15. What is single loss expectancy? What is annualized loss expectancy?
16. What is the difference between benchmarking and baselining?
17. What is the difference between organizational feasibility and operational feasibility?
18. What is a hybrid risk assessment?
19. What is the OCTAVE Method? What does it provide to those who adopt it?
20. How does Microsoft define "risk management"? What phases are used in its approach?

Exercises

1. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company (Asset value: $1,200,000 in projected revenues)		
Threat Category	**Cost per Incident**	**Frequency of Occurrence**
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per 6 months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Viruses, worms, Trojan horses	$1,500	1 per week
Denial-of-service attack	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

2. How did the XYZ Software Company arrive at the values shown in the table that is included in Exercise 1? For each row in the table, describe the process of determining the cost per incident and the frequency of occurrence.
3. How could we determine EF if there is no percentage given? Which method is easier for determining the SLE: a percentage of value lost or cost per incident?

4. Assume a year has passed and XYZ has improved its security. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company (Asset value: $1,200,000 in projected revenues)				
Threat Category	**Cost per Incident**	**Frequency of Occurrence**	**Cost of Controls**	**Type of Control**
Programmer mistakes	$5,000	1 per month	$20,000	Training
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security
Web defacement	$500	1 per quarter	$10,000	Firewall
Theft of equipment	$5,000	1 per 2 year	$15,000	Physical security
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus
Denial-of-service attack	$2,500	1 per 6 months	$10,000	Firewall
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups

5. Why have some values changed in the following columns: Cost per Incident and Frequency of Occurrence? How could a control affect one but not the other?
6. Assume that the costs of controls presented in the table for Exercise 4 were unique costs directly associated with protecting against that threat. In other words, do not worry about overlapping costs between threats. Calculate the CBA for each control. Are they worth the costs listed?
7. Using the Web, research the costs associated with the following items when implemented by a firm with 1,000 employees and 100 servers:
   - Managed antivirus software (not open source) licenses for 500 workstations
   - Cisco firewall (other than residential models from LinkSys)
   - Tripwire host-based IDS for 10 servers
   - Java programming continuing education training program for 10 employees
   - Checkpoint Firewall solutions