat	Hard drive failure	No data backup	Data loss and unrecoverable downtime

Placing a Value on Assets

Now, before you can really manage risk, you must know what's most valuable to the organization. You need to put a value on the organization's assets. You might be thinking that by *value*, we are discussing dollar amounts. That is one way to assess value, called *quantitative assessment*. You also have the choice to perform a *qualitative assessment*. If you choose to perform a qualitative assessment, you won't be dealing with dollar amounts because this is usually scenario driven. Qualitative and quantitative assessment techniques are described more in the following two sections.

Quantitative Assessment

Quantitative assessment deals with numbers and dollar amounts. It attempts to assign a cost (monetary value) to the elements of risk assessment and to the assets and threats of a risk analysis.

To fully complete a quantitative risk assessment, all elements of the process (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability) are quantified. Therein lies the problem with purely quantitative risk assessment: It is difficult, if not impossible, to assign dollar values to all elements; therefore, some qualitative measures must be applied to quantitative elements. A quantitative assessment requires substantial time and personnel resources. The quantitative assessment process involves the following three steps:

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

   Single loss expectancy x Asset value = Exposure factor

   Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the annual rate of occurrence (ARO). Simply stated, how many times is this expected to happen in one year?

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

   Annualized loss expectancy (ALE) x Single loss expectancy (SLE) = Annualized rate of occurrence (ARO)

When performing the calculations discussed in this section, you should include all associated costs, such as these:

- Lost productivity
- Cost of repair
- Value of the damaged equipment or lost data
- Cost to replace the equipment or reload the data

When these costs are accumulated and specific threats are determined, the annualized loss expectancy can be calculated. This builds a complete picture of the organization's risk and allows the organization to plan an effective strategy.

Review Table 3.2; we can work through the virus risk example given there. First, you need to calculate the SLE. The SLE requires that you multiply the exposure factor by the asset value:

$9,450 X .17 = $1,650

The asset value is the value you have determined the asset to be worth. The exposure factor is the amount of damage that the risk poses to the asset. For example, the risk-management team might consult with its experts and determine that 17% of its Word documents and data could be destroyed from a virus.

Next, the ARO is calculated. The ARO is the frequency at which this event is expected to happen within a given period of time. For example, the experts might have determined that there is a 90% chance of this event occurring within a 1-year period.

Finally, the ALE is calculated. The ALE is the SLE multiplied by the ARO:

$1,650 X .9 = $1,485

This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. You can interpret this figure to mean that the business should expect to lose an average of $1,485 each year due to computer viruses.

Table 3.2 How SLE, ARO, and ALE Are Used

Asset	Risk	Asset Value	Exposure Factor	SLE	Annualized Frequency	ALE
Customer database	Hacked	$432,000	.74	$320,000	.25	$80,000
Word documents and data files	Virus	$9,450	.17	$ 1,650	.9	$1,485
Domain controller	Server failure	$82,500	.88	$ 72,500	.25	$18,125
E-commerce website	DDoS	$250,000	.44	$110,000	.45	$49,500

Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.

CAUTION

A lot of math can be involved in a quantitative assessment, but the CISSP exam focuses on the SLE, ALE, and ARO formulas.

Qualitative Assessment

Maybe you are thinking that there has to be another way to perform an assessment. If so, you are right. *Qualitative assessment* is scenario driven and does not attempt to assign dollar values to components of the risk analysis. Purely quantitative risk assessment is hard to achieve because some items are difficult to tie to fixed dollar amounts. Absolute qualitative risk analysis is possible because it ranks the seriousness of threats and sensitivity of assets into grades or classes, such as low, medium, and high. An example of this can be seen in NIST 800-26, a document that uses confidentiality, integrity, and availability as categories of loss and then ranks each loss based on a scale of low, medium, and high. The ranking is subjective:

- **Low**—Minor inconvenience that could be tolerated for a short period of time.
- **Medium**—Could result in damage to the organization or cost a moderate amount of money to repair.
- **High**—Would result in loss of goodwill between the company and clients or employees. Could result in a legal action or fine, or cause the company to lose revenue or earnings.

Table 3.3 displays an example of how this process is performed. As you can see, no dollar amounts are used. Potential loss is only ranked as high, medium, or low.

Table 3.3 Performing a Qualitative Assessment

Asset	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Customer database	High	High	Medium

Internal documents	Medium	Medium	Low
Advertising literature	Low	Medium	Low
HR records	High	High	Medium

The downside of performing a qualitative assessment is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management. Another downside is that it is derived from gut feelings or opinions of experts in the company, not always an "exact assessment" that senior management will want to receive from you.

Other types of qualitative assessment techniques include these:

- **The Delphi Technique**—A group assessment process that allows individuals to contribute anonymous opinions.
- **Facilitated Risk Assessment Process (FRAP)**—A subjective process that obtains results by asking questions. It is designed to be completed in a matter of hours, making it a quick process to perform.

The NSA Information Assurance Methodology (IAM)

The NSA developed the IAM in 1998 in response to Presidential Decision Directive (PDD)-63. PDD-63 mandated that all federal computer systems be assessed to determine their overall security. The purpose of the IAM is to review an organization's INFOSEC posture, identify potential vulnerabilities, and provide recommendations on their elimination or mitigation. It uses the security triad (confidentiality, integrity, and availability) as a basis of assessment.

Handling Risk

Now that you have been introduced to some of the ways to determine risk, you are tasked with making a decision on how to deal with what you have found. Risk can be dealt with in four general ways, either individually or in combination.

- **Risk reduction**—Implement a countermeasure to alter or reduce the risk.
- **Risk transference**—Purchase insurance to transfer a portion or all of the potential cost of a loss to a third party.
- **Risk acceptance**—Deal with risk by accepting the potential cost and loss if the risk occurs.
- **Risk rejection**—Pretend that the risk doesn't exist and ignore it. Although this is not a prudent course of action, it is one that some organizations choose to take.

Which is the best way to handle risk? This depends on the cost of the countermeasure, the value of the asset, and the amount by which risk-reduction techniques reduce the total risk. Companies usually choose the one that provides the greatest risk reduction while maintaining the lowest annual cost. These concepts are expressed numerically as the following formulas:

Threat X Vulnerability X Asset value = Total risk

Total risk - Countermeasures = Residual risk

No organization can ever be 100% secure. There will always be remaining risk. The residual risk is the amount that is left after safeguards and controls have been put in place.

NOTE

What's cost-effective? The cost-effectiveness of a safeguard can be measured as follows:

ALE before the safeguard - ALE after the safeguard = Value of the safeguard to the organization

This formula can be used to evaluate the cost-effectiveness of a safeguard or to compare various safeguards to determine which are most effective. The higher the resulting value is, the more cost-effective the safeguard is.