# Table of Contents

**PART I  The Treatment and Analysis of Risk**

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Vulnerability and Threat Identification</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>Risk Measurement</td>
<td>22</td>
</tr>
<tr>
<td>4</td>
<td>Quantifying and Prioritizing Loss Potential</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>Cost/Benefit Analysis</td>
<td>46</td>
</tr>
<tr>
<td>6</td>
<td>Other Risk Analysis Methodologies</td>
<td>57</td>
</tr>
<tr>
<td>7</td>
<td>The Security Survey: An Overview</td>
<td>74</td>
</tr>
<tr>
<td>8</td>
<td>Management Audit Techniques and the Preliminary Survey</td>
<td>88</td>
</tr>
<tr>
<td>9</td>
<td>The Survey Report</td>
<td>106</td>
</tr>
<tr>
<td>10</td>
<td>Crime Prediction</td>
<td>127</td>
</tr>
<tr>
<td>11</td>
<td>Determining Insurance Requirements</td>
<td>142</td>
</tr>
</tbody>
</table>

**PART II  Emergency Management and Business Continuity Planning**

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Mitigation and Preparedness</td>
<td>157</td>
</tr>
<tr>
<td>13</td>
<td>Response Planning</td>
<td>177</td>
</tr>
<tr>
<td>14</td>
<td>Business Continuity Planning</td>
<td>237</td>
</tr>
<tr>
<td>15</td>
<td>Business Impact Analysis</td>
<td>260</td>
</tr>
<tr>
<td>16</td>
<td>Plan Documentation</td>
<td>280</td>
</tr>
<tr>
<td>17</td>
<td>Crisis Management Planning for Kidnap, Ransom and Extortion</td>
<td>298</td>
</tr>
<tr>
<td>18</td>
<td>Monitoring Safeguards</td>
<td>318</td>
</tr>
<tr>
<td>19</td>
<td>The Security Consultant</td>
<td>331</td>
</tr>
</tbody>
</table>
Introduction

The outlines and sample questions in this edition of the Instructor Manual to Risk Analysis and the Security Survey are updated and revised to fit the new material and the rearranging of some topics between chapters.

In most cases we have followed the exact progression of material in the chapter;, in a few others we have varied slightly to, hopefully, enable a better oral presentation of the content.

The subject of Risk Analysis and Business Continuity Planning is changing rapidly post September 11 with the introduction of different methodologies, terminology, and increasing regulation. Competing standards vying for dominance may make issues confusing. Many of these standards are industry and country specific. The topic of third party liability is also one subject to change as court decisions will revise some of the specifics and other fine points of the law, but the basic concepts should remain the same. In the text we have tried to address these issues in a way that perpetuates the material; however, educators must keep abreast of these changing environments.

Eugene Tucker, CPP, CFE, CBCP
President and Co-author
Praetorian Protective Services®, LLC
Orinda, California
Chapter 1: Risk

Learning Objectives

- Define key terms.
- Distinguish between pure and speculative risks.
- Introduce the basic tasks required for risk analysis.
- Understand management’s role in the risk process.
- Introduce risk exposure assessment.

Presentation Outline

I. Risk

A. What is risk?
   1. Uncertainty of financial loss.
   2. Variations between actual and expected results.
   3. Probability that a loss has occurred or will occur.
Risk Analysis and the Security Survey, 3rd edition

a. ‘The thing insured.’

b. Also the possible occurrence of an undesirable event.

B. Perils are the causes of risk.

1. Examples: Fires, flood, earthquake.

C. Hazards contribute to peril.

1. Examples: Loaded gun, bunch of oily rags.

D. Risks are Speculative or Pure.

F. Three common categories of Risk:

1. Personal (people assets).
2. Property (material assets).
3. Liability (legal).

II. Risk Analysis

A. Method to estimate expected loss from an adverse event.

B. Tool to determine what management decides to accept as a loss.

C. Basic tasks:

1. Identify assets that need protection.
2. Identify risk or perils that may affect assets.
3. Determine their probability of occurrence.
4. Determine the impact if a loss occurs.

D. More art than science.
III. Advantages to Management

A. Provides information to base decisions:
   1. Prevention.
   2. Contain the effects.
   3. Do nothing.

B. Goal to strike a balance between impact and cost of countermeasures.

C. Benefits to Management:
   1. Will show current security posture.
   2. Highlight need for greater or reduced security.
   3. Develop and justify countermeasures.
   4. Increase security awareness.

D. Analysis also important at facility or system design phase.

E. Management commitment (resources) required.

IV. Role of Management.

A. Management must:
   1. Express support at all levels.
   2. Delineate purpose and scope.
   3. Select qualified team.
   4. Formally delegate authority.
   5. Review team findings.
6. Decide which recommendations to implement.

7. Establish order of priorities.

B. Threats

1. Adversely affect enterprise or assets.

2. Three classifications:
   a. Natural hazards.
   b. Accidents.
   c. Intentional acts.

3. Threat rate and probabilities developed from:
   a. Reports.
   b. Interviews.
   c. Studies in like industries.

C. Vulnerabilities

1. Weakness, flaw, or anything exploited by a threat.

2. Most easily identified by interviewing, inspections, and document review.

V. Risk Exposure Assessment

A. Risk Assessment must be completed before corrective actions taken.

B. Identify and evaluate in quantitative terms:

1. Determine types of loss or risk (perils) that can affect assets.

2. Estimate the probability of occurrence.

3. Quantify (prioritize) loss potential.
Sample Test Questions

True or False

1. Errors and Omission is best categorized as a property (material asset) risk. \textit{Answer: F (p. 3)}

2. Perils are the causes of risk. \textit{Answer: T (p. 3)}

3. Fires, floods, and earthquakes are examples of hazards. \textit{Answer: F (p. 3)}

4. A Risk Analysis cannot show the current security posture of an organization. \textit{Answer: F (p. 4)}

5. A Risk Analysis will help to increase security awareness. \textit{Answer: T (p. 5)}

6. Once a Risk Analysis is completed, it does not make sense to incorporate risk analysis into the design phase of new facilities or systems. \textit{Answer: F (p. 5)}

7. When delineating the scope of the analysis, it is improper to state what the project does not cover. \textit{Answer: F (p. 6)}

8. Historical data are never used to identify threats. \textit{Answer: F (p. 6)}
9. If a risk is unlikely to occur, it should not be considered in the Risk Analysis. Answer: F (p. 7)

10. Speculative risks are considered in the Risk Analysis. Answer: F (p. 3)

Multiple Choice

1. Which is a pure risk? Answer: a (p. 3)
   a. A risk that, overall, can only result in a loss to the organization.
   b. A night at the casino where you lose $1,000.00.
   c. A risk that has 100% probability.
   d. The stock market.

2. The common categories of risk include: Answer: c (p. 3)
   a. Gambling, total loss, risk transfer.
   b. Assets, risk transfer, liability.
   c. Personal, property, liability.
   d. Personal, property, insurance.
3. Risk Analysis is primarily:  
   \textit{Answer: a (p. 4)}
   
   a. A tool to determine what management decides to accept as a loss.
   b. A tool to decide what management must spend to remain solvent after a loss.
   c. An exact science. A tool to ensure 100% security.

4. The primary goal of Risk Analysis is to:  
   \textit{Answer: d (p. 4)}
   
   a. Identify all risks the organization may face.
   b. Justify current security expenditures.
   c. Best allocate insurance resources.
   d. Strike an economic balance between a risk’s impact and the cost of its countermeasure.

5. Subsequent Risk Analysis:  
   \textit{Answer: b (p. 5)}
   
   a. Will generally require more time and expense than the original.
   b. Will generally require less time and expense than the original.
   c. Will generally require the same amount of time and expense as the original.
   d. Should not be completed.

6. If management does not commit necessary resources to the Risk Analysis, it is usually best to:  
   \textit{Answer: a (p. 5)}
a. Delay or abandon the analysis.
b. Complete the analysis without the commitment.
c. Reduce the scope of the analysis.
d. Use an outside consultant to complete the analysis.

7. Vulnerabilities are most easily identified through: Answer: d (p. 6)

a. Interviews.
b. Inspections.
c. Document review.
d. All of the above.

8. Steps in a Risk Exposure Assessment include: Answer: d (p. 6)

a. Determine types of loss or risk.
b. Estimate the probability of occurrence.
c. Quantify (prioritize) loss potential.
d. All of the above.

9. Quantifying a loss should mean: Answer: b (p. 7)

a. Stating the loss in the number of times per year it is expected to occur.
b. Assigning a dollar value to assets.

c. Assigning it to a loss category.

d. None of the above.

10. Which of the following is true: **Answer: a (p. 5)**

   a. A larger organization will require more time to complete the risk analysis.

   b. If a risk can affect multiple buildings or assets in the same site, it should be counted more than once.

   c. Risks that don’t fit into a risk category are not included in the analysis.

   d. None of the above.

**Short Answer**

1. Discuss the differences between the terms threat, risk, hazard and peril.

   **Answer:** Hazards such as a loaded gun or a bunch of oily rags contribute to perils. Perils include fires, floods and earthquakes. Perils are the cause of risk. A threat is a term that is sometimes used interchangeably with risk and means anything that could adversely affect the enterprise or the assets. (p. 3)

2. Briefly explain the three steps to conduct a Risk Exposure Analysis.
**Answer:** In quantitative terms, determine types of loss or risk (perils) that can affect assets, estimate the probability of occurrence, and quantify (prioritize) the loss potential. (p. 6)

3. Why do we distinguish between a pure and speculative risk?

**Answer:** We have defined risk to mean the uncertainty of financial loss, the variations between actual and expected results, or the probability that a loss has occurred or will occur. A speculative risk is one that may have a positive outcome, i.e., not result in a loss. Speculative risk does not directly relate to our job responsibilities. (p. 3)

4. A newly hired security manager decides to conduct a Risk Analysis of his new company’s operations and facilities. Predict how he might fail to complete an effective analysis.

**Answer:** The question intimates that the security manager does not or did not obtain management support for the project and consequently no support was communicated to all levels of the organization. For the project to be successful, the manager must define the purpose and scope of the analysis and must select a qualified team with delegated authority to carry out their tasks. Since risk analysis is a management tool, he must have management’s involvement to review the team’s
findings and decide which recommendations need implementation and to establish the priorities of this implementation. (p. 5)

Research

1. How does the insurance industry define the terms threat, risk, hazard and peril?

Answer: The insurance industry can define these terms in a variety of ways, but they closely parallel those found in the text. A threat is the period during which the likelihood of a major loss increases rapidly, but the specific occurrence of the peril has not yet begun, for example, a weather service warning of the potential formation of a tornado. Risk is often defined as accidental loss. Some in the insurance industry define a hazard as a condition or circumstance that makes a loss more likely or severe. Perils are the cause of a loss (windstorm, hail, etc.).

Case Study

You are the corporate security manager for an international Fortune 500 corporation and have just completed a briefing to executive management trying to justify your assets protection budget. You ask if there are any questions and the CEO says, “You keep talking about minimizing risks and risk analysis, its role in management decision making.
Please explain in layman’s terms what you mean by all that.” What would you tell the CEO and other executive management at that meeting?

**Answer:** The answer should include a definition of risk, executive management’s role in risk analysis, risk exposure assessment, and what a risk analysis methodology can do for management.
Chapter 2: Vulnerability and Threat Identification

Learning Objectives

- Understand the rationale of using security surveys to gather risk information.
- The purpose of risk identification and classification is to allocate resources.
- Students will avoid some common pitfalls in the gathering of information.
- Steps used to gather data are introduced.

Presentation Outline

I. Risk Identification

   A. Risk control begins with identification and classification of risk.
   
   B. Allocates resources.
   
   C. Three considerations:
      1. Assets.
      2. Exposure.
      3. Losses.
D. Data developed through:
   1. Review policies and procedures.
   2. Insurance and risk related files.
   3. Interviews.
   4. Inspections.

E. Asset data
   1. Identify all company assets:
      a. Tangible.
      b. Intangible.
   2. Locate assets and identify exposures.
   3. Determine value:
      a. Owned.
      b. Leased.
      c. Facilities.

F. The risk identification procedure will limit the security survey or inspection.
   1. Must have the ability to recognize applicability of risk to the enterprise.

II. Problems of identification

   A. Confusing terms.

   B. Uniformity of practice.

III. Security Checklist
Chapter 2: Vulnerability and Threat Identification

A. Used to gather information for risk identification.
   1. Provides logical recording of information.
   2. Ensures no important questions go unasked.
   3. Can be in any format.

B. Broad topics to cover:
   1. Policy and Program.
   3. Control of Entry and Movement.
   5. Lighting.
   7. Alarms.
   8. Communications.
  11. Personnel Screening.
Sample Test Questions

True or False

11. Risk control has no relationship to the classification of risk. Answer: F (p. 9)

12. A major goal of risk identification and classification is the allocation of resources. Answer: T (p. 9)

13. All company assets are identified to develop asset data. Answer: T (p. 10)

14. It is not important to identify and value leased assets. Answer: F (p. 10)

15. Security checklists must be in a standard format. Answer: F (p. 12)

Multiple Choice

11. The analyst should develop information for which of the following? Answer: d (p. 9)

   a. Valuation, insurance coverage, profits.
   b. ROI, countermeasures, resources.
   c. Assets, resources, valuation.
   d. Assets, exposures, losses.
12. Data is developed through: Answer: d (p. 10)

a. A review of policies and procedures.
b. Insurance and risk related files.
c. Interviews and inspections.
d. All of the above.

13. When valuing assets, they should be broken down into these three categories: Answer: a (p. 10)

d. Owned, leased and facilities losses.
e. Direct, indirect, deferred.
f. Capitol, expense, budgeted. None of the above.

14. Which of the following risks are generally considered: Answer: d (p. 10)

a. Product liability.
b. The liability of officers and directors.
c. Crime losses
d. All of the above.

15. The purpose of a security survey is to: Answer: d (p. 12)
a. Gather information for risk identification.

b. Provide logical recording of information.

c. Ensure no important questions go unasked.

d. All of the above.

**Short Answer**

5. Information collected can be inaccurate due to the belief of some individuals that certain terms, such as robbery and burglary, are synonymous. Discuss other ways information taken from records and interviews may be inaccurate.

*Answer:* Belief in exclusivity, fraud vs. internal theft, robbery vs. internal theft, burglary vs. internal theft. Others not listed in the text could include: poor recollection, misconceptions, document fraud, incomplete records or information, sexual assault vs. rape, assault vs. battery, sabotage vs. vandalism, explosives vs. incendiary, etc. (p. 11)

6. Discuss how risk identification and classification are used to allocate resources.

*Answer:* When the risks associated with the various systems and subsystems within a given enterprise are known, the allocation of countermeasures (resources) can be more carefully planned. (p. 9)
7. List five broad topics that should be examined in a security survey.

*Answer:* The answer should be from among the following: policy and program, security organization, control of entry and movement, barriers, lighting, locks and keys, alarms, communications, property control, emergency planning, personnel screening, additional comments. (p. 12-19)

4. Which techniques are used to develop data for risk identification?

*Answer:* Review company policies, procedures (or their absence), organization, and activities to ascertain what risks have been identified and to what extent they are perceived as management responsibilities. Review insurance and risk-related files, including claims and loss records. Interviews with the heads of departments that have experienced loss exposures can develop vital information on the organization and functioning of loss-control procedures. Conducting inspections and interviewing management and other personnel in enough locations and activities will develop a complete picture of the company’s risk exposures as a basis for later evaluation of loss control procedures and their effectiveness. (p. 10)

**Case Study**
You are a security specialist who is called into the office of your boss who is the Chief Security Officer (CSO) for the company. The CSO says that, as part of developing a corporate security assets protection program, a risk management program is to be developed.

The CSO goes on to say that the program must begin with an established baseline, and that the best way to do that is to begin with a checklist to be used in conducting a security survey indicating the current status of assets protection within the company. You are asked to develop that checklist. Develop that checklist in as much detail as you believe is needed to provide an overall baseline.

**Answer:** The answer should include the following major sections:

- **Policy and program**
- **Security organization**
- **Control of entry and movement**
- **Barriers**
- **Lighting**
- **Locks and keys**
- **Alarms**
- **Communications**
- **Property control**
- **Emergency planning**
- Personnel screening
- Additional comments
Risk Analysis and the Security Survey 3rd edition

Chapter 3: Risk Measurement

Learning Objectives

- Risk can be expressed in terms of probability of occurrence.
- Annual Loss Expectancy calculations and alternate methods to express the values are illustrated.
- Students will understand the principals of probability.
- How probability applies to risk measurement is discussed.
- Students will apply the principals of Risk Measurement to effective security solutions.

Presentation Outline

I. Introduction

   A. Risk measurement used later to determine the cost of an unfavorable event.
   B. Aids in predicting how often an event may occur in a given time period.
C. Two necessities:

1. Quantitative means to express cost.
2. Logical expression of frequency of occurrence.
   a. Year most logical time period because of budget cycles.

II. Cost Valuation and Frequency of Occurrence

A. Unnecessary to make precise statements of impact and probability.

B. Impact and frequency simplified into factors of 10.

C. Annual Loss Expectancy (ALE):

1. \( ALE = 10^{(f \cdot i) / 3} \).
2. \( i \) = cost valuation (impact).
   a. If $10 value then \( i = 1 \) to $100,000,000 then \( i = 8 \).
3. \( f \) = frequency of occurrence.
   a. If occurs once in 3,000 years then \( f = 1 \) to 100 times/day then \( f = 8 \).
4. Alternate method (table).
5. Commonality of events.
   a. Access.
   b. Natural disasters.
   c. Environmental hazards.
   d. Facility housing.
   e. Work environment.
   f. Value.
III. Principals of Probability

A. Risk is the possible happening of an undesirable event.

B. An event is a definable occurrence and can be described in two ways:
   1. In terms of the damage it will present if it occurs.
   2. In terms of the probability of its occurrence.

C. A Risk should be described in terms of its potential occurrence and its capacity for potential loss.

D. Probability is the study of the possibility of occurrence.

E. Probability is based on philosophical (rather than mathematical) proofs derived in 1792 by the Marquis de Laplace.

F. The ten principals:
   1. Probability is defined as the ratio of the number of favorable cases to all possible cases.
   2. If the cases are not equally possible then the probability is the sum of the possibilities of each favorable case.
   3. When the events are independent of each other, the probability of their simultaneous occurrence is the product of their separate probabilities.
   4. If two events are dependent on each other, then the probability of the combined event is the product of the probability of the occurrence of the first event and the probability that the second event will occur given the occurrence of the first event.
5. If the probability of a combined event first phase and that of the second phase is determined, then the second probability divided by the first is the probability of the expected event drawn from an observed event.

6. When an observed event is linked to a cause, the probability of the existence of the cause is the probability of the event resulting from the cause divided by the sum of the probabilities of all causes.

7. The probability that the possibility of an event falls within given limits is the sum of the fractions [#6 above] falling within these limits.

8. The definition of *mathematical hope* is the product of the potential gain and the probability of obtaining it.

9. In a series of probable events, of which some produce a benefit and the others a loss, we shall have the advantage that results from it by making a sum of the products of the probability of each favorable event by the benefit that it procures, and subtracting from this sum that of the products of the probability of each unfavorable event by the loss that is attached to it. If the second sum is greater than the first, the benefit becomes a loss and hope is changed to fear.

10. Moral hope is defined as the relation between its absolute value divided by the total assets of the involved entity. This principle deals with the relation of potential gain to potential loss and describes the basis for not exposing all assets to the same risk.
IV. Probability, Risk, and Security

A. The goal of security design is to decrease the ratio of unfavorable events to total events.

B. Similar events in different locations – add the ratios of favorable cases where the probabilities are different.

C. Two events that have no relation to each other are considered to be independent:
   1. Lightning striking twice is one example.
   2. Security penetration and simultaneous security system failure is another example.
   3. Applies to principal #3.

D. Principle 4 expresses the relation between dependent events (probability of the first event is multiplied by the probability of the second event if the second event).
   1. Breaking and entering followed by theft, to produce a burglary, is an example.

E. Past events do not affect future events (principal #5).
   1. Cannot assume that a security breach will not occur again.
   2. Probabilities of events are not guarantees.

F. Principal #6 describes the relation between all causes and probable causes.
   1. Circumstantial evidence, for example.

G. Principal 7 involves the basis of confidence limits.
H. Mathematical hope relates the potential gain to the probability of obtaining the gain (principal 8).
   1. Allows the utility of a procedure to be expressed in both monetary and probabilistic terms.
I. Principle 9 allows for the fact that any solution to a problem introduces risk (i.e., it may fail).
J. Principle 10 relates the amount and potential of risk to the wealth of the protected entity.
   1. Solution could be to do nothing.

V. Estimating Frequency of Occurrence

A. Loss expectancy can be projected with a satisfactory degree of confidence.
   1. Must have sufficiently large database or becomes educated guess.
Sample Test Questions

True or False

16. Events with long recurrence rates such as a ‘three hundred year flood’ cannot be expressed in annual terms when measuring risk. *Answer: F (p. 21)*

17. Laplace’s principals of probability are based on mathematical proofs. *Answer: F (p. 24)*

18. Laplace developed 15 principals of probability. *Answer: F (p. 24)*

19. When the events are independent of each other, their combined probability cannot be calculated. *Answer: F (p. 25)*

20. A risk analysis cannot be accurately completed without the application of detailed principals of probability. *Answer: F (p. 21)*

21. The goal of security design is to decrease the ratio of unfavorable events to favorable events. *Answer: F (p. 25)*

22. The high probability of an event is a guarantee that it will occur. *Answer: F (p. 25)*
23. The risk management solution of doing nothing about a risk cannot be justified by using the principals of probability.  
   \textit{Answer: F (p. 26)}

24. Annual loss expectancy (ALE) is the product of probability and frequency.  
   \textit{Answer: F (p. 22)}

25. The use of probability will help balance conclusions based on very small data sets.  
   \textit{Answer: F (p. 27)}

\textbf{Multiple Choice}

16. An annual time period is used to express frequency because it:  
   \textit{Answer: a (p. 21)}

\hspace{1cm}a. Coincides with budget cycles.
\hspace{1cm}b. Provides sufficient time to draw statistical inferences.
\hspace{1cm}c. Accounts for all four seasons.
\hspace{1cm}d. Crime statistics are tracked annually.

17. Annual loss expectancy is expressed as:  
   \textit{Answer: b (p. 22)}

\hspace{1cm}a. Probability times value.
\hspace{1cm}b. $10^{(f+3)/3}$.
\hspace{1cm}c. Annual loss divided by 12.
d. The statistical mean of the Minimum and Maximum Expected Loss of each event added together.

18. Probability is defined as:  \textit{Answer: c} (p. 24)

   g. A mathematical guess.
   h. The ratio of all probable outcomes to the number of attempts.
   i. The ratio of the number of favorable cases to all possible cases. The ratio of the number unfavorable cases to all possible outcomes.

19. The definition of \textit{mathematical hope} is:  \textit{Answer: d} (p. 24)

   a. The ratio of all probable outcomes to the number of attempts.
   b. A statistical extrapolation when probability cannot be accurately predicted.
   c. An alternate definition for probability.
   d. The product of the potential gain and the probability of obtaining it.

20. The principle that deals with the relation of potential gain to potential loss and describes the basis for not exposing all assets to the same risk is:  \textit{Answer: a} (p. 24)

   a. Moral hope.
   b. Mathematical hope.
   c. Mathematical fear.
21. Two events that have no relation to each other are considered to be: \textit{Answer: b} (p. 25)

a. Not statistically predictable.

b. Independent.

c. Insignificant.

d. None of the above.

22. The probability of lightning striking in the same place twice is: \textit{Answer: c} (p. 25)

a. The probability of the first strike times two.

b. The probability of the first strike divided by two.

c. The same as lightning striking the first time.

d. Lightning cannot strike in the same place twice.

23. When dealing with the probability of events: \textit{Answer: d} (p. 25)

a. Determine types of loss or risk.

b. The probabilities of historical events are added together.

c. Past events affect the probability of future events.

d. The past does not affect the future.
24. Which of the following is true?  \textit{Answer: a (p. 22)}

e. ALE can be determined by referring to a matrix.

f. ALE must be an exact calculation.

g. ALE is the only way to measure risk.

h. ALE is the same as Maximum Probable Loss.

25. It is better to describe risk:  \textit{Answer: a (p. 24)}

5. In terms of its potential occurrence and its capacity for potential loss.

6. In terms of its occurrence.

7. In terms of its capacity for loss.

8. In terms of its probability.

\textbf{Short Answer}

1. Discuss why we state the impact of an adverse impact in financial terms.

\textit{Answer:} According to the text, there is no better way to state the impact of an adverse circumstance — whether the damage or cost is actual or abstract, or the victim a person, a piece of machinery, or the entire facility — than to assign it a monetary value. Ascertaining the cost of any adverse event is the logical way to
equate value in our society. For a company that is concerned with cost, it is the only way. (p. 21)

2. Why is it neither necessary nor desirable to make precise statements of impact and probability?

*Answer:* The time needed for the analysis will be considerably reduced, and its usefulness will not be decreased, if impact \((i)\) and frequency \((f)\) correlations are given in factors of ten. It does not really matter to the overall estimation of threats whether the cost of the threat is valued at $110,000 or $130,000, or whether the anticipated frequency is eight or twelve times a year. What is necessary in the beginning is simplifying the measurement and quantification process, for reasons of efficiency and speed. This will facilitate the task by decreasing the amount of time spent on the analysis. (p. 21)

3. List some of the common factors that deserve consideration when gaining an understanding of the elements that may affect frequency estimation in risk measurement.

*Answer:* Access, natural disasters, environmental hazards, facility housing, work environment, value. (p. 23)

4. Your facility that can anticipate one fire every 10 years is located next to another facility that expects one fire every 20 years. Because of the prevailing wind conditions, hot
embers were blown onto your facility from this 20-year fire. The impact from the 10-year fire averages $1,000,000. Compute the approximate annual loss expectancy and apply the principals of probability to show how the situation above may affect the ALE.

**Answer:** The approximate annual loss expectancy is $30,000. There is no effect on this figure from fires located at the adjacent facility because no historical loss data is given and mitigating factors that may affect frequency and risk measurement, such as improvements to the fire resistance of the building and surroundings, are not discussed. The probabilities of their simultaneous occurrence as described in Laplace’s principal of independent events could affect the frequency by multiplying their separate probabilities, but one could argue that since the embers have blown onto the facility in the past, probability does not guarantee they will do so in the future. (Chapter 3)

**Case Study**

As the corporate security manager, you decide to hold a staff meeting and explain to your staff that you want to develop a risk management program, which will include estimating the potential for the loss of assets. You explain to the staff that in the risk management program the probability of adverse impact to corporate assets can be viewed by looking at the cost valuation (impact) of the assets and the potential or estimated frequency of occurrence of an adverse event. You explain to them that the annual loss expectancy (ALE) is the product of impact and frequency. When using the values of $f$ and $i$, you can compute the annual loss
expectancy of an asset. The formula you can use is: \( ALE = 10^{(f+i-3)/3} \). Your staff looks at you, bewildered. So, you decide to explain the formula and how to use it.

- What explanation would you give so that your staff understands that formula?
- Provide an example of how to use the formula.
- Develop a matrix using the formula as part of your example.

*Answer:* See pages 21-25 of the text.
Chapter 4: Quantifying and Prioritizing Loss Potential

Learning Objectives

- Students will understand risk quantification.
- When to accept or to minimize risk.
- Assessing Criticality or Severity.
- How to prioritize risk.
- Considerations in the selection of security solutions.

Presentation Outline

I. Introduction

A. It is necessary to quantify and prioritize loss potentials to establish conclusions and recommendations for corrective action.

B. Many risks may be classified as things that might happen but that have not yet occurred.
1. Such risks can either be accepted or minimized.

2. Acceptance assumes that the risk is:
   a. Not sufficiently serious to justify the cost of reduction.
   b. That recovery measures will ensure survival.
   c. That cessation of operations is an acceptable alternative.

3. Minimizing the risk presupposes that:
   a. It may be serious enough to justify the cost of eliminating or reducing the possibility of its occurrence.
   b. Recovery measures alone will not always be effective in ensuring survival.
   c. Cessation of operations is unacceptable.

C. Trade-offs to establishing new systems:
   a. Cost.
   b. Inconvenience.

II. Assessing Criticality or Severity

A. Approximate dollar values for the loss probabilities previously identified.

B. Find meaningful solutions with priorities based on a common denominator.

C. Three-stage approach:
   a. Prevention attempts to stop undesirable incidents before they get started.
   b. Control seeks to keep these incidents from impacting assets, or to minimize the loss.
   c. Recovery restores the operation after assets have been adversely affected.
D. Another technique prepares a segmented schedule of overhead, installation, and operating costs:
   a. All costs identified must be directly chargeable to expected benefits.
   b. Crucial to show that the benefits (risk prevention or reduction) will outweigh the cost.
   c. Referred to as a cost/benefit summary.

III. The Decision Matrix.

A. Another technique for prioritizing loss potential.

B. Uses the adjectives high, medium, and low as factors to measure both frequency and severity of loss.

C. Quantification and prioritizing of loss potential account for “intuitive” security control concepts and detailed cost/benefit analysis.

   1. Both must consider:

      a. Available information resources.
      
      b. Reliable probability relationships.
      
      c. Minimum time and resource requirements and availability.
      
      d. Maximum incentives for management cooperation.
      
      e. A realistic evaluation of existing or planned security control effectiveness.

D. Application of controls makes sense to the environment and reality of the entity studied.

E. Order-of-magnitude expressions indicate relative degrees of risk:
1. “Low,” “moderate,” and “high” equate with probability ranges of 1–3, 4–6, and 7–10, respectively.

2. Low risk should be taken seriously if the potential damage (or danger) is assessed as being moderate to high.
Sample Test Questions

True or False

26. It is necessary to quantify and prioritize the loss potentials to establish correct conclusions and then to make recommendations for corrective action. \textit{Answer: T} \hspace{1em} (p. 29)

27. Many risks may be classified as things that might happen but that have not yet occurred. \textit{Answer: T} \hspace{1em} (p. 29)

28. Costs and inconvenience are tradeoffs to establishing a new security system. \textit{Answer: T} \hspace{1em} (p. 30)

29. Criticality is the identification of the loss probabilities of events or conditions. \textit{Answer: F} \hspace{1em} (p. 30)

30. A technique for assessing security is to prepare a segmented schedule of overhead, installation, and operating costs for the security project. \textit{Answer: T} \hspace{1em} (p. 30)

31. The use of a decision matrix is an acceptable way to prioritize loss potential. \textit{Answer: F} \hspace{1em} (p. 31)
32. Application of controls is independent of the environment and reality of the entity studied. *Answer: F* (p. 31)

33. Order-of-magnitude expressions, such as low, moderate, and high, are more than adequate for most risk-control surveys. *Answer: T* (p. 32)

34. Low risk should be taken seriously if the potential damage (or danger) is assessed as being moderate to high. *Answer: T* (p. 32)

35. A cost/benefit summary may show that the benefits (risk prevention or reduction) will outweigh the cost. *Answer: T* (p. 30)

**Multiple Choice**

1. The misapplication of controls without regard to risk in the real-world environment often results in controls that are: *Answer: d.* (p. 31)

   b. Inappropriate.
   c. Ineffective.
   d. Costly.
   e. All of the above.
2. Acceptance of a risk assumes: \textit{Answer: d (p. 29)}

a. That the risk is not sufficiently serious to justify the cost of reduction.

b. That recovery measures will ensure survival.

c. That cessation of operations is an acceptable alternative.

d. All of the above.

3. Minimizing the risk presupposes that: \textit{Answer: d (p. 29)}

j. It may be serious enough to justify the cost of eliminating or reducing the possibility of its occurrence.

k. Recovery measures alone will not always be effective in ensuring survival.

l. Cessation of operations is unacceptable. All of the above.

4. The three-stage approach to security solutions includes: \textit{Answer: a (p. 30)}

a. Prevention, control, and recovery.

b. Risk identification, loss potential, and criticality.

c. Risk acceptance, risk minimization, and risk control.

d. None of the above.

5. Quantification and prioritizing of loss potential should account for: \textit{Answer: d (p. 31)}

Copyright 2006 © Elsevier, Inc. All rights reserved.
a. Reliable probability relationships.

b. Maximum incentives for management cooperation.

c. A realistic evaluation of existing or planned security control effectiveness.

d. All of the above.

**Short Answer**

4. Discuss the outcome where there are insufficient data for reliable forecasting because the data either have not or cannot be collected.

*Answer:* Where there are insufficient data for reliable forecasting because the data either have not or cannot be collected, the conclusions will be nothing more than exercises in educated guessing. Since much of this process is an educated guess, this may not be a negative in all cases. (p. 29)

5. When would you accept a risk or minimize a risk?

*Answer:* Acceptance assumes that the risk is not sufficiently serious to justify the cost of reduction, or that recovery measures will ensure survival, or that cessation of operations, if the risk should occur in its most serious magnitude, is an acceptable alternative. Minimizing the risk presupposes that it is or may be serious enough to justify the cost of eliminating or reducing the possibility of its occurrence, and that recovery measures alone will not always be effective in
ensuring survival. Also, it postulates that the remaining alternative — cessation of operations — is unacceptable. (p. 29)

6. How can a security solution cause more ‘harm’ than good?

\textit{Answer}: Cost, inconvenience, probable impact on employee morale, especially if the employees perceive (rightly or wrongly) that the inconvenience caused them is greater than the threat. (p. 30)

4. Differentiate the best way to handle the following risks:

High Severity, High Frequency; High Severity, Low Frequency; Medium Severity, and a risk with a probability range of 4-6; Low Severity, High Frequency; Low Severity, Low Frequency.

\textit{Answer}: Risk avoidance is used to handle a risk that has a high severity and high frequency; risk transfer is used for high severity, low frequency; loss prevention and risk transfer is used to handle a medium severity, medium frequency risk; loss prevention for low severity, high frequency; and risk assumption for a low severity, low frequency risk. (p. 31-32)

\textbf{Case Study}
As the corporate security manager working with your inexperienced staff to develop a risk management program, you have introduced them to the quantitative approach using the annual loss expectancy (ALE) formula. Your staff is confused as to how to actually use this quantitative method. Therefore, you decided that a qualitative method may be easier for them to use. Once experience is gained in using that method and the staff understands the philosophy behind it, you can reintroduce the quantitative method to them. You explain to your staff that the qualitative method consists of using an estimated frequency-of-loss approach. The risk management model will use the adjectives high, medium, and low as factors to measure both frequency and severity of loss. Develop a decision matrix model to be used as a risk-handling decision aid and give an example of its use.

*Answer:* See pages 30-32 of the text.
Chapter 5: Cost/Benefit Analysis

Learning Objectives

- Students introduced to the cost/benefit analysis of security systems.
- Elements of a good security program and system design are introduced.
- Understand techniques to avoid system over design using a phased approach.
- The selection of security countermeasures is further developed.
- The importance of redundancy from an overall system perspective is understood.
- Competitive vs. sole source bidding for security equipment and serviced is outlined.

Presentation Outline

I. Introduction

   F. Efficiency versus cost is the first phase of balancing the cost/benefit ratio.
      1. Consider only solutions responsive to a demonstrated need or requirement.
2. Use only tools or techniques that perform the task effectively at the least possible cost.

II. System Design Engineering

A. Elements of a security program are adequate, inadequate, or nonexistent.

B. A good system design consists of the following elements:
   1. Written policy, procedures, and guidelines.
   2. Hardware (lock and key controls, card access, anti-intrusion alarms).
   3. Manpower (guard service or security personnel).

C. Three basic criteria must be considered before the proper procedure or countermeasure is selected:
   1. Cost.
   2. Reliability.
   3. Delay.

D. Cost:
   1. Initially concerned with acquisition cost.
   2. Must also consider life cycle cost factors.
   3. Must also consider replacement cost factors.

E. Reliability:
   1. Reliability is critical with hardware and electronic devices.
   2. Inspect the installation of a like unit with the same problems or environment.
3. Include a clause in the purchase contract to withhold final payment until the end of a sufficient test period.

F. Delay.

1. Time delay to implement.

2. Overlapping countermeasures.

3. Guard costs:

   a. 4.2 guards 24 hours, 7 day per week.

III. Building Redundancy into the System

A. Achieves very high levels of reliability in security programs.

B. Examples of redundancy:

   1. Multi-technology sensors.

   2. Redundant system monitoring (in-house and central station).


   4. Redundant systems (i.e., camera watching alarmed area).

C. Decreases odds of total system failure.

D. Increases odds of detection.

E. Makes circumvention difficult.

F. Written procedures are less expensive than hardware, but hardware is less expensive than manpower.

G. May be necessary to use redundancy to design an adequate system.
IV. Security Countermeasures

A. Implementation in phases.

B. Cost out each system in terms of the minimum level of security that one or more will provide.

C. Add more security measures to each phase, adding ever-increasing cost to the project’s countermeasures plan.

D. Prevent system over design.

E. Cost-effective security systems use a combination of manpower and hardware to achieve the proper countermeasures balance.

F. Must be cost-effective before ‘sold’ to management.

G. Use competitive bidding with security vendors:

   1. Inform bidders of competitive process but not of other bidders.
Sample Test Questions

True or False

36. Efficiency versus cost is the first phase of balancing the cost/benefit ratio.  \textit{Answer: T} (p. 33)

37. Elements of a security program are either: adequate, inadequate, or cost-effective.  \textit{Answer: F} (p. 33)

38. When figuring costs, you are concerned with acquisition, life cycle, and replacement factors.  \textit{Answer: T} (p. 34)

39. It is considered unprofessional to include a clause in a purchase contract withholding the last payment until the system has been on line for a sufficient test period.  \textit{Answer: F} (p. 34)

40. Generally speaking, hardware costs are less expensive than manpower costs.  \textit{Answer: T} (p. 35)

41. The design of a security system should never be done in phases.  \textit{Answer: F} (p. 36)
42. One method to prevent the overdesign of security systems is to design it in phases.

*Answer: T* (p. 37)

43. Most cost-effective security systems use a combination of manpower and hardware (electronics) to achieve the proper countermeasures balance. *Answer: T* (p. 37)

44. The average monthly cost of a security officer 24 hours per day, 7 days per week at $9.50 per hour is $7,068. *Answer: T* (p. 35)

45. It is often correct to start with basic countermeasures and then work up to the more complex and, thus, more costly countermeasures. *Answer: T* (p. 36)

**Multiple Choice**

6. A good system design consists of the following elements: *Answer: d. (p. 33-34)

   a. Procedures.

   b. Hardware.

   c. Manpower.

   d. All of the above.

7. Three basic criteria that must be considered before the proper procedure or countermeasure is selected are: *Answer: a. (p. 34)
a. Cost, reliability, and delay.
b. Cost/benefit, redundancy, and competitive bidding.
c. Procedures, overlapping countermeasures, and cost.
d. Cost, redundancy, and alternates.

8. When staffing a guard post 24 hour per day, seven days per week, you will need how many personnel per week if staffed for 1 year? *Answer: b* (p. 35)

m. 4.
n. 4.2.
o. 4.9. 5.4.

9. ‘CC&Rs’ means: *Answer: a* (p. 37)

e. Codes, Covenants, and Restrictions.
f. Control, Costs and Restrictions.
g. Countermeasures, Costs and Restrictions.
h. Criticality, Controls, and Reliability.

10. Building redundancy into a system: *Answer: d* (p. 36)

a. Decreases odds of total system failure.
b. Increases odds of detection.
c. Makes circumvention difficult.

d. All of the above.

**Short answer**

7. Discuss reasons why some electronic systems can be unreliable.

The state of the art in electronics systems is advancing quickly; units are being manufactured, distributed, and installed before being properly field-tested. (p. 34)

8. What are the advantages and disadvantages to sole source bidding on security vendor contract proposals?

**Competitive bids are not only a proven, cost-effective technique, but they tend to keep everyone honest.** Sole-source procurement is seldom cost effective and more often than not provides fertile ground for financial manipulation, which is seldom in the client’s best interest. (p. 38)

9. List methods to help ensure the reliability of electronic systems.

**Building redundancy into the system and field-testing will help ensure the reliability of electronic systems.** Also, the inspection and demonstration of a like unit installed on a property with the same or similar security or access-control...
problems will help ensure reliability. Including a clause in the purchase contract withholding the last payment until the system has been on line for a sufficient test period, to ensure that the product is problem free and all bugs have been located and eliminated, will also help. (p. 34)

Research

Using the material in Appendix H and from other sources, craft a sample security system specification for an integrated access control and alarm system.

See Appendix H. The specification should include at least the following elements:

Cover letter

Bidders Conference information  
Contract award date and/or other deadlines or milestones

Introduction

Scope of Work

System Requirements (Description of System)

Installation Requirements

User Requirements

Case Study

You are the corporate security manager of a large corporation. You have been told by your boss that your budget for the next year is being reduced; you must continue to provide the same level
of service and, at the same time, find ways to live within your budget. You know that the highest budget costs are related to employees. Your staff is already working at a very efficient and effective level. Reducing staff would mean reducing security service and support, which you must try not to do.

You decided to therefore look at outsourcing some of the security functions. Because the guard force accounts for the majority of your employees, you decided to look at outsourcing the guard services first. As part of the process of determining whether or not outsourcing would be cost beneficial, you must know what the guard force costs you on an annual basis.

You know that each guard post is a 24/7 operation and with breaks, sick time, and vacations; you know that for each guard post you require 4.2 guards on a 24-hour shift. You have 12 guard posts. Each guard receives an average pay of $9.75 an hour. According to the Human Resources staff, the benefits paid to each guard cost the corporation $2,135 per year.

In coordination with the corporate contracts office staff, you have already gone out for bids to five security guard service providers. However, you must be able to compare their bids with the costs you are already incurring with your proprietary guard force. Based on the previous information, you will compare the bids with the total costs of your proprietary guard force. What is the annual cost of your guard force considering benefits and without considering benefits?

**Answer:** The answer is a simple mathematical answer of multiplication, as shown on page 35 of the text.
Chapter 6: Other Risk Analysis Methodologies

Learning Objectives

- Other risk analysis methodologies exist and are mandated by US Federal Law.
- Although similar in nature, differences in methodologies exist.
- Major methodologies include RAM/VSAT, Operational Risk Management, and CARVER + Shock.

Presentation Outline

I. Critical Infrastructure Protection

   A. Presidential Directive 63 defined sectors of economy.
   
      
      1. Each uses different assessment methodology.
      
      2. Similar but different.
II. Vulnerability Self Assessment Tool – VSAT

A. Assessment tool and software program.

1. Protects specific targets from specific acts.

2. Considered qualitatively-based (asset-based) methodology.

3. Goals are to:
   a. Assess vulnerabilities.
   b. Develop priorities based on cost and feasibility of remediation.
   c. Determine solutions for prioritized vulnerabilities.

B. Developed for water, wastewater and process intensive systems.

C. Organizes vulnerabilities into a color coded threat matrix.

D. Uses baseline assessment and improvement analysis to compute Risk Reduction Units.

E. Eleven-step process:

1. Identify assets and assign categories:
   a. Physical.
   b. People.
   c. Knowledge base.
   d. Information Technology.
   e. Customers.

2. Identify assets:
   a. Assess if threats pose risk to each asset.
   b. Consider extent of threat.

3. Determine criticality:
a. Low to Very High.

b. Defined in context of specific environment.

4. Identify existing countermeasures.

5. Determine probability of failure.

6. Assign vulnerability:
   a. Probability of failure and occurrence.
   b. Measures likelihood of threat and ability to cause damage.

7. Determine acceptability of risk:
   a. Red = unacceptable.
   b. Yellow = managerial decision.
   c. Green = accepted.

8. Develop new countermeasures.

9. Perform risk-cost analysis:
   a. Simple method.
   b. Debt Payment method.

10. Develop business continuity plan.

F. Allows cost vs. risk comparison.

III. Operational Risk Management (ORM)

A. Engineering based risk management system:
   1. Used by Federal Aviation Administration (FAA) and military.
   2. Identifies operational risk and benefits.
   3. Adopted by FDA for use in food security and safety.
B. ORM defined.

C. Identifies hazards and impact through probability and severity.

D. Allows focus on worst hazard first.

E. ‘Defensive’ assessment tool.

F. Six-step process:

1. Identify hazards in operations.

2. Assess the risk:
   a. Determine probability, severity, and exposure.
   b. Probability defined as:
      i. Frequently: takes place often, and persons are continuously exposed.
      ii. Likely: takes place several times, and persons are regularly exposed.
      iii. Occasional: will happen, and exposure is sporadic.
      iv. Seldom: may happen, and exposure is infrequent.
      v. Unlikely: likelihood and exposure are rare.
   c. Severity defined as:
      i. Catastrophic: complete business failure or loss of facility asset due to attack resulting in fatalities.
      ii. Critical: major business impact resulting from severe illnesses or incident.
      iii. Moderate: minor business impact resulting from minor illnesses or incident.
      iv. Negligible: less than minor business impact or illness.
   d. Risks are then ranked using a matrix.

3. Analyze Risk Control Measures.

5. Implement Risk Controls.

6. Supervise and Review.

G. ORM principals:

1. Accept no unnecessary risk.

2. Make risk decisions at the appropriate level.

3. Accept risk when the benefits outweigh the costs.

4. Integrate ORM into planning at all levels.

IV. CARVER + Shock

A. Identifies vulnerabilities from a terrorist’s point of view.

B. Offensive military target prioritization tool.

C. Considers seven factors:

1. Criticality.

2. Accessibility.

3. Recuperability.

4. Vulnerability.

5. Effect.

6. Recognizability.

7. Shock.
Sample Test Questions

True or False

46. Presidential Directive 63, the Policy on Critical Infrastructure Protection, was signed prior to September 11, 2001.  
   Answer: T  (p. 39)

47. The critical infrastructure is the sectors of the economy considered critical to national security.  
   Answer: T  (p. 39)

48. The supply of clean and safe water is considered a critical infrastructure.  
   Answer: T  (p. 39)

49. Presidential Directive 63 mandated the use of a consistent risk analysis methodology for all critical infrastructure.  
   Answer: F  (p. 39)

50. The Vulnerability Self Assessment Tool is considered to be a quantitative methodology.  
   Answer: F  (p. 40)

51. Risk Identification Units are used as part of the Vulnerability Self Assessment Tool.  
   Answer: F  (p. 40)
52. Operational Risk Management is a methodology commonly used by the Environmental Protection Agency (EPA). \textit{Answer: F} (p. 42)

53. Operational Risk Management is defined as an offensive vulnerability assessment tool. \textit{Answer: F} (p. 42)

54. In the Operational Risk Management methodology, it is not assumed that a singular person or department is the best decision maker to implement controls. \textit{Answer: T} (p. 43)

55. CARVER + Shock is a military targeting methodology. \textit{Answer: T} (p. 44)

\textbf{Multiple Choice}

11. Which of the following is not an example of critical infrastructure? \textit{Answer: d} (p. 39)

e. Banking and Finance.

f. Utilities (gas and electric).

g. Emergency services.

h. Intelligence.

12. The Vulnerability Self Assessment Tool was developed from which methodology: \textit{Answer: a} (p. 40)

b. Operational Risk Management.

c. CARVER + Shock

d. Shock.

13. Which of the following methodologies identifies existing countermeasures to understand the level of vulnerability? \textit{Answer: a}  \hspace{1em} (p. 41)

p. Vulnerability Self Assessment Tool

q. Operational Risk Management.

r. CARVER + Shock None of the above.

14. The Vulnerability Self Assessment Tool requires the analyst to identify and group assets into five categories that include: \textit{Answer: d}  \hspace{1em} (p. 41)

i. Physical, People, Expendable, Information Technology, and Vulnerable.


k. Physical, People, Operational, Information Technology, and Financial.

l. Physical, People, Knowledge Base, Information Technology, and Customers

15. The Vulnerability Self Assessment Tool requires the analyst to: \textit{Answer: c}  \hspace{1em} (p. 41)
a. Consider the length of an exposure.

b. Consider the ability of the system to recover from an attack.

c. Determine the probability of the failure of existing countermeasures when pitted against the threats.

d. Determine the risk of loss resulting from inadequate or failed processes.

16. Levels of risk acceptability in the Vulnerability Self Assessment Tool are represented by which of the following:  
   Answer: d (p. 41)

   a. Red represents unacceptable risk.

   b. Yellow represents a managerial decision to accept an unacceptable risk.

   c. Green represents no risk.

   d. a and b.

17. Operational Risk Management, in part, allows the manager to:  
   Answer: a (p. 42)

   a. Focus on the worst hazard first.

   b. Assign Risk Reduction Units.

   c. Satisfy the requirements of the Environmental Protection Agency (EPA).

   d. Integrate Operational Risk Management with the Vulnerability Self Assessment Tool.
18. In Operational Risk Management, an example of a process can include: \textit{Answer: b} (p. 42)

\begin{itemize}
  \item[a.] Intentional contamination of food.
  \item[b.] Serving food to customers.
  \item[c.] The continuous evaluation of program effectiveness.
  \item[d.] The growth of a pathogen.
\end{itemize}

19. When discussing the severity of an attack, Operation Risk Management assigns which categories? \textit{Answer: c} (p. 43)

\begin{itemize}
  \item[a.] Very high, high, medium, and low.
  \item[b.] Red, Yellow, and Green.
  \item[c.] Catastrophic, critical, moderate, or negligible.
  \item[d.] System failure, recoverable damage, some effect, no effect.
\end{itemize}

20. CARVER is intended to: \textit{Answer: d} (p. 44)

\begin{itemize}
  \item[a.] Identify vulnerabilities from a terrorist’s point of view.
  \item[b.] Identify critical nodes most likely to be targets.
  \item[c.] Integrate with Operational Risk Management.
  \item[d.] All of the above.
\end{itemize}

*Answer:* They assigned oversight of each critical infrastructure to a separate governmental agency that is responsible for the development of risk assessment protocols for the protection of the assets under its purview. (p. 39)

11. Identify at least five differences in RAM/VSAT, ORM, and CARVER + Shock.

*Answer:*

- RAM/VSAT is used under the Federal Drug Administration (FDA) guidelines, ORM and CARVER + Shock are used under the Environmental Protection Agency (EPA) guidelines.
- ORM is defensive, CARVER + Shock is offensive.
- VSAT considers the probability of countermeasure failure (CARVER looks at recoverability). ORM does not.
- Each use different criteria or terminology to assign severity levels.
- ORM allows the assignment of responsibility to multiple persons or departments.
- CARVER directly considers psychological effects.
- ORM considers the time element of exposure.
- RAM/VSAT is also developed as software programs.
RAM/VSAT prioritizes countermeasures based on the anticipated risk reduction per dollar spent. (ch. 6)

12. Explain VSAT’s simple cost method.

*Answer:* The simple cost method returns the annualized costs through the sum of the annual operating costs plus the capital costs divided by the useful life of the countermeasure. (p. 41-42)

4. Contrast the Operational Risk Management principal of ‘accept no unnecessary risk’ with ‘accept risk when the benefits outweigh the costs.’

*Answer:* Some degree of risk is a fundamental reality. Unnecessary risk comes without a commensurate return in terms of real benefits or available opportunities. Risks without this benefit or without some type of controlling or mitigating circumstance, especially if controls can be cost-effectively implemented, should not be accepted.

All identified benefits should be compared to all identified costs. The goal is the best strategy at the least cost, not at any cost. For example: a lock on a door, good lighting and alarms are less expensive that around the clock guard service. We accept the risk of entry by an aggressor because we have put in redundant controls and the benefits of the security officer do not outweigh the additional
Risk acceptance is not always a black and white proposition. One key is to allocate limited resources so that your goals, to protect lives and property, are best achieved. (Section I, Risk Analysis and the Security Survey)

5. How does the Vulnerability Self Assessment Tool (VSAT) define vulnerability?

*Answer:* Vulnerability is defined as the probability of failure and the probability of occurrence after countermeasures are implemented. (p. 41)

**Case Study**

Your company is considering a move to a new city overseas that suffers from a high crime rate and a neighboring government that is not very stable. Certain threats have been identified, but management wants to get a better idea about the risk and about the financial consequences of the controls security might recommend to mitigate the risks. In the report, they want security to list the steps they used to make these determinations. Which of the risk assessment methodologies would you use and what steps would you complete to arrive at your analysis?

*Answer:* Of the three methodologies covered in the chapter, RAM/VSAT, ORM, and CARVER + Shock, VSAT is probably the best to use, as it is better designed to derive financial information about how countermeasures will reduce risk. The steps to conduct a VSAT analysis are:

- Identify assets
- Identify threats
- Determine criticality
- Identify existing countermeasures
- Determine risk level
- Determine the probability of failure
- Assign vulnerability
- Determine whether the risk is acceptable
- Develop new countermeasures
- Perform risk-cost analysis
- Develop a business continuity plan.

Author’s Notes

RAM or Risk Assessment Methodology was developed by Sandia National Laboratories to, according to their website, (http://www.sandia.gov/ram/) assess risk at various types of facilities and critical infrastructures. The methodology is based on the traditional risk equation:

$$\text{Risk} = P_A \times (1 - P_E) \times C,$$

$P_A$ is the likelihood of adversary attack,

$P_E$ is security system effectiveness,

$1 - P_E$ is adversary success, and

$C$ is consequence of loss of the asset.
The process begins with a characterization of the facility, including identification of the undesired events and the respective critical assets. Guidance for defining threats is included, as well as for using the definition of the threat to estimate the likelihood of adversary attack at a specific facility. Relative values of consequence are estimated. Methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, risk is calculated. In the event that the value of risk is deemed to be unacceptable (too high), the methodology addresses a process for identifying and evaluating security system upgrades in order to reduce risk.

RAM-W for water districts, RAM-T for transportation systems, RAM-C for communities, and RAM-D for dam owners and operators are examples of the variations of this model.

---------

Homeland Security Presidential Directives 7 and 9 were established to assign responsibility for the protection of Critical Infrastructure to various governmental agencies, with HSPD 9 specific to the protection of food and agriculture from terrorist attack and damage from disasters.

Since responsibility for Food Security was assigned to the FDA, they have used existing food safety programs to address security. These programs include Good Management or Manufacturing Practices and Hazard Analysis and Critical Control Point (HACCP). HACCP, as the name implies, is process-intensive and identifies specific hazards and measures for their
control to ensure the safety of food. HACCP is based on prevention and reduces the reliance on end-product inspection and testing. ORM works well with these programs because it is process-based.

The HACCP system consists of the following seven principles:

- Conduct a hazard analysis. Identify the potential hazard(s) associated with food production at all stages, from primary production, processing, manufacture and distribution until the point of consumption. Assess the likelihood of occurrence of the hazard(s) and identify the measures for their control.

- Establish the Critical Control Points. Identify the points, procedures or operational steps that can be controlled to eliminate the hazard(s) or minimize the likelihood of occurrence. A "step" means any stage in food production and/or manufacture, including the receipt and/or production of raw materials, harvesting, transport, formulation, processing, storage, etc.

- Determine critical limit(s). Establish critical limit(s) that must be met to ensure the Critical Control Points are under control.

- Establish a system to monitor control of the Critical Control Points by scheduled testing or observations.
- Implement corrective action taken when monitoring indicates that a particular Critical Control Point is not under control.

- Develop procedures for verification to confirm that the HACCP system is working effectively.

- Document all procedures and records appropriate to these principles and their application.

-----------------

Other common risk assessment methodologies are used in the environmental health and safety profession to assess the dangers to persons and the environment from the use of hazardous waste or hazardous substances.
Chapter 7: The Security Survey: An Overview

Learning Objectives

- Define a security survey.
- Students will justify the need for a security survey.
- Calculate the impact of loss verses net profits.
- Expectations and results of a survey.
- Convincing management of program need.

Presentation Outline

I. Introduction

H. Security surveys are used to identify risk.
I. The primary vehicle used in a security assessment is the survey (Sennewald).
J. The survey gathers data that reflects who, what, how, where, when and why of an existing operation.
II. Why Are Security Surveys Needed?

A. The cost of fraud and abuse to American business exceeds forty billion dollars per year.

B. Most general business security surveys calculate losses at 6 percent of annual revenue.

C. Crime losses far exceed losses to business caused by fire and industrial accidents:
   1. Estimates put this loss at twice as great as fire and industrial accidents.

D. 2002 Report To the Nation on Occupational Fraud and Abuse:
   1. Average organization loss equals $4,500 per employee year (based on $600 billion).
   2. Fraud and abuse cost U.S. organizations more than $600 billion annually.

E. These estimates of the cost of fraud vary widely:
   1. Distributed evenly among government, public, private, and non-profit firms.

F. Indirect costs to consider:
   1. Loss of productivity.
   2. Legal action.
   3. Increased unemployment.
   5. Other hidden costs.

G. Managers may not know or not want to know they have a problem.
III. Who Needs Security Surveys?

A. Stanford Research Institute report, *Business Property Security*: “Likely victims are growing businesses where expansion occurs faster than control systems are set up and large companies where close control over branches and divisions is not feasible.”

B. Most business security is directed toward external problems.

C. Internal theft by employees a simple process of rationalization.

D. Most predominant form of business crime is employee theft:
   1. Asset misappropriation accounts for the majority of employee theft.
   2. Bribery and corruption are second or third form of business crime.
   3. Companies with a hundred or fewer employees are the most vulnerable to fraud and abuse.

E. Amount required to offset losses in stolen merchandise, equipment, and supplies is not 1:1:
   1. At 2% net profit, a company must sell $25,000 worth of merchandise to break even for the theft of a $500 item.

IV. Business Attitude Toward Security

A. Managerial attitudes toward security can be influenced by:
   1. Cost of security regarded as reducing the profit line.
   2. Poor knowledge of the need for adequate protection.
3. Reliance on sales pitches that overemphasize manpower (guards) or hardware (alarms or electronics).

V. What Can a Security Survey Accomplish?

A. Establish whether the plan is up to date and adequate.

B. Consolidate procedures and safeguards so that the components complement one another.

C. Establish the need for a security plan.

D. Identify critical factors affecting the security of the premises or operation.

E. Analyze the vulnerabilities and recommend cost-effective protection.

F. Most frequently needed programs include:

1. Protection against:
   a. Internal and external theft.
   b. Embezzlement.
   c. Fraud.
   d. Burglary.
   e. Robbery.
   f. Industrial espionage.
   g. Theft of trade secrets and proprietary information.

2. Access-control procedures for facility perimeter, computer facilities, executive offices.

3. Establish lock and key-control procedures.
4. Design, supervise, and review installation of anti-intrusion and detection systems.

5. Workplace violence program.

6. Control over the movement and identification of employees, customers, and visitors.

7. Selection, training, and deployment of security personnel, proprietary or contract.

8. Emergency and disaster plans and guidelines.

9. Internal resources available and needed for an effective security program.

10. Seminars for management and operations personnel in all the above areas.

VI. Why the Need for a Security Professional?

A. Improve net profits, reduce frequency of disruptive acts.

B. Eliminating, preventing, or controlling a company’s losses.

VII. How Do You Sell Security?

A. Management’s attention is obtained after a serious problem.

B. Bring a situation into prospective.

C. Establish a meaningful dialogue with the decision makers.

D. Deal in principles, not personalities.

E. Be professional about security.

F. Keep proposals to management as brief as possible.

G. Know where to go to get the help.
H. Suggest that management hire an outside consultant.

I. Present your position at the right time.

J. Sell it to everyone in the organization.
Sample Test Questions

True or False

56. Security surveys are used to identify risk. Answer: T (p. 45)

57. The survey gathers data that reflects the who, what, how, where, when and why of an existing operation. Answer: T (p. 45)

58. Most general business security surveys calculate losses at 18 percent of annual revenue. Answer: F (p. 46)

59. The theft of one small item, multiplied ten thousand times each year in many large companies, adds up to an annual loss that can far exceed the total loss to external theft over the entire period of a firm’s corporate existence. Answer: T (p. 47)

60. Business managers often do not know they have a security problem. Answer: T (p. 45)

61. Likely victims of theft and internal crime are growing businesses where expansion occurs faster than control systems are set up. Answer: T (p. 46)
62. Businesses often focus their attention on internal theft when most of their losses are caused by external theft and other crimes.  
   Answer:  F  (p. 46)

63. Security vendors can adversely influence managers’ decisions to implement an effective security program.  
   Answer:  T  (p. 48)

64. A security survey can help to consolidate procedures and safeguards.  
   Answer:  T  (p. 49)

65. When selling your security programs to managers, it is more important to take their personalities into consideration than it is to stick to the principals of the plan.  
   Answer:  F  (p. 51)

**Multiple Choice**

21. Examples of indirect losses due to theft include:  
   Answer:  d.  (p. 46)

   i. Loss of productivity.
   j. Legal action.
   k. Government intervention.
   l. All of the above.
22. A security survey can:  \textit{Answer: d. (p. 49)}

a. Identify critical factors affecting the security of the premises or operation.

b. Analyze vulnerabilities.

c. Identify risk.

d. All of the above.

23. Why are security professionals needed to put programs together?  \textit{Answer: a (p. 50)}

s. To help ensure the proper application of protection techniques.

t. They best understand the cost/benefit of security hardware.

u. They will not over- or underinflate loss figures. All of the above.

24. The theft of one five hundred dollar fax machine means the company must sell how much more merchandise if it is to break even for the theft, if it is in the 6 percent net-profit category?  \textit{Answer: d (p. 48)}

m. $500.

n. $530.

o. $3,000.

p. $8,333.

25. The security survey:  \textit{Answer: c (p. 45)}
a. Examines physical security risks.
b. Is the primary vehicle to establish cost/benefit.
c. Gathers data that reflects the who, what, how, where, when and why of an existing operation.
d. Is not effective in evaluating existing security operations.

Short Answer

13. Discuss ways an employee might rationalize internal theft from their employer.

*Answer:* Crimes against the ‘Establishment’ are perceived by many to be permissible, in fact, not crimes at all. The lack of personal identification with a company by its employees and the dramatic dilution of ethical and moral standards among the general public combine to make internal theft by employees a simple process of rationalization. “They won’t miss one small wrench or screwdriver that I need for my workshop at home.” (p. 47)

14. Why would a business manager adjust his or her loss figures to reflect a lower amount?

*Answer:* Some managers seem to prefer to keep things as they are and to regard any suggestion of a need for increased security as direct or indirect criticism of their abilities to manage their operations. (p. 45)
15. Discuss ways to sell your security program.

*Answer:* Establish a meaningful dialogue with the decision makers in the management hierarchy. Find out what they really want a security program to accomplish for them, if, in fact, they want anything. Marshal the facts. Research the history of security losses experienced by the company and use this information to develop trend projections. Deal in principles, not personalities. Avoid internecine power struggles at all costs. Maintain a position of objective neutrality. Be as professional about security as you can. In making a proposal to management, hit the highlights and make your proposal as brief as possible. In any proposal that will cost money, make certain you have developed the cost figures as accurately as possible. If you need outside help, do not be reluctant to admit it. Suggest that management hire an outside consultant. Present your position at the right time. Recognize that management’s priority is first and foremost the generation of profit. Develop a program of public relations. Once you have management thinking favorably about your proposal, you will need to sell it to everyone in the organization in order for it to be successfully implemented. (p. 50-52)

4. Produce a brief (one- to two-page) justification to management for the implementation or increase of the budget of a security program or security survey in a company with revenues of $10,000,000 that operates on a 6% profit margin.
Answer: XYZ Corporation operates in a highly competitive environment, subject to numerous and intense market pressures. In our conversations with senior management [establish a dialog with decision makers] over the last six months, they have expressed the need to control costs and to increase profits. This [need] has translated into a reluctance to increase funding for current and future programs, including expenditures for additional security programs [ascertain their feelings about security].

During the preceding six-month period, our company has implemented a number of initiatives designed to control costs. These initiatives, applied across all sectors of the business, have only resulted in a two-percent decrease in costs and projections indicate that this figure will remain constant. [Use the technique of non-attribution for all unpublished sources of information. With published sources, such as interoffice memos, excerpt the pertinent data if possible.] The average organization loses about 6 percent of its total annual revenue to fraud and abuse committed by its own employees (source: Risk Analysis and the Security Survey, et. al.). [Research the history of security losses experienced by the company and use this information to develop trend projections.] In our company, this translates into a loss of $600,000 annually; however, because we operate on a six-percent margin, we are required to increase our sales by $9,999,600 just to break even for this loss.
Security best practices and security departments in competitive organizations that have experienced similar problems have found that the implementation of the programs we will propose have resulted in significant decreases in losses.

[Develop contacts with other security professionals who share similar problems.  
Don’t reinvent the wheel: attend security seminars, purchase relevant books, study, and do research, be professional] We intend to increase the number of video cameras and to upgrade our alarm and access control system at a cost of approximately $250,000. [In making a proposal to management, hit the highlights and make your proposal as brief as possible. Save the details for later. In any proposal that will cost money, make certain you have developed the cost figures as accurately as possible. If the figures are estimated, label them as such and err on the high side.] These programs are in part based on the recommendations of our outside consultant who has verified the need and costs for the program and who will continue to provide guidance in the implementation of the program.

[Suggest that management hire an outside consultant.]

Our consultant will also assist in developing a program to make all employees aware of the problems we face and how our strategies will prevent their occurrence, help increase their safety and security, and to maintain the financial health of the company. [Once you have management thinking favorably about your proposal, you will need to sell it to everyone in the organization in order for it to be successfully implemented.]
As you know, we recently suffered a significant loss due to what we believe was internal theft. We cannot continue to repeat these incidents without a major impact to our operating costs and continued profitability. The increase in our budget to implement the above measures will help ensure the vision and goals of the company are maintained. [Recognize that management’s priority is first and foremost the generation of profit. In order to capture management’s attention, wait for the right circumstances.] (ch. 7)

Case Study

You have just been hired as the corporate security manager for a major corporation. Your boss told you that your primary responsibility is to establish and manage a corporate assets protection program. You are told that no program currently exists and only recently has executive management grudgingly agreed that a formal assets protection program is needed.

Based on your previous experience, you know that, to establish a successful corporate assets protection program, you must ‘sell’ security to executive management – convince them that the assets protection program is worth the costs.

Answer: See pages 50-52 of the text.
Risk Analysis and the Security Survey 3rd edition

Chapter 8: Management Audit Techniques and the Preliminary Survey

Learning Objectives

- Differences and similarities between audits and investigations and how they relate to the preliminary survey;
- Understand the purpose of a preliminary survey;
- What and how to measure in the field;
- How to prepare for the initial interview and meeting;
- How to gather information for the preliminary survey.

Presentation Outline

I. Audit Guides and Procedures

K. Audits: Aids to Surveys

1. Many similarities between auditing and investigating.
2. Audit technique is counter to investigative training.

3. Auditor appraises the truth or falsity of a proposition.

4. Borrow techniques used by internal auditors.

5. Security surveys are specialized internal audits.

6. Auditing and investigating presuppose cooperation and fear.
   a. The first task is to allay fear.
   b. Fear is an impediment to communication.
   c. Open communication leads to successful investigation and audit.
   d. Use candor.
   e. Explain expectations.

7. Internal (management) auditing is “a comprehensive review, verification, analysis, and appraisal of the various functions (operations) of an organization, as a service to management.”

L. Successful methods used by auditors include:

1. Fieldwork
   a. 50 percent of survey work is done in the field.
   b. 50 percent is divided between planning and the final report.
   c. Fieldwork consists of collecting and analyzing data, records, and procedures.
   d. It is measurement and evaluation of the effectiveness of the program under review.
   e. Measurement must have as its basis an objective standard.
   f. Construct standards or acceptable practices when none exist.
g. Only the technically qualified should render a judgment or validate measurements of technical standards.

h. Evaluate obsolesce of recognized standards or acceptable practices.

i. Measurement concerns three aspects of the security operation:
   i. Quality.
   ii. Reliability.
   iii. Cost.

j. Other considerations include:
   i. Effectiveness of the procedure, technique, hardware, or electronic device.
   ii. Reliably and properly addresses or solves a problem.
   iii. Perform at less cost.

k. The objective of measurement is to assess the adequacy, effectiveness, and efficiency of an existing or proposed system.

l. The objective is accomplished by applying six basic forms or methods of field work:
   i. Observing.
   ii. Questioning (oral and written).
   iii. Analyzing.
   iv. Verifying.
   v. Investigating
   vi. Evaluating

m. Evaluating.
   i. Evaluation in a survey occurs constantly.
ii. Evaluate what the results imply.

iii. Evaluation calls for judgment.

iv. Query with who, what, when, where, why and how questions.

II. The Preliminary Survey

A. Definition and Purpose

1. The basic purpose of the preliminary survey is familiarization.

2. Understand the management concepts used, along with the qualifications and abilities of the employees.

3. The preliminary survey will:

   a. Allow a well-thought-out program.
   
   b. Deploy efforts efficiently and economically.
   
   c. Form a foundation for the detailed examination that follows.
   
   d. Test the client’s sincerity.
   
   e. Avoid misunderstandings.

4. Cuts through the mass of detail that obscures the objective.

5. A preliminary survey answers the following questions:

   a. What is the operation?
   
   b. Who or what does the operation?
   
   c. Why is it done (where and when)?
   
   d. How is the operation accomplished?

6. Focus on the highlights, order, and methodology.
B. The Initial Interview

1. The nature of the questions asked will vary:
   a. Organizational survey (people-oriented questions are the general rule).
   b. Functional survey (concerned with the actual workflow).
   c. Operational survey (primarily interested in hardware, software or related procedures).

2. The initial interview should elicit the following:
   a. Management’s perception of the major problem areas.
   b. Management’s expectations.

3. Schedule the initial meeting.
   a. Prepare management memorandum.
      i. Signed by the highest authority possible.
      ii. Introduces the survey team.
      iii. Describes the objective of the survey.
      iv. Solicits the assistance and cooperation of all company employees.
      v. Authorizes access to all documents and information.
      vi. Sent to affected department heads in advance of the arrival of the survey team.
   b. Introduce survey team at meeting with all department heads present.

4. Schedule a second meeting.
   a. Give the client a brief report of initial impressions obtained.
   b. Explain how the surveyor perceives the objectives, activities, or functions under review.
c. Establish agreement as to what will be accomplished.

d. Briefly outline the general plan of attack.

5. Ensure that both parties are in total agreement with the objective of the project.

C. Obtaining Information

1. What information to obtain:

   a. The Charter for the operation.
      i. Copies of policy statements.
      ii. Directives.
      iii. Statements of functions.
      iv. Responsibilities.
      v. Goals.
      vi. Delegations of authority.
      vii. Job descriptions of the people directly involved in the activity.
      viii. Position descriptions.
      ix. Nature, size, and location of ancillary or satellite activities.
      x. Interfacing operations and their relationship to the activity under review.

   b. Financial information.
   c. Operating instructions.
   d. Problem areas and deficiencies.
   e. Matters of special concern.

2. Sources of information:

   a. Discussions with supervisors and employees directly engaged in the activity under review. This is important because:
i. Are usually aware of the problems and have worked out the solutions.

ii. Need to obtain their cooperation for implementation.

iii. More inclined to work for the success of the recommendations.

b. Discussions with supervisors downstream and upstream of the operations under review.

c. Correspondence files.

d. Prior survey, audit, or inspection reports.

e. Incident/crime reports.

f. Budget data.

g. Mission or objective statements or reports.

h. Procedural (operational) manuals.

i. Reports by or to government agencies.

3. Physical Observation.

a. Two phases:

   i. Familiarization tour of the entire facility.

   ii. Subsequent tours.

4. Flow Charting

   a. Easiest way to obtain a visual grasp of a system or procedure.

   b. Ready means of analyzing complex operations.

III. Summary

A. Fieldwork measures what *is* against what *should be.*
B. Requires both methods of measurement and the existence of acceptable practices and standards.

C. Security surveys measure three basic factors: quality, reliability, and cost.

D. To measure, perform surveys, review and test.

E. Fieldwork is observing, questioning, analyzing, verifying, investigating, and evaluating.

F. Fieldwork gathers data and accumulates, analyses, and evaluates evidence before recommendations are developed.

G. The preliminary survey charts the course for the main voyage and provides a clear view of activities to eliminate the need for further review.

H. The preliminary survey allows the investigator to meet people, understand operations, and focus on objectives, controls, and risks.
Sample Test Questions

True or False

66. Borrowing techniques used by auditors is not recommended because auditors deal with procedures already in place.  
   \textit{Answer: F} (p. 54)

67. As much as 50\% of survey work is done in the field.  
   \textit{Answer: T} (p. 54)

68. If, during the course of a survey, you uncover impropriety, it is not your duty to refer it to the proper authorities within the entity being surveyed.  
   \textit{Answer: F} (p. 56)

69. Internal auditing is “a comprehensive review, verification, analysis, and appraisal of the various functions (operations) of an organization, as a service to management.”  
   \textit{Answer: T} (p. 54)

70. Where no standards or acceptable practice exists, the surveyor should never create one.  
   \textit{Answer: F} (p. 55)

71. Fieldwork consists of collecting and analyzing data, records, and procedures.  
   \textit{Answer: T} (p. 54)

72. The basic purpose of the preliminary survey is familiarization.  
   \textit{Answer: T} (p. 58)
73. Testing the client’s sincerity is not a goal of the preliminary survey.  
*Answer: F* (p. 58)

74. The preliminary survey should not ask why something is done.  
*Answer: F* (p. 59)

75. Meeting with the client or participants both before and after the survey is excessive.  
*Answer: F* (p. 60)

**Multiple Choice**

1. Which audit technique differs from investigative training?  
*Answer: d.* (p. 53)

   m. Analyzing facts.

   n. Drawing conclusions.

   o. Making recommendations.

   p. All of the above.

2. Measurement normally concerns at least these aspects of the security operation:  
*Answer: c.* (p. 55)

   a. Standards, procedures, and conditions.
b. Verifying, analyzing, and reporting.

c. Quality, reliability, and cost.

d. None of the above.

3. The objective of measurement is to assess:  \textit{Answer: a} \ (p. 55)

\textitem{v.} Adequacy, effectiveness, efficiency.

\textitem{w.} Standards, procedures, conditions.

\textitem{x.} Criticality, cost, recommendations. None of the above.

26. A preliminary survey will:  \textit{Answer: d} \ (p. 58)

\textitem{q.} Allow one to develop a well thought-out program.

\textitem{r.} Manage the main survey efficiently and economically.

\textitem{s.} Avoid misunderstandings about the details of the project.

\textitem{t.} All of the above.

27. The nature of the questions asked in an initial meeting may include:  \textit{Answer: c} \ (p. 60)

\textitem{a.} Probing, never open-ended.

\textitem{b.} Questions that will not overlap with those asked in the main survey.

\textitem{c.} Organizational, functional, and operational.

\textitem{d.} All of the above.
28. Questions asked during the initial interviews should elicit answers to:  \textit{Answer: b.} (p. 60)

a. Probability/criticality.

b. What does management perceive to be the major problem areas?

c. Standards in use.

d. None of the above.

29. At the initial meeting, the surveyor should:  \textit{Answer: d.} (p. 60)

a. Describe the objectives of the survey.

b. Solicit assistance and cooperation.

c. Introduce the survey team.

d. All of the above.

30. Financial information:  \textit{Answer: b} (p. 61)

a. Is of no use during the preliminary survey.

b. Is obtained for review if it has a bearing on the subject at hand.

c. Does not consider indirect costs in this phase of the survey.

d. None of the above.
31. Evaluate recognized standards to determine if they are:  \textit{Answer: d (p. 55)}

\begin{itemize}
  \item [a.] Obsolete.
  \item [b.] Reliable.
  \item [c.] Effective.
  \item [d.] All of the above.
\end{itemize}

32. Another name for the initial interview is:  \textit{Answer: a (p. 60)}

\begin{itemize}
  \item [a.] Opening conference.
  \item [b.] Pre-survey orientation.
  \item [c.] Operational introduction.
  \item [d.] Phase 1 meeting.
\end{itemize}

\textbf{Short Answer}

16. List three of the six basic forms or methods of fieldwork.

\textit{Answer: Observing, questioning, analyzing, verifying, investigating, evaluating. (p. 55-56)}

17. Contrast differences and similarities between criminal investigators and internal auditors.
**Answer:** There are many similarities between auditing and investigating, but there is one important difference: the audit technique of analyzing facts, drawing conclusions, and making recommendations is absent from the investigator’s background and training. Investigators are trained to obtain evidence, report objectively, and scrupulously avoid drawing conclusions or making recommendations. These processes they leave for their clients.

The auditor is trained to appraise the truth or falsity of a proposition — not to take things for granted, jump to conclusions, or accept plausible appearance for hard fact. Audit training postulates that accepting appearance for substance is the surest way to arrive at improper conclusions. To be able to differentiate between appearance and substance and draw the proper conclusions is the heart and marrow of the auditor’s task. Both disciplines pursue fact — a *fact* being something that has actual existence, something that can be inferred with certainty, a proposition that is verifiable. The auditor is trained not only to adduce facts but to appraise, draw conclusions, and make recommendations from them — the very techniques the investigator is trained to avoid. (p. 53-55)

18. What information should be obtained for the preliminary survey, and what are some sources of this information?

**Answer:** The Charter for the operation, policy statements, directives, statements of functions, responsibilities, goals, and delegations of authority, job descriptions,
objectives of the operation, the nature, size, and location of ancillary or satellite activities, interfacing operations and their relationship to the activity under review, financial information, operating instructions, problem areas, procedures or controls that have supposedly been designed to alleviate difficulties, matters of special interest.

Discussions with supervisors and employees directly engaged in the activity under review, correspondence files, prior survey, audit, or inspection reports, incident/crime reports, budget data, mission or objective statements or reports, procedural (operational) manuals, reports by or to government, state and federal organizations (OSHA, for example), physical observation, and flow-charting are the sources for the above. (p. 61-63)

19. Sketch a simple flow chart of the following process: Instructor hands out examination, students take test, instructor walks through class, students hand in examination, instructor grades examination, records grade and sends to administration, hands back examination.

```
Instructor            |              Student              |           Administration
                    |    |                             |    |
                    |     |                             |    |
                    |     |                             |    |
                    |     |                             |    |
                    ⊙    |                             |    |
                    |     |                             |    |
                    |     |                             |    |
                    |     |                             |    |
                    |     | Examination                |
```
Chapter 8: Management Audit Techniques and the Preliminary Survey

Rec

Forward Grade

E

Hands Back

Research

Copyright 2006 © Elsevier, Inc. All rights reserved.
1. What other types of flowcharting are used in business today?

Answer: Answer should include at least the following: Computer or network flowchart, Cause and Effect (fishbone), PERT chart, Gantt chart, swim lanes, timeline.

Case Study

You are the security manager of a company with multiple domestic locations. Your department is tasked with completing 12 surveys per year, 6 of which are complete. The person who is trained to conduct these surveys quit suddenly and you have only a short time to complete the remainder. You have no money left in your budget for outside consulting services. A member of your supervisory staff, who has had a number of years experience in security and security systems design, has offered to complete the surveys, but has never done one in the past.

What do you need to tell this person to do so they can accomplish a preliminary security survey?

Answer: See Chapter 8
Chapter 9: The Survey Report

Learning Objectives

- Importance of good writing skills.
- Describe some of the time-tested methods for writing better reports.
- Elements to include in survey reports.
- Use of flow charts for clarity.

Presentation Outline

I. Introduction

M. Good writing requires good thinking.

N. More likely to be judged by ability to write a good report than ability to do good fieldwork.

II. “I Must Write, Therefore, I Shall”
A. Key to good writing lies in:
   1. Good fieldwork.
   2. A well-structured outline.
   3. Copious notes or working papers.
   4. Persistence.

B. Report outline contains the following sections:
   1. Purpose.
   2. Scope:
      a. Persons interviewed.
      b. Premises visited, times, and so forth.
      c. Categories of documents reviewed.
   3. Findings:
      a. Description of facilities, environment, operations, products or services.
      b. Description of the organizational structure and number of employees.
      c. Physical security features.
      d. Internal controls.
      e. Data systems and records.
      f. Status and extent of planning, organization, and training.
      g. Proprietary information and trade secrets.
   4. Conclusions and evaluation of protective measures discussed in findings.
   5. Recommendations.

C. Immediately take pen to paper.
D. Two functions of survey reports:
   1. Communicate.
   2. Persuade.

III. Five Criteria of Good Writing

A. Fieldwork is largely measurement.
   a. Implies the existence of acceptable practices and standards.

B. Reports are measured against standards.

C. Report must meet the following criteria:
   1. Accuracy.
      a. Report must be factual, based on evidence.
      b. Speaks with authority.
      c. Clearly identify the source when not personally observed.
      d. Avoid personal attribution.
      e. Balance and perspective.
   2. Clarity.
      a. Cannot write clearly about what one does not understand.
      b. Poor structure is an impediment to clarity.
      c. Avoid acronyms and technical jargon.
      d. Reporting a finding without setting the stage leads to misunderstanding.
      e. Flow charts, schedules, and graphs aid clarity and understanding.
   3. Conciseness.
a. Eliminate that which is unessential.

b. Conciseness does not mean brevity.

c. Short, simple, easy-to-understand sentences.

4. Timeliness.

a. Submitted in a timely fashion.

b. Interim report used for details that must be disclosed without delay.

c. Designed to be short and to the point.

i. Address one to two subjects.

d. Clearly identified as “interim.”

e. Establish goals and time frames.

5. Slant or Pitch.

a. The tone of the report is courteous.

b. Strive for impersonality.

c. Minimize minor details or trivialities.

6. Format.

a. Form dictated by the type of report.

b. Formal or informal, final or interim, written or oral.

c. Form depends upon report recipient.

d. No universal style or format.

e. Elements in survey reports:

i. Cover letter.

   1. Brief synopsis.

   2. Limited to one page.

1. Title.

2. Brief introduction or forward.

3. Purpose.

4. Scope.

5. Findings.

   a. Report both positive and negative findings.

   b. Include a summary of the findings.

      i. Criteria or standards of measurement used.

      ii. Conditions found.

      iii. Significance of deficiencies.

      iv. Cause and effect

      v. Recommendations for corrective action.

   c. When presenting a negative finding:

      i. Describe nature of the problem.

      ii. Identify who or what procedures are tasked with its solution.

      iii. Disclose what is actually being done, if anything.

      iv. Detail how the situation is allowed to happen.

      v. Identify who is responsible to take corrective action.

      vi. Describe what corrective action is necessary.


   a. Not all reports contain opinions or conclusions.
b. Comments should be both positive and negative.

c. Some believe conclusions should be eliminated entirely.

d. Conclusions or opinions must be justified and supported by fact.

IV. Summary.

A. Reports are evaluated according to their accuracy, clarity, conciseness, timeliness, and slant (or pitch).

B. Whatever format is used, they include one or more elements:

   a. Cover letter.

   b. Body of the report.

      i. Title.

      ii. Forward or introduction.

      iii. Purpose.

      iv. Scope.

      v. Findings.

      vi. Opinions and conclusions.

      vii. Recommendations.

C. Good writing takes constant practice and effort.

D. Begin by preparing a logical outline.

E. Flow charts, schedules, and graphs aid clarity and understanding.

F. There is no such thing as good writing; there is only good rewriting.
Sample Test Questions

True or False

76. A poorly written report can negate the positive effects of exceptionally good fieldwork.

   Answer: T  (p. 67)

77. For a report to be accurate, it must encompass truth, relevancy, and perspective. It must also have balance.

   Answer: T  (p. 71)

78. An interim report wastes valuable time and will delay completion of the final survey report.

   Answer: F  (p. 72)

79. The scope of the project should not be stated in the final report.

   Answer: F  (p. 74)

80. It is most often best to delay the start of your report so that you can better think about how to organize your thoughts.

   Answer: F  (p. 72)

81. Reports can be measured against standards.

   Answer: T  (p. 70)

82. Conciseness does not necessarily mean brevity.

   Answer: T  (p. 72)
83. Good fieldwork is important because it is difficult to write about something you don’t understand.  
   Answer: T (p. 71)

84. The liberal use of flowcharts, schedules, and graphics in your final report should be minimized.  
   Answer: F (p. 71)

85. A function of the survey report is to communicate; it should never be used to persuade.  
   Answer: F (p. 70)

**Multiple Choice**

33. The key to good writing is found in:  
   Answer: d. (p. 68)

   q. Good fieldwork.
   r. A well-structured outline.
   s. Persistence.
   t. All of the above.

34. Criteria of a good report include:  
   Answer: a. (p. 70-73)

   a. Accuracy, clarity, conciseness, timeliness.
   b. Fieldwork notes, data, observations.
   c. Facts, data, findings and recommendations.
d. Completeness, volume, comprehensiveness.

35. Acronyms: Answer: d (p. 71)

y. Keep your report brief and should be easily understood by your target audience.
z. Demonstrate to management your understanding of the profession.

aa. Add clarity to the report. Should be avoided and never used without explanation.

36. Interim reports: Answer: b (p. 72)

u. Should not be used.
v. Address only one or two subjects.
w. Are intended to be a progress report.
x. Are intended to briefly synopsize all elements contained in the final report.

37. The final report should: Answer: c (p. 73)

a. Clearly identify those persons directly responsible for inadequacies found in the survey.
b. Include all minor details found in the survey.
c. Strive for impersonality.
d. All of the above.
38. The body of the report should:  Answer: c.  (p. 75)

   a. Report positive findings.
   
   b. Report only negative findings.
   
   c. Report both positive and negative findings.
   
   d. All findings should be positive.

39. In preparing to present a negative finding, you should be able to answer:  Answer: d.  (p. 75)

   a. What are people or procedures suppose to be doing about the problem?
   
   b. How was this situation allowed to happen?
   
   c. What should be done about it?
   
   d. All of the above.

40. The format of the report:  Answer: b  (p. 73)

   a. Should be exactly the same for each and every project.
   
   b. Is dictated by the type of the report.
   
   c. Should never be informal. Is universal.

41. Opinions and conclusions in the survey report:  Answer: b  (p. 76)
a. Are always included.
b. Must be fully supported by fact and fully justified.
c. Must be specifically identified as an opinion or conclusion.
d. All of the above.

42. A cover letter to the survey report:  
   \textit{Answer: b (p. 73)}

a. Is redundant.
b. Can include a brief synopsis of the report findings.
c. Should be several pages in length.
d. Both b and c.

\textbf{Short Answer}

20. Discuss how reports can be measured against standards.

\textit{Answer: A good report must meet the following criteria: accuracy, clarity, conciseness, timeliness, and slant (or pitch). The report must be factual, based entirely on hard evidence. Likewise, the report should speak with authority. When it is necessary to report matters not personally observed, the report should clearly identify the source. One must be careful to avoid personal attribution unless one can personally certify the existence or extent of the condition reported. Facts must be reported in the proper perspective. An}
orderly progression of ideas lends to clarity and thus understanding. This is accomplished by starting with an outline. Acronyms and technical jargon should be avoided where possible. Avoid misunderstanding by setting the stage for recommendations and include a discussion of what now exists and why it isn’t working. Charts and pictures will add to clarity. There must be sufficient detail in the report to make it meaningful to all levels of the audience, but it must be short and concise. The report must be submitted in a timely fashion, with the use of an interim report when appropriate. The tone of the report should be courteous and not identify or highlight the mistakes of easily identified individuals, small units, or departments. The report must not be overly concerned with minor details or trivialities. It must avoid sounding narrow-minded, concentrating instead on that which has real meaning and substance. The report should clearly be identified with the needs, desires, and goals of sound management. (p. 70-73)

21. Write an interim report about a theoretical project.

*Answer:* The report should contain the following elements:

- The subject of the report must be of such importance or magnitude that the details must be reported to management without delay;
- Should communicate the need for immediate attention and immediate corrective action;
Chapter 9: The Survey Report

- Should document that the deficiency was orally communicated prior to the report, although this documentation was not mentioned in the text;
- Short and to the point, should address one or two subjects;
- Should be identified as “interim,” and contain a written disclaimer against accepting it as the final word on the subject being reported;
- Should show attention to accuracy, clarity, conciseness, timeliness, and slant (or pitch).

(p. 72-73)

22. How can reporting a finding without properly setting the stage lead to misunderstanding?

Answer: Only by reporting relevant information and background can the author expect the reader to understand the process or condition and thus appreciate the significance of the finding. If one is recommending a new procedure, one should first tell what procedure, if any, now exists and why it isn’t working. This makes the client fully cognizant of the procedures in question and much better positioned to consider the proposed change favorably. (p. 71)

4. The Director of Security for XYZ Company, Erik Bailey, asked you to complete a security survey of Building B at his 12-building complex. This building represents the source of his largest number of thefts of high-energy trinkets at the entire site. He believes the building manager, Ben Davis, does not enforce access and property
control procedures sufficiently. Employees are to use only one door for entry and exit, but often use other doors located on the ground floor without consequence. A security officer who monitors a building alarm system sits at the entry door.

Create a short Survey Report. Include assumed items.

**Answer:** The following elements should be present:

**Cover Letter:**

- Properly titled
- May include a brief synopsis of the findings
- Limited to one page
- Proper letter format

Title that fully identifies the name and address, with zip code, of the entity being surveyed. It should also include the dates between which the survey was conducted.

Introduction or Forward that contains information to acquaint the reader with the subject under review, identifies the sites or departments toured, the persons interviewed, the documents examined and the authority for the survey.

Purpose. Include a brief description of the objectives of the survey.
Scope. The statement of scope should be a clear delineation of exactly what areas are being reviewed and to what extent they are being examined.

Findings. The statement of reported findings may include a summary of the findings (due to the limited information, this may not be possible unless the student embellishes the findings), the criteria or standards of measurement used, the conditions found, and, for deficiencies, their significance, causes and effects, and recommendations for corrective action. The fact that access and property control procedures are in place and are found not to be followed by observation and possibly interviews with the guard and other employees should be noted without blame. Since this is a single guard, it may be assumed that while the guard is on rounds, he or she is not able to enforce the procedures. The student may recommend additional personnel, employee training, local audible on alarms on unauthorized doors, etc. The findings and recommendations should answer the following:

- What is the problem?
- What are people (procedures) supposed to be doing about this problem?
- What are they actually doing, if anything?
- How was this situation allowed to happen?
- What should be done about it?
- Who is responsible to ensure that corrective action will be taken (if appropriate, i.e., is this an internal or external report)?
What corrective action is necessary to remove the deficiency?

Conclusion. May include a conclusion, summary, closing statement, or conclusion identified as such in some way and supported by the facts.

The report must meet the criteria for a good report: accuracy, clarity, conciseness, timeliness, and slant (or pitch).

Brief example:

------------------

November 18, 2005

Erik Bailey
Director of Security
XYZ Corporation
22 Twain Road
Anytown, CA 94063

Dear Mr. Bailey:

Attached is a copy of our Security Survey report of your Building 12 facility located at your main campus. Overall, we believe that you have implemented a good security program. In our report, we have identified several areas that we believe
can be improved with the addition of electronic equipment and by an increase in staffing.

We appreciate the opportunity to work with XYZ.

Sincerely,

Ima Student
Security Consultant

SECURITY SURVEY REPORT

XYZ CORPORATION
BUILDING 12
22 Twain Road
Anytown, CA 94063

CONDUCTED BY:
Ima Student
INTRODUCTION

We were asked by XYZ’s Director of Security to complete a security survey of Building B in an effort to reduce the theft rate. This building represents the source of his largest number of thefts of high-energy trinkets at the entire site. During this survey we interviewed the following persons:

Erik Bailey, Director of Security
Ben Davis, Building Manager
Florence Nightinjail, XYZ employee
Dan Smith, XYZ security officer.

We also completed an inspection of the entire facility and observed employee activity on November 17, 2004. Security policy and procedure documents, along with alarm and access control records were examined. Our findings and recommendations are summarized in this report.
The purpose of this survey is to identify areas of deficiency in the security policy and procedure and to offer recommendations to reduce theft.

SCOPE

This survey pertains to the operations of XYZ’s departments located in Building 12 of their main campus located at 22 Twain Road. We did not survey the remaining facilities at this campus. We examined only those policies and procedures related to the theft of high-energy trinkets.

FINDINGS

In our interviews and observations of employees in Building 12 we found that employees use all of the exit doors in the building. Written security policy directs employees to only use the lobby entrance. These doors are monitored only by an alarm that annunciates at the guard station and by the time the guard arrives at the door to investigate the alarm, employees are no longer in the area. When the security officer is on rounds, he or she is not able to detect alarms until they return to the guard station. There are no local audible alarms or camera systems installed in the vicinity of the doors.

Security has informed the building manager of the problem, but building management does not believe a lax enforcement contributes to a security problem.
These conditions contribute the opportunity for employees to remove high-energy trinkets without delay or fear of detection.

The Director of Security in conjunction with building management should implement the following:

- Install local audible alarms on all unauthorized exit doors. The alarm will alert other employees in the area that the door has been opened and they may be able to identify employees who use these doors.
- Install CCTV cameras to view these doors to act as an additional deterrent and to identify those who use the doors.
- Increase security staffing or provide alarm monitoring coverage while the guard is on his or her rounds so there is no delay in the response to opened doors.
- Educate building management on the scope of the problem and suggested corrective measures.

CONCLUSION

We believe the above recommendations will help to improve the security of Building 12 and to reduce the theft of high-energy trinkets from this facility.
Case Study

As an experienced corporate security manager, you know that ‘unless it is in writing, it doesn’t exist.’ Your staff is about to conduct security surveys. However, they must have a format approved by you for reporting their findings. You decided to develop one for their use. Develop a security survey report format and explain the purpose of each element or section.

Answer: See Chapter 9. Example:

- Purpose
- Scope
- Findings
- Conclusions
- Recommendations
Chapter 10: Crime Prediction

Learning Objectives

- Identify and estimate crime hazards.
- Apply systematic indication of future crime risk to better justify the allocation of resources.
- Understand duty of care and third party liability.
- Establish foreseeability and notice.

Presentation Outline

I. Introduction

A. Why crime prediction?
   4. Identify and estimate crime hazards.
   5. Justify the allocation of resources.
   6. Protect against inadequate security claims.
B. Difficult to establish or defend claims:
   1. Laws differ between jurisdictions.
   2. Duty owed differs for various properties.
   3. Case law and decisions change.
   4. Assignment of responsibility differs.

C. Crime prediction is an inexact science.

D. Based on recidivism rates.

E. Other theories based on:
   1. Age.
   2. Demographics.
   3. Causation.

II. Analysis of Internal Crime

A. Relies on historical data.
   1. Use statistically significant data if possible.

B. Crime analysis vs. crime prediction:
   1. Crime analysis uses old data.
   2. Projection provides better understanding.

C. Internal Data Sources.
   1. Use caution with anecdotal data.
   2. Incident reports.
   3. Other departments.

D. Adjust figures for future influences.
1. Changes in staffing.
2. Changes in demographics.
3. Union contract renewals.

E. Projections represented as a rate.
   1. Helps maintain consistency.
   2. Look for cyclical trends.

F. Data used to best allocate resources:
   1. Manpower.
   3. Physical security.

III. Analysis of External Crime

A. Risk associated with criminal behavior from the community.

B. Three reasons to analyze:
   1. Crime potential to ‘spill over.’
   2. Third party liability.
   3. Defend against claims.

C. Often simply benchmark with others.
   1. Ensure valid comparisons.

D. Methodology to predict external crime:
   1. Method not tested or validated.
   2. Best used to justify budget and manpower.

E. Select the crimes to measure or predict:
1. Murder.
2. Non-negligent manslaughter.
3. Forcible rape.
4. Robbery.
5. Aggravated assault.
7. Grand theft.
8. Motor vehicle theft.
9. Arson.
10. Other pertinent crimes or special risks.

F. Research crime rates:

   a. Underreporting.
   b. Differing interpretations in definition of crimes.
   c. Targeted enforcement.
   d. Efficiency.
3. National Incident-Based Reporting System Program.
4. Count crimes for appropriate distance.
5. Count crimes by appropriate time.
6. Calculate increase / decrease each time period.

G. Adjust data unreported crime.

1. Each category.
2. True rate of crime.

H. Reduce by recidivism rate.
   1. Debatable step.
   2. Can use demographics.

I. Calculate expected recurrence of crime.
   1. Use number per time period.

J. Assign probable loss figures.
   1. Direct and indirect losses.
   2. Subtract insurance reimbursement.
   3. Add penalties and other costs.

IV. Inadequate Security

A. Notice and foreseeability.

B. Forseeability study.
   1. May lead to a summary judgment.
   2. Concentrate guard staff and patrols.
   3. Improve security planning.
   4. Justify budgets and programs.
   5. Site selection.

C. Must satisfy three conditions:
   1. Owner had a duty to protect.
   2. Owner breached the duty.
3. Breach was proximate cause of injury.

D. Analysis more stringent.

E. Duty to Protect:
   1. Actual vs. ‘apparent’ control.
   2. Varies with jurisdiction.
   3. Poor design.
   4. Distance.
   5. Adjacent properties.
   6. Determined at trial.

F. Breach of Duty.
   1. What level of security is reasonable?
   2. Proximate cause often difficult to prove.
   3. Standards.

G. Establishment of Notice.
   1. Notice is based on prior similar incidents.
   2. Determine if criminal behavior is likely to pose a risk.
   3. Analyze crime data over varying time periods and distances.
   4. Analyze ‘relevant crimes.’
   5. Anticipate the types of incidents that may cause negligence.
   6. Make comparisons as similar as possible.
   7. Examine adjacent property or a 2-3,000 foot radius.
   8. Police calls during the last five years.
Sample Test Questions

**True or False**

86. The prediction of crime, like risk analysis, is an exact science.  
    \textit{Answer: F}  \ (p. 78)

87. Similar to risk analysis, the prediction of internal crime relies on historical data.  
    \textit{Answer: T}  \ (p. 78)

88. Criminological theories that tend to predict criminal behavior include recidivism, age, demographics, and causation.  
    \textit{Answer: T}  \ (p. 78)

89. Cyclical trends in crime are not of interest to the analyst.  
    \textit{Answer: F}  \ (p. 79)

90. Inadequate security claims are always covered by insurance.  
    \textit{Answer: F}  \ (p. 83)

91. You can extract the raw number of crimes committed from the rate by multiplying the basis by the rate.  
    \textit{Answer: T}  \ (p. 81)

92. Crime analysis completed for security planning purposes is usually not sufficient for presentation to the court subsequent to a negligence (inadequate security) claim.  
    \textit{Answer: T}  \ (p. 83)
93. All courts hold that a business owner gets ‘one free crime’ before foreseeability is established.  
   \textit{Answer: F} (p. 85)

94. Security protection deemed ‘adequate’ by a court of law means these same protections will prevent a business owner from inadequate security liability.  
   \textit{Answer: F} (p. 84)

95. The number of police calls to a location can be used as ‘notice.’  
   \textit{Answer: T} (p. 86)

\textbf{Multiple Choice}

26. If the business- or landowner is ‘on notice’ that future crime is foreseeable they must:  
   \textit{Answer: d} (p. 77)

   a. Immediately post uniformed security officers.
   b. Acknowledge the notice in court.
   c. Become more vigilant.
   d. Prevent the crime, mitigate its effects, and warn of the danger.

27. It is often difficult to defend against inadequate security because:  
   \textit{Answer: a} (p. 84)

   a. The assignment of responsibility can vary from court to court.
   b. Forseeability is difficult to predict.
   c. The concept of ‘notice’ is always after the fact.
d. Attorneys are difficult to find.

28. One justification for using crime prediction over crime analysis is:  \textit{Answer: b} (p. 78)

   bb. It better establishes notice.

   cc. Crime analysis relies on old data.

   dd. It eliminates the ‘hierarchy rule.’ It is used by governmental agencies.

29. Crime statistics are counted for both: \textit{Answer: a} (p. 81)

   a. Time and distance.

   b. Severity and probability.

   c. Relevance and probability.

   d. Direct and indirect loss.

30. The Uniform Crime Report: \textit{Answer: d} (p. 80)

   a. Includes unreported crime.

   b. Derives its data from victimization studies.

   c. Accurately represents crimes across all jurisdictions.

   d. None of the above.

31. The recidivism rate: \textit{Answer: a} (p. 81)
Chapter 10: Crime Prediction

32. When analyzing figures for internal crime, you should: **Answer: a** (p. 78)

33. When attempting to establish notice, the courts have considered crime incidence for a: **Answer: d** (p. 81)

34. ’Notice’ is based upon: **Answer: b** (p. 85)
i. Any prior crime.

j. Prior similar incidents.

k. Breach of control.

l. The posting of security warnings.

35. Courts have held that crime in the neighborhood cannot put a shopping center ‘on notice.’

The analyst should: Answer: a (p. 86)

9. Include neighborhood crime in their study anyway and let the courts decide if it is relevant.

10. Do not include the neighborhood data.

11. Offer your opinion in the analysis as to why the court should or should not consider the data.

12. Because of the court decision, there is no need to complete the analysis.

Short Answer

1. List five Category 1 crimes.

Answer:

Murder

Non-negligent manslaughter

Forcible rape
Robbery
Aggravated assault
Burglary
Grand theft
Motor vehicle theft
Arson

(p. 80)

2. List three factors that affect recidivism rates.

*Answer:*

Evading recapture
Overestimation of the number of re-offenders due to political agendas
Racism

(p. 81)

3. List five direct and indirect costs associated with crime.

*Answer: *Contractual penalties for non-delivery of product, potential loss of market share, extra costs for remanufacturing, the cost of posttraumatic stress counseling, civil litigation, loss of morale, restricted access during crime-scene investigation,
clean-up costs (blood and glass), replacement of the injured worker, and increased worker-compensation premiums. (p. 82)

4. Contrast the differences between crime analysis for budgetary purposes and for defending against a claim of inadequate security.

*Answer:* Crime analysis completed for security-planning purposes is usually not sufficient for presentation to a court subsequent to a negligence (inadequate security) claim. The necessary scope of the analysis, including the type of data analyzed, will change. Property (as opposed to violent) crime, concentration on the specific cause of the injury, and the sources of the data become more important. You must match or exceed the sources of information the opposing parties intend to use in their attempt to establish notice. If the opposition bases its analysis on data that includes arrest and incident numbers, you need to do the same. (p. 83)

5. List five uses of a foreseeability study.

*Answer:*

Lead to a summary judgment of the case;
Pinpoint areas of concentration for guard staff and patrols;
Lead to better utilization of resources and equipment;
Improve overall security and financial planning;
Help to justify security budgets and programs;
Aid in site selection for new facilities;
Lead to better understanding of crime risk.

(p. 83)

Case Study

As part of the risk management program you have established for the corporation, you know you must include the identification of potential threats to corporate assets. Your corporation is in a high crime area. Therefore, the threats to corporate assets must of course include external, man-made threats. Identify the sources you would use to obtain external man-made (crime) threat information and explain why you chose those sources. Your answer should include at least 10 sources.

Answer: See pages 86-88 of the text.
Author’s Notes

Instructors should research the latest legal precedent regard premises and third party liability as court decisions can change the rules radically. Web-based searches, legal journals, and legal consultation can help to monitor or append information contained in the text.
Risk Analysis and the Security Survey 3rd edition

Chapter 11: Determining Insurance Requirements

Learning Objectives

- Students will define risk management.
- Outline risk control options.
- Introduction to crime insurance.
- Gain knowledge to work with risk managers concerning crime insurance.
- Understand mistakes to avoid that may invalidate K&R coverage.

Presentation Outline

I. Risk Management Defined

   A. *Risk management* is the process by which an entity identifies its potential losses and then decides how to treat these potential losses.

   B. Method to treat risk is chosen after a risk is identified, analyzed, and evaluated.

   C. The effect of a risk is the result of a risk analysis.
D. The analysis should tell where, when, and how the risk is incurred.

E. The analysis indicates the extent of loss or liability.

F. The risk manager designs programs to cover losses, exposures, and liabilities.

G. Three basic risk options:
   1. Avoid, eliminate, or reduce to manageable proportions.
   2. Assumed or retained.
   3. Transferred to a third party.

II. Risk Control

A. The process of eliminating or reducing risk to manageable proportions is referred to as “loss control.”

B. By assuming the risk, the company makes itself liable for the loss.
   1. No effort is made to control, eliminate, or minimize the risk.
   2. Self-insurance is referred to as risk retention.

C. Risk transfer endeavors to find the best insurance program.
   1. To be insurable, risks must meet the following requirements:
      a. The risk should be worth the cost and effort to insure.
      b. The risks are calculable.
      c. Losses can be clearly established.
      d. Losses must be accidental, unexpected, and unintentional.
III. Crime Insurance

A. Crime insurance supplements the security program.
   1. Crime insurance has no deterrent effect on crime.
   2. Reimburses the company for losses sustained in a burglary, robbery or internal theft.

B. Most begin with a blanket crime or broad-form storekeepers’ policy.
   1. Comprehensive dishonesty, disappearance, and destruction.
   2. Referred to as a “3D” policy.
   3. This coverage will usually reimburse a company for losses due to:
      a. Employee dishonesty.
      b. Counterfeit currency.
      c. Loss of money, securities, or merchandise through robbery, burglary, or mysterious disappearance.
      d. Certain types of check forgery.
      e. Damage to the premises or equipment resulting from a break-in.

C. Some crime insurance coverage for specific needs includes:
   1. Mercantile safe-burglary policy.
   2. Mercantile open-stock policy.
   3. Fidelity bonds.
   4. Forgery bonds.

D. Insurance premiums vary.

E. Insurance protects against risk that cannot be avoided or controlled.
F. Prevention is the best approach.

G. Most insurance programs do not fully compensate for loss.
   1. Management must become more interested in *avoiding loss*.
   2. Deductibles are intended to reduce the cost of insurance premiums

IV. K&R (Kidnap and Ransom) Coverage

A. Premium costs and the scope of coverage are the basis for selecting insurance providers.

B. Basic coverage provides reimbursement for monies surrendered as a ransom.

C. Several features are incorporated into the policy contract:
   1. Business premises extension reimburses for money lost while on the premises.
   2. Transit extension reimburses funds stolen between leaving the premises and reaching the kidnappers.
   3. Reward extension includes coverage for monies paid to informants.
   4. Personal assets extension reimburses personal assets that are used as a ransom.
   5. Negotiations, fees, and expenses reimburse for expenses incurred to secure the release of a hostage.
   6. Property damage extension covers threats to cause damage to property.
   7. Defense costs, fees, and judgments cover costs resulting from a suit for damages brought by an insured person.

D. General requirements to avoid exclusions:
1. The ransom or extortion demand is specifically made against the named insured.

2. The extortionate demand is made during the time frame of coverage.

3. The company ensures that the existence of the coverage is not disclosed.

E. If a kidnap occurs, reasonable effort is made to determine that:

1. The insured person has been abducted.

2. The police department or Federal Bureau of Investigation has been notified prior to payment.

3. Instructions of the police or FBI are accomplished.

4. The insurance company is notified at the earliest practical time.

5. The serial numbers of the ransom payment are recorded.

F. Some underwriters require written policy and procedural guidelines.

1. Develop a crisis-management program.

2. Helps eliminate confusion before the crisis.

V. Additional Information.

Sample Test Questions

**True or False**

96. Risk management can be defined as the process by which an entity identifies its potential losses and then decides how to treat these potential losses. *Answer: T* (p. 91)

97. The risk analysis will allow the risk manager to design a program to cover the company’s losses, exposures, and liabilities. *Answer: T* (p. 91)

98. Insurance is a form of risk control. *Answer: F* (p. 92)

99. Crime insurance has a significant preventative effect on internal crime. *Answer: F* (p. 93)

100. A forgery bond reimburses merchants and banks for loss due to embezzlement and employee theft of money, and securities. *Answer: F* (p. 93)

101. Insurance should be used for protection only against risk that cannot be avoided or controlled through the effective use of property, casualty (safety), and security techniques. *Answer: T* (p. 93)
102. A transit extension covers employees who are kidnapped while traveling.  
   \textit{Answer: F} (p. 95)

103. Some K&R policies require you to name specific individuals that are covered.  
   \textit{Answer: T} (p. 95)

104. Making the specifics of a K&R insurance policy known to the public will help to prevent a K&R incident and make reimbursement easier. \textit{Answer: F} (p. 96)

105. Insurance companies do not generally indemnify against being sued by a kidnapped employee. \textit{Answer: F} (p. 95)

\textbf{Multiple Choice}

36. Self-insurance is referred to as: \textit{Answer: c} (p. 92)

   a. Risk control.
   b. Risk transfer.
   c. Risk retention.
   d. Risk avoidance.

37. To be insurable, risks must substantially meet the following requirement: \textit{Answer: a} (p. 92)
a. Losses can be clearly established as to occurrences and amounts.
b. Losses are not ‘accidental’ in nature.
c. Deductibles are not set too high.
d. Any risk is insurable.

38. A ‘3D’ policy means:  *Answer: a*  (p. 93)

   ff. Dishonesty, disappearance, and destruction.
   gg. Disaster, deceit, and duplicity.
   hh. Devastation, deception, and damage. Duplicity, deception, and destruction.

39. Insurance premiums vary according to:  *Answer: d*  (p. 93)

   a. Type of business.
   b. Location.
   c. Prior losses.
   d. All of the above.

40. Most insurance programs:  *Answer: a*  (p. 94)

   a. Do not fully compensate for a loss, regardless of the coverage.
   b. Compensate completely for a loss, if coverage is high enough.
c. Compensate fully only if you have deductible coverage.

d. None of the above.

41. Which of the following can render K&R coverage invalid?  
   Answer: a  (p. 95)

   a. The ransom or extortion demand is not specific to a named insured.
   b. The demand is made 30 days before policy renewal.
   c. International or local law that does not license the insurance company to operate in their jurisdiction.
   d. None of the above.

42. If a kidnap occurs, which of the following must be done?  
   Answer: d  (p. 96)

   a. The police or FBI is notified prior to payment.
   b. The insurance company is notified at the earliest practical time.
   c. Serial numbers of the ransom payment are recorded.
   d. All of the above.

43. Some underwriters require that the following occur immediately upon obtaining coverage:  
   Answer: a  (p. 96)

   b. Development of a comprehensive risk management program.
c. Maintaining profiles on potential victims.

d. All of the above.

44. Security policy and procedure is a form of:  \textit{Answer: a}  (p. 92)

\begin{itemize}
  \item[m.] \textbf{Risk control.}
  \item[n.] \textbf{Risk transfer.}
  \item[o.] \textbf{Risk retention.}
  \item[p.] \textbf{Risk avoidance.}
\end{itemize}

45. Which of the following is true?  \textit{Answer: d}  (p. 94-95)

\begin{itemize}
  \item[13.] Prevention, through risk avoidance, elimination or control, is the best approach to the preservation of corporate assets.
  \item[14.] Management must become more interested in avoiding loss.
  \item[15.] Premium costs and the scope of coverage are generally the basis for deciding which company to place K&R insurance with.
  \item[16.] All of the above.
\end{itemize}

\textbf{Short answer}

1. Explain risk control. Give examples.
**Answer:** Risk control is the risk management process of eliminating or reducing risk to manageable proportions, usually by programming security and safety procedures to do away with problems or to reduce them to acceptable or manageable levels of severity. This is also referred to as “loss control.” Other examples of risk control include: fire sprinklers, electronic security systems, Uninterruptible Power Supply (UPS), etc. (p. 92)

2. From a high level, outline an executive protection program.

**Answer:**

I. Home and Family

II. Office and Work

III. Travel

IV. Personal Protection

V. Crisis Management

(p. 96-98)

3. Why should, or should not, a business purchase all K&R insurance coverage available?

**Answer:** To cover a situation if the money is lost while it is on the premises, stolen between leaving the premises and reaching the kidnappers, for monies paid to
informants whose information leads to the arrest and conviction of the individuals responsible for the kidnapping, to reimburse the insured persons for their personal assets that are used as a ransom payment if the demand is made on the insured person and not the corporation, to reimburse for reasonable fees and expenses incurred to secure the release of a hostage, including interest on a bank loan to pay a ransom payment and to provide coverage against physical damage to property. Also to cover costs resulting from any suit for damages brought by an insured person.

(p. 95)

4. Recommend a course of action for the owner of a small retail business located in a high-crime area. Include in your recommendation an explanation of why you did or did not include the purchase of insurance.

Answer: Do not purchase insurance – use loss prevention and control measures. Insurance should be used for protection only against risk that cannot be avoided or controlled through the effective use of property, casualty, and security techniques. Merchants operating in some high-risk crime areas and thus needing insurance most are often the least able to afford the premiums. Further, it is difficult to find insurance companies willing to underwrite crime coverage in high-risk crime areas. Companies that experience a number of robberies or burglaries usually face escalating premiums, or worse, canceled policies. Prevention, through risk
avoidance, elimination, or control, is the best approach to the preservation of corporate assets. It is also recognized that most insurance programs do not fully compensate a firm for loss, regardless of the coverage. (p. 93, et al.)

**Research**

1. From a financial point of view, what do companies do when they retain risk?

*Answer:* They can completely expense a loss using an unfounded or funded reserve (these reserves may be investment managed), relying on an affiliated (‘captive’) insurer. A Risk Retention Group is a corporation or other limited liability association, functioning as a captive insurance company and organized for the primary purpose of assuming and spreading the liability risk exposure(s) of its group members (member-owners). A Purchasing Group (PG) is an organization that purchases liability insurance on a group basis from an insurance company or a Risk Retention Group (RRG) for its members. Unlike an RRG, a PG is not an insurance company and its members do not underwrite their own coverage. However, like RRGs, PGs are subject to the same, similar, or related tests pertaining to membership, exposures, and types of coverage(s) offered.
Some sources:

http://www.nrра-usа.org/ National Risk Retention Association

http://www.rrr.com/ Risk Retention Reporter

2. Contact a major insurance company and report on the coverage and services they offer under their K&R policies. To what degree do they provide K&R consulting services?

*Answer:* Most major insurance companies at the time of printing offer K&R or can refer to a carrier that does. Web based searches can reveal companies that specialize in this coverage.

**Case Study**

Some underwriters (insurance companies) require that, immediately upon obtaining coverage, written policies and procedures must be in place to protect the corporate assets. Included in the definition of corporate assets are those in executive management positions whose value to the corporation is determined to be so important that they must be protected as high-value corporate assets.
As the corporate security manager, you have the responsibility for their protection. Develop an executive protection program outline to be used as part of a baseline for an executive protection program.

*Answer: See pages 96-98 of the text.*
Risk Analysis and the Security Survey 3rd edition

Chapter 12: Mitigation and Preparedness

Learning Objectives

- The base concept of disaster and business continuity planning is the Comprehensive Emergency Management model (CEM).
- CEM is increasingly applied to security management.
- Understand additional threat identification methods.
- Select cost-effective mitigation strategies.
- Identify preparedness actions and programs.

Presentation Outline

V. Comprehensive Emergency Management

A. Originated in public sector planning (FEMA).
B. Integrated approach.
C. Addresses the treatment of risk.
D. Consists of four components.

E. Not a linear process.

VI. Mitigation

A. Sustained action that reduces or eliminates risk.

B. Can reduce occurrence of a hazard.

C. Cost-effective
   1. Terrorism cost-benefit more difficult to demonstrate.

D. FEMA methodology
   1. Geared toward regional planning.
   2. Four major steps:
      a. Organize resources.
      b. Assess Risks.
      c. Develop mitigation plan.
      d. Implement plan and monitor progress.
   3. Similar to business model:
      a. Identify hazards.
      b. Devise strategies.
      c. Select cost-effective solutions.
      d. Implement solutions.

E. Hazard Identification
   1. Historical events and conditions:
a. Predict impact of past events.
b. Recurrence rates.
c. Libraries.
d. Historians.
e. Newspapers.
f. Declared disasters.
g. Land use permits and geological reports.
h. Internet.
i. Insurance companies.
j. Community experts.

2. Inspections

a. Use macro and micro view.
b. Community hazards.
c. Cause and effect.
d. Collateral or synergistic damage.

3. Checklists

a. Usage
b. Should answer:
   i. How can employees be injured?
   ii. How can critical systems and assets be damaged or attacked?
   iii. What single points of failure exist?
   iv. What hazards can disrupt operations?
   v. How will hazards affect the environment?
4. HAZUS
   a. Used with GIS software.
   b. Estimates physical and economic damage patterns.

5. Process Analysis
   a. Used for complex operations.
   b. Hazard and Operability (HAZOP):
      i. Deviation from design intent.
      ii. Guide words.
      iii. Consequences mapped.
   c. FMEA
      i. Identifies relative risk of process design.
      ii. Assigns Risk Priority Number.
   d. PrHA
      i. Inventory system of hazards and their risks.
      ii. Develops expected loss rate.

6. Experts
   a. Consultants.
   b. Engineering firms.
   c. Equipment manufacturers.
   d. Department heads or process owners.

7. Cause and Effect
   a. Anticipate the unexpected.
   b. Scenario planning.
i. Devises strategies based on future variables.

ii. Use frame of reference or mindset of the ‘enemy.’

iii. Technical feasibility.

8. Methodology

9. Department of Homeland Security

a. Hazard identification includes four conditions:

   i. Application mode.

   ii. Duration.

   iii. Dynamic and static characteristics.

   iv. Mitigating and exacerbating conditions.

b. Inherent vulnerability.

c. Tactical vulnerability.

d. Identifies vulnerabilities through an examination of:

   i. Visibility.

   ii. Utility.

   iii. Accessibility.

   iv. Asset mobility.

   v. Hazardous materials.

   vi. Collateral damage.

   vii. Occupancy.

e. Threats are ranked to determine criticality.

F. Mitigation Strategies

1. Strategies are both general and specific in nature.
2. General strategies may be classified as:
   a. Risk management.
      i. Hierarchy of control.
   b. Engineering controls.
   c. Regulatory controls.
   d. Administrative controls.
   e. Service agreements.
   f. Redundancies and divergence.
   g. Separation of processes or hazards.

3. Specific Mitigation can include:
   a. Alternate power sources.
      i. Source of most common ‘disasters.’
      ii. Uninterruptible Power Supply.
      iii. Multiple grids.
      iv. Backup generators.
   b. Alternate communications
      i. Network overload.
      ii. Service and replacement agreements.
      iii. Bypass circuits and fax lines.
      iv. Divergent routing.
      v. Cellular backup.
      vi. Satellite systems.
      vii. Hot/cold sites.
viii. Third party call centers.

c. Policies and procedures.

d. Data backup strategies:

   i. Daily incremental.

   ii. Full backup.

   iii. Archiving.

   iv. Data taken off site.

e. Records management:

   i. Loss of records major risk.

   ii. Loss could bring criminal sanctions.

   iii. Vital records are important to continued and future operation.

   iv. Examples.

   v. Protection of vital records.

f. Facilities salvage and restoration:

   i. Consequences or a fire or flood.

   ii. Services available.

   iii. Equipment and expertise not generally available internally.


   v. Pre-registration.

G. Cost-Effectiveness of Mitigation.

1. Solutions must be:

   a. Cost-effective.

   b. Technically feasible.
c. Not create additional hazards.

2. Mitigation often represents significant capitol outlay.
   a. Prioritize projects.
   b. Spread over multiple funding sources.
   c. Solve multiple risks with fewest strategies.
   d. Have alternate strategies.
   e. Demonstrate cost of ‘losses avoided’ and displacement costs.
      i. Consider ‘upgrade’ costs.

VII. Preparedness

A. Steps taken to enable response.

B. National preparedness goals.

C. Important component of CEM.

D. Examples of preparedness.

E. Personal preparedness:
   1. Value to business.
   2. Training topics.
   3. CERT training.

F. Emergency supplies:
   1. Minimum 72 hour supply.
   2. Contents of cache.
   3. Spare parts.
G. Service level agreements.

H. Justification.
Sample Test Questions

True or False

106. Mitigation and preparedness are two of the five components that comprise Comprehensive Emergency Management. Answer: F (p. 101)

107. Preparedness is sustained action that reduces or eliminates long-term risk to people and property from hazards and their effects. Answer: F (p. 102)

108. Some companies have reported saving millions of dollars due to their mitigation strategies. Answer: T (p. 102)

109. The concepts of crime prevention and prevention in general fall with the category of preparedness. Answer: F (p. 102)

110. Terrorist acts that are committed by those who think rationally are more difficult to predict than acts committed by those who do not. Answer: F (p. 107)

111. The technical ability of a terrorist to carry out an attack is not considered in your analysis. Answer: F (p. 108)

Copyright 2006 © Elsevier, Inc. All rights reserved.
112. An examination of what other companies have done in the way of mitigation is a waste of valuable resources, as the circumstances and environment of other companies are likely different from your company.  *Answer: F* (p. 109)

113. FEMA and other preparedness agencies advocate that businesses and individuals have the ability to sustain themselves for a period of 48 hours after a disaster.  *Answer: F* (p. 120)

114. Vendor relationships are often cited as the most important element that gets organizations back in business quickly after a disaster.  *Answer: T* (p. 120)

115. Unlike mitigation, preparedness measures, although generally far less expensive, may be more difficult to justify or to elicit cooperation.  *Answer: T* (p. 121)

**Multiple Choice**

43. FEMA’s mitigation planning encompasses the following steps:  *Answer: d.* (p. 103)

   u. Obtain agreement, identify hazards, determine costs, and list mitigation solutions.

   v. Identify hazards, develop mitigation plan, and implement plan.

   w. Assess risks, conduct Business Impact Analysis, develop plan, implement plan.

   x. Organize resources, assess risks, develop mitigation plan, and implement and monitor the plan.
44. The cost/benefit ratio of mitigation strategies is more difficult to determine when dealing with terrorist acts because:  
   Answer:  d. (p. 103)  
   
   a. The recurrence rate is more of a guess.  
   b. Quantification of damage may not be predictable.  
   c. Time period of exposure may vary.  
   d. All of the above.  

45. Which of the following is not true about checklists?  
   Answer:  a (p. 105)  
    
   ii. Because of their detail, they can identify all hazards.  
   jj. They should ask how employees may be injured.  
   kk. They should examine perils under both normal and disaster conditions. They are best used as reminders.  

46. Which of the following is true about scenario planning?  
   Answer:  a (p. 107)  
   
   a. It is a tool to identify and devise strategies based on future variables.  
   b. It helps to justify the mitigation budget.  
   c. It is only effective when used by those certified in its methods.  
   d. It is not a structured process.
47. The Hierarchy of Control, in the proper order, consists of: \textit{Answer: c (p. 110)}

a. Engineering, Elimination, Substitution, and Administrative controls.

b. Administrative, Elimination, Substitution, and Engineering controls.

c. Elimination, Substitution, Engineering, and Administrative controls.

\textit{Answer: c (p. 110)}

d. Substitution, Elimination, Engineering, and Administrative controls.

48. One of the most common and low-cost forms of mitigation is: \textit{Answer: c (p. 111)}

a. Engineering Controls.

b. Separation of Hazards.

c. Uninterruptible Power Supply.

d. Third party call centers.

49. Most ‘data disasters’ are caused by: \textit{Answer: c (p. 114)}

a. Lightning.

b. Equipment failure.

c. Users.

d. Software crashes.

\textit{Answer: c (p. 114)}

50. Many businesses that have not recovered after a disaster considered the loss of which of the following as the primary cause of the business failure: \textit{Answer: c (p. 115)}
a. No insurance.

b. Loss of inventory.

c. Loss of business records.

d. Disaster impact on customers.

51. Restoration service providers claim that restoration can save up to what percent over replacement costs?  \textit{Answer:} \textbf{c} (p. 117)

52. Displacement costs:  \textit{Answer:} \textbf{a} (p. 117)

a. Represent the dollar amount to relocate a function or building’s functions on a temporary or permanent basis.

b. Do not consider the loss of sublease revenue.

c. Do not consider costs to relocate back to the original facility.

d. All of the above.

53. Preparedness information is most effective when:  \textit{Answer:} \textbf{a} (p. 121)
a. Presented repeatedly.

b. Graphic pictures of what can happen are shown.

c. Delivered through ‘official’ channels.

d. Presented in technical terms.

54. The National Preparedness goals are primarily intended to: **Answer:** c (p. 118)

a. Ensure the public maintains a 72 hour supply of provisions.

b. Mandate preparedness programs for business and industry.

c. Guide federal, state, and local entities.

d. Develop response procedures.

55. Public-private partnerships: **Answer:** d (p. 120)

a. Can be difficult to cultivate.

b. Can be advantageous to both business and government.

c. May be restricted by regulation.

d. All of the above.
Short Answer

5. Justify the position that Comprehensive Emergency Management is not a linear process.

*Answer:* Mitigation is generally considered the first phase of CEM, as its goal is to reduce risks prior to an event, but it is not a linear process. Many believe it is important to integrate the recovery and mitigation phases, but acknowledge that mitigation takes place during the other three phases of emergency management. The availability of funds and interest in taking action is at its highest post-disaster (and therefore in the response and recovery phase) and the opportunity to design mitigation into building replacement at a time when insurance funds are available also occur post-disaster. Lessons learned after the response and recovery phase are also incorporated into design and program updates. Mitigation should start and end the process. (p. 103)

6. Contrast the argument that terrorist acts are easy to predict with the argument that they cannot be identified or predicted.

*Answer:* Organized groups such as Al Qaeda, the Irish Republican Army, and others tend to follow the same methods and use the same destructive tactics throughout their existence. Kidnapping may be the preferred method of one, whereas bombings may be used by another group, often with little variation. Scenario planning can be used to anticipate acts against targets.
Unlike natural hazards that follow the laws of nature, occur more often, and are therefore more predictable, the acts of a terrorist are more difficult to anticipate. Because targets are often mobile and the terrorist can select those most vulnerable and that return the highest “yield” to their objective, many argue that the threats they pose cannot be identified or predicted. Terrorists whose thought processes are on the fringe or delusional are more difficult to predict.

(p. 107)

7. Many companies stockpile catches of disaster supplies and provisions in a central location for use by employees during or after a disaster. Discuss the disadvantages of this practice and suggest an alternate.

*Answer:* It can be expensive through the need to replenish the supplies every 3-5 years, locating all of the supplies in one location exposes them to vulnerability to damage, theft, or sabotage, and cannot provide for the needs of individual employees. An alternate method, at least for smaller supplies, is to issue a carry bag of supplies (food, water, basic first aid supplies, light sticks, battery powered radio, etc.) when they are first hired. Employees then keep these in their desk or car with instructions to customize the contents to their individual needs (prescription medications, reading glasses, pictures of loved ones, clean underwear, etc.). The bag can contain the company or department logo. (p. 120)
8. Outline the topics you would cover if asked to give a home disaster preparedness presentation to your employees.

*Answer:*

**Topics should include:**

- Emergency contacts and meeting locations;
- Emergency supplies (food, water, medical, sanitary);
- Structural and non-structural mitigation;
- Insurance considerations and documentation;
- Fire prevention and control;
- First Aid CPR;
- Shelter in Place instructions;
- Emergency procedures;
- Evacuation routes;
- Warnings and media sources;
- Light search and rescue;
- What to do and not to do.

(p. 119)

9. Discuss why the loss of vital records is an important issue.
Answer: The loss of these records can severely damage future sales, cash flow and insurance reimbursements. The failure to protect them and their subsequent loss can bring criminal sanctions against management. The availability of vital records will reduce recovery time. Their loss can cause the failure of the company. (p. 115)

Case Study

During your business impact analysis, you identify that one of your office buildings next to a small river is located about five miles below an earthen dam that was constructed about one hundred years ago and recent geological reports indicate a degree of weakening. Your company owns the building and sub-leases 100,000 square feet at $2.25 per square foot. Your company occupies 85,000 square feet. The value of your equipment located in the building is $4,250,000 and the combined salaries total about $7,650,000. Revenue produced last year for this facility was $20,000,000. New building construction averages about 6 months to complete at a cost of $5.50 per square foot. Justify the mitigation solutions you would recommend.

Answer: There are many solutions or approaches to this problem. History has shown, especially in areas at high risk from earthquake, heavy rain and ice, that earthen dams, once weakened, are prone to sudden catastrophic rupture. A diversion dam or other type of diversion near the facility would likely be ineffective. Probably the best solution is to recommend that the property be sold and the company relocate operations elsewhere. This could be in a newly constructed building or one that is leased. In their justification, they
should explain the rationale for their solution, and include a cost comparison of the potential loss versus the cost to relocate, rebuild, moving costs and other costs. The costs could include liability for employee injury, lost revenue, etc. If moving to a temporary location, they should include costs to move to the permanent location.
Chapter 13: Response Planning

Learning Objectives

- Importance of response planning.
- Understand the Incident Command System and other elements of emergency response.
- Basic awareness of potential disaster conditions.
- Recommended response guidelines.

Presentation Outline

I. Introduction
   A. Change in focus post-September 11, 2001.
   B. Ramifications of poor response to emergencies.
   C. Response planning an element of Comprehensive Emergency Management.
   D. Services not always available post-disaster.
   E. All organizations must have a response capability:
      1. Required in the US under Fed OSHA.
3. Many States also require response planning.
4. Requirement under NFPA 1600.
5. Civil liability.

F. Emergency response defined.

G. National Response Plan.

H. National Incident Management System.

II. Incident Command System

A. System used by fire and police to manage the response to an emergency.
   1. Primarily field response.
   3. Advantages to organizing business response organizations under ICS.
   4. Relies on management by objectives.
   5. Small span of control.

B. Five Major Functional Units:
   1. Command.
   2. Operations.
   3. Planning and Intelligence.
   4. Logistics.
   5. Finance and Administration.
   6. Not All Units (Sections) Need Activation.

C. Command.
   1. Incident Commander (IC) has overall responsibility.
2. Role Filled By:
   a. First to Arrive.
   b. Designated Commander.

3. Establishes a Command Post (CP).

4. Section Chiefs and IC wear distinctive vests.

D. Duties of the IC include:

1. Field management of the emergency.
2. Coordination with the EOC or other IC’s.
3. Ultimate responsibility for safety of responders.
4. Approval of all plans and resources.
5. Setting objectives and priorities.
6. Delegating authority as necessary.
7. Primary responder until others arrive.

E. IC may establish the following positions:

1. Information Officer (PIO).
2. Safety Officer.
3. Liaison Officer.

F. Operations Section:

1. Implements action plans and objectives.
2. ‘Reality’ check goals.
3. Direct necessary resources.
4. Provide status reports to IC.

G. Planning and Intelligence:
Chapter 13: Response Planning

1. Develop Incident Action Plans.
2. Determine necessary resources.
3. Analyze conditions and the scope of the incident.
4. Project or predict changing conditions.
5. Prepare contingency plans.
6. Track resources.

H. Logistics:
   1. Obtains all resources and services.

I. Finance and Administration:
   1. Maintains the history of the response.
   2. Tracks and approves expenditures.
   3. Produces final cost report.

III. Emergency Operations Center

A. The Emergency Operations Center (EOC) directs or coordinates the response or the business recovery:
   1. Also called Command Center.
   2. Should have alternate location.
   3. Governmental is more resource oriented, business is more strategic.

B. Primary functions of a governmental EOC:
   1. Coordinate response to large or multiple events.
   2. Create or refine policy.
   3. Allocate resources.
4. Collect and manage information about the incident, responses, and decisions.

5. Release information to the public.

6. Maintain appropriate records.

C. The design must anticipate complexity:

1. Must facilitate the flow of information.

2. Should be located in:
   a. Secure, structurally safe building.
   b. Centrally located.
   c. Easily accessible.

3. Can be a large conference room.

D. EOC should contain:

1. Extra phone sets and phone jacks.

2. Room for status boards.

3. Separate work space.

4. Fax machines.

5. Supplies.

E. Access control (security) is important.

F. Connected to a back-up power generator.

G. Must be ‘user friendly.’

H. Designed to operate continuously.

I. Keep operations as quiet as possible.

J. Video conferencing capability is useful.
K. Don’t overwork the EOC staff.

IV. Emergency Response Team

A. Internal organization of employees.
B. Typically volunteers from various functions.
C. Should use an ICS structure.
D. Advantages:
   1. Intervene and stabilize emergencies.
   2. Reduce injuries and loss.
   3. Prevent adverse publicity.
   4. Demonstrate management concern.
   5. Minimize impact on the environment.
   6. Comply with regulatory requirements.
   7. Become the sole response in a disaster situation.
E. Basic steps to form team:
   1. Management acceptance and support.
   2. Determine scope of the team’s duties and responsibilities.
   3. Develop response plans, policies, procedures.
   4. Determine equipment and resource needs.
   5. Recruit team members.
   6. Develop training programs.
   7. Conduct regular drills.
8. Advertise.

VI. Emergency Response Procedures

A. Necessary to identify and understand the characteristic of hazards.

B. General guidelines.

C. Does not list all foreseeable emergencies.

D. Always assess situation before response.

E. Mitigation/prevention, response, limited recovery format.

F. Bomb threats:
   1. Terrorists bombings expected to increase.
   2. Improvised Explosive devices (IED), VBIED.
   3. History and extent of use.
   5. Effects.
   6. Threat evaluation:
      a. Low probability.
      b. Evacuation generally not result.
      c. Always search.
      d. Credibility and evaluation (Risk Profile):
         i. Level of security.
         ii. Controversial business activity.
         iii. Recent events.
iv. History of bombings and threats.

v. Intelligence.

vi. Contents of threat.

7. Evacuation
   a. Controversial and difficult decision:
      i. Cause needless loss of productivity.
      ii. Decrease employee morale.
      iii. Increase the possibility of injury from the evacuation.
      iv. Satisfy the intent of the caller.
   b. Typical placement of devices:
   c. If device found:
      i. Evacuate safe distance away from blast effects or send employees home.
      ii. If threat is credible with less than 30 minutes delay, search and evacuate.
      iii. If credible with time greater than 30 minutes, initiate a search.

8. Searches:
   a. Almost always search.
   b. Who should search?
   c. Search must be systematic, rapid, and thorough.
   d. Use of communication devices.

9. Device found (see response):
a. Attempt to find owner of suspicious objects.

b. Isolate area.

c. Evacuate.

d. Open doors and windows around the blast area.

e. Shut off hazardous processes and utilities in the area.

f. Continue to search for other devices.

g. Do not touch or move the object.

h. Do not cover the object or cut any wires.

i. Do not put the object in water or pour water on it.


10. Package bomb:

a. Characteristics:

   i. Unusual postmarks or places of origin.

   ii. Excessive postage.

   iii. Incorrect addresses or titles of recipients.

   iv. Excessive handling, wrapping, taping or inappropriate bulkiness.

   v. Excess weight, stiffness, bulges or uneven balance and feel.

   vi. Smudges and greasy-looking spots or areas.

   vii. An odor of almonds or a chemical odor.

   viii. Protruding wire or string.

   ix. Pinholes.

b. Prevention and response.
11. Suicide Bombs:
   a. Description.
   b. Perpetrators.
   c. Response.

12. Radiological Dispersal Device (RDD):
   a. Description.
   b. Capabilities and limitations.
   c. Impact of use.

13. Mitigation:
   a. Intelligence program.
   b. Engineering evaluations.
   c. Dampers on vents located away from the ground.
   d. Improve fire prevention and protection systems.
   e. Locate critical facilities, offices, and processes away from the perimeter.
   f. Remove hiding places for IED’s.
   g. Design crash-through protection.
   h. Establish no-parking zones.
   i. Isolate employee parking.
   j. Create space.
   k. Other environmental design.

14. Prevention:
   a. Analyze exposure.
b. Audit.
c. Physical security.
d. Incoming inspection.
e. Access and internal controls.
f. Threat questionnaires placement.
g. Provide specific training.
h. Establish who will evaluate threats.
i. Develop relevant procedures.
j. Establish evacuation criteria and protocols.
k. Identify search methods and personnel.
l. Identify and prioritize search areas.
m. Establish a procedure to track the progress of a search.
n. Test all procedures.
o. Review plans, procedures, and phone numbers regularly.
p. Understand community’s capabilities.

15. Response:

a. Write down the *exact* time of a telephoned threat.
b. Ask:

   ii. When will it explode?
   iii. Where is it located?
   iv. What does it look like?
   v. Why was it placed?
   vi. Who is calling?
c. Attempt to transfer the call.

d. Initiate a search.

e. Make other notifications as appropriate.

f. If a device is found:
   i. Evacuate at least three hundred yards out of the line of sight.
   ii. Call emergency services (police, fire).
   iii. Identify/evaluate the object.
   iv. Do not touch, move, dismantle, or pour water on object.
   v. Open doors and windows.
   vi. Isolate (secure) the area from entry.
   vii. Consider shutting down utilities and hazardous processes.
   viii. Continue the search for additional bombs.
   ix. Relocate vital records and back-up computer systems.
   x. Activate the crisis management plan.
   xi. Stage emergency response equipment and strategic resources.
   xii. Restrict access to the area.
   xiii. Remove injured immediately.

g. If RDD is suspected:
   i. Move upwind or go inside.
   ii. Cover or filter your mouth and nose.
   iii. Once inside, remove clothing and seal it in a plastic bag.
   iv. Shower to remove the remainder of the dust.
   v. Shut all windows, outside doors, and dampers.
vi. Turn off fans and HVAC.

vii. Monitor TV and radio stations for news and instructions.

16. Recovery:
   a. Care for the injured.
   b. Begin rescue operations.
   c. Assess damage.
   d. Begin salvage and cleanup.
   e. Test for blast damage.
   f. Keep employees informed.
   g. Provide posttraumatic stress counseling.
   h. Begin relocation and reconstruction.
   i. Investigate and prosecute every incident.

G. Earthquake.

1. Causes:
   a. Tectonic plates.
   b. Fault zones.

2. Measurement:
   a. Richter scale.
   b. Modified Mercalli Scale.

3. Effects:
   a. Soil conditions.
   b. Liquefaction.
c. Structures.
d. Infrastructure.
e. Emergency services.
f. Collateral damage.
g. Tsunami.

4. Forecasting.

5. Mitigation:
   a. Understand seismic risk for your area.
   b. Identify structural and non-structural hazards.
   c. Use sway bracing on automatic fire-sprinkler systems.
   d. Bolt or base-isolate tall and heavy objects.
   e. Strap (secure) sensitive, critical, or expensive equipment.
   f. Identify and mitigate other nonstructural hazards.
   g. Strap water heaters to the wall.
   h. Install flexible connections to the gas line.
   i. Install seismic switches.
   j. Prepare a mass causality plan.

6. Preparedness:
   a. Stockpile food, water, lighting, and disaster first aid supplies.
   b. Encourage individual and family preparedness.
   c. Consult with a structural engineer.
   d. Train personnel in the location of emergency shutoff valves.
   e. Train employees in first aid and cardiopulmonary resuscitation.
f. Maintain an adequate supply of cash.

g. Set up an agreement with city and local inspectors.

h. Earthquake insurance.

7. Response:

a. Duck, cover, and hold.

b. Move away from windows, buildings, or overpasses.

c. Do not run outside during the shaking.

d. After shaking, evacuate the building if structural damage.

e. Avoid use of the telephone.

f. If wires fall onto your vehicle, stay inside until rescued.

g. Do not use open flames.

8. Recovery:

a. Check for injuries.

b. Rescue victims.

c. Check the structural integrity of the building.

d. Check for fires and other damage.

e. Clean up hazardous material spills.

f. Turn off non-critical electrical equipment if power is out.

g. Avoid the use of open flames.

h. Use caution when reentering damaged buildings.

i. Check for separation of vents and exhaust pipes.

j. Listen to radio and TV stations.

k. Begin relocation and reconstruction if necessary.
H. Chemical or Biological Attack.

1. Source of threat and intent.

2. Threats:
   a. Synergistic targets.
   c. Vesicants.

3. Challenges for delivery.


5. Warning signs of attack:
   a. Not always immediately apparent.
   b. Hospitals may be the first to detect.
   c. Sudden high levels of absenteeism.
   d. Droplets of oily film on surfaces or water.
   e. Unusual dead or dying animals in the area.
   f. Unusual or unauthorized spraying (crop dusting).
   g. Symptoms of illness.
   h. Mass casualties.
   i. Low-lying clouds or fog, dust or particles unrelated to weather.
   j. People unusually dressed.
   k. Unexplained odors.
   l. Observation of dispersal devices.
6. **Mitigation:**
   a. Control toxic and hazardous chemicals.
   b. Store chemical tankers inside buildings or secured yards.
   c. Substitute less toxic substances.
   d. Minimize the amount of chemicals used.
   e. Secure access to ground level air intakes.
   f. Install filters on air systems.
   g. Protect building utilities from tampering.
   h. Install HVAC venting and purging systems.
   i. Design security into new construction.
   j. Isolate mail rooms.

7. **Preparedness:**
   a. Understand the types and properties of biological and chemical agents.
   b. Identify businesses in the immediate area that could affect your operations.
   c. Develop procedures to notify of imminent hazard.
   d. Develop evacuation routes and procedures.
   e. Assess the physical security of buildings.
   f. Restrict access to mechanical rooms.
   g. Identify safe rooms to use for sheltering-in-place.
   h. Develop procedures and training programs for employees.
   i. Develop a means to quickly monitor conditions.
j. Identify sudden, out-of-the-ordinary absenteeism.

8. Response:
   a. Move upwind from the source of the attack.
   b. Move indoors to an interior room on a higher floor.
   c. Close building dampers, windows, and doors.
   d. Turn off HVAC systems.
   e. ‘Shelter in place.’
      i. Close all windows and exterior doors.
      ii. Shut off air conditioning and heating systems.
      iii. Use duct tape to seal cracks around windows and doorframes.
      iv. Cover bare arms and legs and bandage any cuts or abrasions.
      v. Choose a room with access to a bathroom and telephone.
      vi. Store provisions.
   f. If splashed with an agent:
      i. Wash off using warm soapy water or 10:1 bleach solution.
      ii. Take off clothing.
      iii. Place your clothing in a sealed plastic bag.
      iv. Locate a fountain, pool, or other source of water to rinse if outside.
      v. Use talcum powder or flour if no water.
   g. If in a car, shut off outside air intake vents and roll up windows.
   h. Seek medical assistance as soon as possible.
   i. If anthrax is suspected:
i. Do not handle, shake, or empty the letter or package.

ii. Place contents in plastic Ziploc bag.

iii. Wash your hands with soap and warm water and then wash your face.

iv. Blow and wipe your nose.

v. Close the doors and windows of the room where the package or letter is located.

vi. Turn off air conditioning, heating and fans.

vii. Collect the names of all persons who have had contact with the letter or package.

viii. See your health care provider immediately.

ix. Call the police and fire department.

j. Monitor news broadcasts.

k. Maintain resource information.

9. Recovery:

a. Plan for an extended relocation.

b. Track employees who may be quarantined, killed, or evacuated.

c. Develop a mass casualty plan.

d. Establish work-at-home capability or alternate work sites.

e. Cross-train employees.

f. Minimize direct contact with others.

g. Disinfect phones and other work surfaces on a regular basis.

h. Maintain out-of-region resources to meet continuity objectives.
i. Keep copies of building design and engineering data off site.

j. Educate employees about building re-entry.

I. Evacuation Planning:

1. Post-September 11, 2001 changes.

2. Consequences of evacuation.

3. Employee orientation and training.

4. Relocation.

5. Verification:
   a. Roll call.
   b. Floor Wardens:
      i. Duties and responsibilities.
      ii. Identification.
      iii. Search areas.
      iv. Training.

6. Include visitors and disabled.

7. Drills.

8. Mitigation:
   a. Connect warning systems and fire panels to backup power.
   b. Ensure planning conforms with codes and standards.
   c. Assign a dedicated Fire Safety Director.
   d. Upgrade life safety elements of the building.
   e. Increase the evacuation discharge area.
f. Keep current on the latest standards and evacuation procedures.

g. Have redundant communication systems in place.

h. Ensure stairwell doors unlock during an evacuation or fire.

i. Maintain close ties with the fire department.

j. Determine if the fire department will search stairwells.

9. Preparedness:

   a. Determine who will plan, coordinate, and authorize evacuations.

   b. Develop a script(s) to use when announcing an evacuation.

   c. Develop unobstructed emergency escape routes.

   d. Devise special procedures for employees to stay behind.

   e. Select and train evacuation monitors or floor wardens.

   f. List methods used to notify employees of an evacuation.

   g. Identify employees with handicaps.

   h. Establish assembly points.

   i. Devise a method to account for employees and guests.

   j. Establish ‘all clear’ (re-entry) procedures and guidelines.

   k. Document the plan.

   l. Conduct drills often.

10. Response:

    a. Shut down hazardous processes prior to evacuation.

    b. Train all employees to recognize the evacuation signal.

    c. Leave immediately by the nearest exit.

    d. Do not return to the work area.
e. Do not use elevators in a fire situation.

f. Assist the disabled.

g. Go directly to the assembly point.

h. Do not reenter the building until the “all clear” is given.

i. Ensure that all employees and guests evacuate.

j. Notify emergency officials if anyone is not accounted for.

k. Keep employees informed.

l. Close stairwell doors after you enter, do not prop them open.

m. Remove high heel or flip-flop shoes if descending stairs.

11. Recovery:

a. Establish methods to disseminate return-to-work instructions.

b. Review the plan and procedures at least annually.

c. Instruct business continuity team members to take laptop computers with them.

J. Fires.

1. Consequences:

a. Greatest number of losses to business.

b. 64 to 70 percent of businesses never recover.

c. Death and injury.

2. Causes:

a. Equipment failure.

b. Careless acts.
c. Natural and man-made disasters.
d. Arson and terrorism.

3. Fire science:
a. Fires develop when a combustible fuel comes in contact with an ignition source.
b. Ignition source can include radiant energy.
c. Ignition temperature.
d. Easier to control ignition sources.

4. Mitigation:
a. Understand how to prevent the ignition and spread of fires.
b. Bring buildings up to the latest fire codes.
c. Install fire extinguishers.
d. Conduct fire prevention inspections.
e. Maintain fire equipment.
f. Establish vegetation “clear zones.”
g. Ensure the address is clearly marked.
h. Work with the fire department to develop “pre-fire” plans.
i. Establish no-smoking policies.

5. Preparedness:
a. Establish a written fire prevention plan:
   i. List fire hazards, proper handling and storage procedures.
   ii. List potential ignition sources and their control procedures.
   iii. Include names of those responsible for maintenance of
iv. Identify responsibility for the control of accumulation of flammable or combustible materials.

v. Housekeeping procedures.

vi. Employee training.
   i. System maintenance procedures.
   b. Install automatic fire detection, suppression and warning systems.
   c. Establish guidelines and other written material for employees.
   d. Train employees in fire safety and evacuation.
   e. Shut off utilities, processes, and electronic systems.
   f. Place escape vehicles in position before evacuation is ordered.
   g. Ensure electrical systems are properly maintained.
   h. Inspect gas lines, furnaces, and boilers.
   i. Daily inspections.
   j. Control traffic and parking.
   k. Pre-register with restoration service companies.

6. Response:
   a. Obtain basic information about the fire.
   b. Ask if anyone is trapped or injured by the fire or smoke.
   c. Evacuate the immediate area.
   d. Call the fire department.
   e. Fight the fire, if qualified.
   f. Shut off heating, ventilation, and air conditioning systems.
g. Send people to meet the fire department.

h. Remove impediments to responding equipment.

i. Monitor the post indicator valve (PIV).

j. Assign a person to check or start the fire pump.

k. Decide whether equipment or processes should be shut down.

l. Move flammable or hazardous materials.

7. Recovery:

   a. Contact a restoration service.

   b. Prevent further damage.

   c. Restrict access to the damaged area.

   d. Contact insurance carrier or broker.

   e. Determine if production schedules are affected.

   f. Remove critical equipment or records not damaged.

   g. Recreate any lost vital records.

   h. Provide status reports to major customers and employees.

   i. Replenish used fire control equipment.

   j. Begin relocation and reconstruction.

K. Floods and Heavy Rain.

1. Second most common natural disaster.

2. Great loss of life.

3. Property damage exceeds $1 billion.

4. Can occur suddenly.
5. Tend to re-occur in same area.

6. Consequences and effects.

7. Flood maps and risk determination:
   a. 100-year flood.
   b. 500-year flood.
   c. Software.

8. Mitigation:
   a. Maintain a flood mitigation and response plan.
   b. Keep streams, culverts, and other waterways clean of debris.
   c. Install architectural barricades.
   d. Don’t develop or expand into flood prone areas.
   e. Ensure power shutdown authority and procedure.
   f. Fill underground tanks with water.
   g. Develop a plan to evacuate animals or equipment.
   h. Develop a contingency delivery plan.
   i. Consider the purchase of flood insurance.
   j. Build diversion channels, straighten river channels.
   k. Increase sewer and storm water capacity.

9. Preparedness:
   a. Know your flood risk.
   b. Install monitoring devices.
   c. Know the community alert signals.
   d. Review the contents of your community’s flood plan.
e. Pre-register with restoration service.

f. Be prepared for erosion or landslides.

g. Keep roof and parking lot drainage free of debris.

h. Inspect roofs for signs of potential weakness.

i. Remove any yard storage from low-lying areas.

j. Install check-valves in sewer traps.

k. Maintain an adequate supply of sandbags.

l. Maintain a supply of waterproofing materials.

m. Park vehicles on the escape side of bridges.

n. Keep vehicles fueled.

o. Monitor conditions:

1. Flood Watches (flooding is possible).

2. Flood Warnings (flooding is imminent or occurring).

p. Stockpile other materials.

q. Inspect fire protection equipment.

r. Sandbag protection equipment.

s. Move equipment and documents to upper levels.

t. Back-up data systems.

10. Response:

a. De-energize equipment.

b. Cover equipment and product.

c. Monitor conditions and escape routes.

d. Shut off electrical power and utilities.
Chapter 13: Response Planning

e. Immediately evacuate to higher ground.
f. Watch for and avoid low-lying areas.
g. Don’t attempt to cross flowing streams or to swim to safety.
h. Beware of snakes and other animals.

11. Recovery:
   a. Inspect foundations for damage.
   b. Assess damage.
   c. Contact the restoration service provider.
   d. Do not turn on utilities until checked.
   e. Be sure water supplies are safe to drink.
   f. Obtain permit for repairs and reconstruction.
   g. Retrofit structures during repair and reconstruction.
   h. Remove at-risk structures from the floodplain.
   i. Begin mitigation planning.
   j. Inform customers of the new location.
   k. Inform employees when they can expect to return.

   1. Hazardous material defined.
   2. Regulation.
   3. Mitigation:
      a. Construct dikes and secondary containment.
      b. Separate incompatible materials.
      c. Train staff in storage, use, hazards, and clean-up.
d. Minimize inventories.

e. Use less toxic alternate chemicals.

f. Store inside containment.

g. Properly mark, store, and remove in an expedient manner.

h. Use seismic shut-off switches.

i. Build dykes or diversion around drains.

4. Preparedness:

a. Identify materials and maintain material data safety sheets.

b. Determine what federal, state, and local regulations apply.

c. Work with local officials to coordinate pre-emergency plans.

d. Place equipment at strategic locations.

e. Maintain the proper equipment.

f. Install panic alarms and CCTV in hazardous areas.

g. Install wind socks and weather stations.

h. Conduct joint training drills.

i. Install a community warning system.

j. Inspect containers and piping for damage or leaks.

5. Response:

a. Evacuate upwind.

b. Isolate the area.

c. Decide need for outside assistance.

d. Wear protective equipment.

e. Remove injured.
Chapter 13: Response Planning

f. Apply first aid.
g. Identify the materials and their properties.
h. Eliminate ignition sources.
i. Stage fire control equipment.
j. Mitigate or eliminate the source.
k. Determine the size of the area affected.
l. Contain the spill.
m. Clean up.
n. Notify regulatory agencies.

6. Recovery:
a. Activate crisis management plan.
b. Decontaminate.
c. Repair damage.
d. File required reports.
e. Monitor health and environmental problems.
f. Investigate the cause.

M. Hurricanes.

1. Causes.

2. Effects and damage:
a. Saffir-Simpson Scale.
b. Wind.
c. Storm Surge.
d. Flooding from rain.
e. Tornadoes.

f. Loss of utilities.

g. Road blockage.

h. Other.

3. Watches and warnings.

4. Mitigation:

   a. Develop shutdown procedures.

   b. Keep trees in good health.

   c. Reduce the potential for wind-borne debris.

   d. Clean drains and catch basins.

   e. Upgrade existing structures.

   f. Incorporate high wind building standards for new construction.

   g. Avoid construction in areas subject to the greatest damage.

   h. Strengthen life lines.

   i. Set up alternate work sites and access to data systems.

5. Preparedness:

   a. Check flood insurance policies.

   b. Stockpile provisions and materials.

   c. Determine where to relocate.

   d. Inspect roof edging strips.

   e. Cover sensitive equipment.

   f. Train employees to prepare.

   g. Pre-qualify restoration and building contractors.
6. **Response:**
   
a. Monitor the progress of the storm.
   
b. Evacuate immediately.
   
c. Move valuables out of the area.
   
d. Secure or store located objects outside.
   
e. Board up windows.
   
f. Turn off utilities and HVAC.
   
g. Arrange for extra security.
   
h. If required to remain, stay inside.

7. **Recovery:**
   
a. Wait before beginning repairs and restoration.
   
b. Evaluate the structural integrity of the building and utilities.
   
c. Ensure that the site is safe for cleanup.
   
d. Account for employees as they return.
   
e. Begin relocation and reconstruction.
   
f. Return vital records.

N. **Serious Injury or Illness.**
   
1. Most common emergency.
   
2. Lost productivity.
   
3. Response is very visible.
   
4. Services not available after disasters.
   
5. Training
   
6. Mitigation
a. Implement effective safety programs.
b. Evaluate the risk and type of injuries.
c. Develop prevention programs.
d. List response procedures.
e. Purchase biohazard cleanup kits.
f. Ensure the address is clearly visible.
g. Sponsor health fairs.

7. Preparedness:

a. Install eye wash stations and showers.
b. Inoculate employees at risk.
c. Track employees with special needs.
d. Train employees in first aid and cardiopulmonary resuscitation.
e. Purchase automated external defibrillators (AEDs).
f. Maintain first aid supplies at strategic locations.
g. Ensure emergency vehicles have access to the facility.

8. Response:

a. Contact emergency services.
b. Determine the extent of the injuries.
c. Provide first aid.
d. Ensure that the victim is not moved.
e. Obtain information about the victim’s condition.
f. Keep those not involved in the emergency away.
g. Escort paramedics to the victim.
h. Hold elevators at the ground floor.

9. Recovery:
   a. Follow biohazard procedures.
   b. Notify regulatory agencies.
   c. Investigate the cause.
   d. Retrain injured employees on safety procedures.
   e. Activate the crisis management plan.
   f. Provide posttraumatic stress counseling.

O. Lightning.

1. Causes.

2. Characteristics.


4. Effects.

5. Mitigation:
   a. Understand the frequency of severe thunderstorms.
   b. Engineering evaluation.
   c. Incorporate lightning protection in structures.
   d. Purchase a backup generator.
   e. Upgrade fire protections systems.
   f. Establish equipment replacement agreements.

6. Preparedness:
   a. Monitor the storm intensity.
b. Install line conditioners.
c. Discontinue outdoor activities.
d. Avoid contact with objects.
e. Train employees about lightning safety.
f. Maintain scheduled backups data systems.
g. Shut down systems.

7. Response:
a. Bring employees inside the building.
b. Contact emergency services if injuries.
c. Treat injured victims.
d. Stand clear of windows, doors and electrical appliances.
e. Avoid contact with piping.
f. Avoid the use of the telephone.
g. Check for and extinguish fires.
h. If power is lost, shut down equipment.

8. Recovery:
a. Log all events, actions, decisions, and expenses.
b. Assess and document damage.
c. Reestablish utilities.
d. Test and replace damaged equipment and connectivity.
e. Restore data if any is lost.

P. Tornadoes.
1. Formation.
Chapter 13: Response Planning

2. Characteristics:
   a. Funnel cloud.
   b. Water spout.

3. Time and locations.


5. Effects.

6. Watches and warnings.

7. Mitigation:
   a. Make trees wind-resistant.
   b. Strengthen the wind resistance of buildings.
   c. Establish tornado warning systems.
   d. Build safe rooms or tornado shelters.

8. Preparedness:
   a. Monitor weather stations.
   b. Learn what tornado conditions look and sound like.
   c. Know the meaning of watches and warnings.
   d. Identify a shelter room.
   e. Instruct employees in local warning systems.
   f. Construct storm shelters if none are close by.
   g. Maintain supplies of food, water, and emergency lighting.
   h. Keep plastic sheeting and other materials on hand.

9. Response:
   a. Seek shelter in a storm cellar, basement, or interior room.
b. Use interior room, hallway, or interior stairwell (high rise).

c. Stay clear of windows, doors, and outside walls.

d. If outside, seek a safe place in a sturdy building.

e. If in a vehicle, seek shelter in a ditch.

f. Leave mobile homes for a storm shelter.

10. Recovery:

a. Assess damage to facilities.

b. Begin search and rescue operations.

c. Treat injuries.

d. Avoid the use of open flames.

e. Monitor news broadcasts.

f. Form teams of volunteers.

g. Document damage for insurance reimbursement.

h. Clear debris.

i. Begin relocation and reconstruction.

Q. Workplace Violence and Civil Disturbance.

1. Effects.

2. Definition:

a. Classifications.

3. Mitigation:

a. Observe good hiring practices.

b. Establish policy.
c. Foster a good working environment.
d. Never degrade an employee when terminating.
e. Audit and improve physical security and access control.
f. Remove objects used by demonstrators to damage property.
g. Construct ‘safe rooms.’
a. Isolate lobbies.

4. Preparedness:

a. Develop a comprehensive program.
b. Train supervisory and management to:
   i. Recognize potentially aggressive behavior.
   ii. Recognize signs of domestic violence.
   iii. Diffuse aggressive behavior.
   iv. Respond immediately to complaints.
   v. Other elements required by the Occupational Safety and Health Administration.
c. Protect potential victims.
d. Evaluate and manage threats or acts of violence.
e. Train security officers.
f. Develop intelligence programs.

5. Response:

a. Type I:
   i. Follow the robber’s directions.
   ii. Do not argue or fight with the robber.
iii. Offer no resistance whatsoever.
iv. Speak to the robber in a cooperative tone.
v. Let them know you intend to follow their instructions.
vi. Never use a weapon.
vii. Move slowly and explain each move.
viii. Do not follow or chase the robber.
ix. Do not touch anything robber has handled.
x. Close and lock all doors.
xi. Call the police immediately.

b. Type III:
i. Assess the situation.
ii. Isolate potential victims.
iii. Lock all doors.
iv. Close blinds.
v. Take cover.
vi. Summon help.
vii. Warn other employees.
viii. Notify appropriate managers.
ix. Account for employees.
x. Do not interact with participants in a disturbance.

6. Recovery:
a. Activate the crisis management plan.
b. Clean up biohazards and physical damage.
c. Provide stress counseling.
d. Review security and response procedures.
Sample Test Questions

True or False

116. A disadvantage to the Incident Command System is that all sections must be activated to be used effectively. Answer: F (p. 125)

117. The role of Incident Commander may be filled by the first person to arrive at the scene of an Emergency. Answer: T (p. 126)

118. A governmental Emergency Operations Center (EOC) is more resource-based, whereas a business EOC tends to be more strategic. Answer: T (p. 129)

119. The formation of an Emergency Response Team is important because after a disaster, businesses may not be able to rely on the response from governmental services. Answer: T (p. 131)

120. All good response plans will remind employees not to panic during an emergency or disaster. Answer: F (p. 133)

121. VBIED is an acronym for ‘Very Big Improvised Explosive Device.’ Answer: F (p. 133)
122. Bombings are no longer expected to be a primary tool of terrorists. *Answer: F* (p. 133)

123. The building should be evacuated after a bomb threat. *Answer: F* (p. 135)

124. If a suspicious object is found after a bomb threat, you should try to find its owner. *Answer: T* (p. 136)

125. Fires account for a major portion of flood damage. *Answer: T* (p. 158)

126. The lack of potable drinking water can result from flooding. *Answer: T* (p. 158)

127. During a hazardous material incident where a ‘Shelter in Place’ order has been issued, you should turn off HVAC or heating systems. *Answer: T* (p. 164)

128. A Tornado Warning is issued when severe thunderstorms and/or tornadoes are most likely to occur and when conditions are favorable for their formation. *Answer: F* (p. 172)

129. Violence is the leading cause of death to women and the second cause of death to men in the workplace. *Answer: T* (p. 175)
130. A good example of Type I workplace violence is an injury to a gas station
attendant resulting from a robbery.  Answer:  T  (p. 175)

Multiple Choice

46. Two of the five sections of the Incident Command System are:  Answer:  d  (p. 125)

a. Command and Control.
b. Finance and Purchasing.
c. Emergency Operations Center and Response.
d. Planning and Intelligence.

47. A function of the Operations Section under ICS is:  Answer:  a  (p. 127)

a. Implement action plans and objectives.
b. Project or predict changing conditions.
c. Develop action plans.
d. Obtain all resources and services.

48. The Emergency Operations Center:  Answer:  d  (p. 129)

li. Coordinates response or recovery.
mm. Collects and manages information.
nn. Creates or refines policy.
oo. All of the above.

49. The Emergency Operations Center:  **Answer: b (p. 130)**

a. Is collocated with the field Incident Commander.

b. Should have strong access controls.

c. Should not be designed for continuous use.

d. Cannot use the Incident Command System.

50. Under Unified Command:  **Answer: a (p. 129)**

a. Resources but not objectives are generally shared.

b. Used when the Operations Section Chief needs command power.

c. Applied when the Incident Command System is impractical.

d. Means that all responders follow the same commander.

51. An Emergency Response Team:  **Answer: d (p. 131)**

a. Can reduce injury and loss.

b. Prevent adverse publicity.

c. Demonstrate management concern.

d. All of the above.
52. In the United States, most bomb threats:  \textit{Answer: a}  \hspace{5mm} (p. 134)

a. Are generally false.

b. Should not result in a search.

c. Should always result in an evacuation.

d. Involve highly technical skills and training to detect a device.

53. In the United States, which is the leading motivation of bombings?  \textit{Answer: a}  \hspace{5mm} (p. 133)

a. Vandalism.

b. Terrorism.

c. Extortion.

d. Labor disputes.

54. What should you depend on the least when searching for a bomb?  \textit{Answer: c}  \hspace{5mm} (p. 134)

a. Radios and cell phones.

b. Dogs.

c. Police officers.

d. Department managers.

55. Suicide bombers:  \textit{Answer: b}  \hspace{5mm} (p. 137)
a. Are always young or middle-aged males.

b. Potentially appear nervous.

c. Always look ‘underdressed’ for the weather.

d. Appear to be from the Middle East.

56. Which is true about a Radiological Dispersal Device?  \textit{Answer: c (p. 138)}

a. They can cause an atomic explosion.

b. An entire city could become contaminated for years.

c. They are primarily designed for fear and intimidation.

d. Its effects are effectively countered by taking Potassium Iodide.

57. Which is a good clue that a biological agent has been unleashed?  \textit{Answer: b (p. 146)}

a. A known terrorist group takes credit.

b. Unusual increase in the absentee rate.

b. Immediately feeling sick after an unusual event.

d. Water and food taste different.

58. During an earthquake, it is best to:  \textit{Answer: a (p. 144)}

a. ‘Duck, Cover and Hold.’

b. Get outside as soon as possible.
c. Find safety under an overpass.

d. Use the telephone to call for help.

59. On a global basis, more lives are lost through: Answer: b (p. 158)

q. Earthquakes.
r. Floods.
s. Hurricanes.
t. Fires.

60. What is term that is used to measure the amount of lightning activity an area receives?

   Answer: a (p. 170)

17. Flash Density.
18. Strike Index.
19. Static Load Index.
20. Fujita Scale.

Short answer:

1. List the five major functional areas of the Incident Command system.

   Answer: Command, Operations, Planning and Intelligence, Logistics, Finance and Administration.

   (p. 125)
2. List five major duties of the Incident Commander.

*Answer:* Field management of the emergency, coordination with the EOC or other IC’s, ultimate responsibility for safety of responders, approval of all plans and resources, setting objectives and priorities, delegating authority as necessary, primary responder until others arrive.

(p. 126)

3. List five ways to prevent and prepare for the effects of a flood.

*Answer:* Know your flood risk, keep creeks and drainage systems free from debris, be prepared for erosion or landslides, inspect roof for potential weakness, remove yard storage in low lying areas, anchor equipment that may float away, install check valves in sewer traps, maintain supply of sandbags and water proofing materials, park vehicles on escape side of bridges, monitor conditions, stockpile provisions and other materials, inspect and protect fire equipment, move equipment, documents to upper levels, backup data systems.

(p. 159)

4. What is the most common type of emergency in business?
Answer: Injury and illness.

(p. 168)

5. List five considerations in the design of an Emergency Operations Center.

Answer: Must anticipate the complexity of its response and recovery, must facilitate the flow of information internally and externally, should be located in a secure, structurally safe building, centrally located, easily accessible, access control, connected to a back-up power generator, must be ‘user friendly,’ designed to operate continuously, keep operations as quiet as possible, video conferencing capability.

(p. 129)

6. Contrast the operations and objectives of a governmental and business Emergency Operations Center.

Answer: Often the differences in the operations and objectives of a governmental vs. a business EOC is one of scale. Since the governmental EOC will deal with the response to larger or more widespread events and consequently will have more decision making in the field, they are more geared toward resource allocation.
A governmental EOC is usually located in a dedicated cold complex fully equipped with electronic displays with theater-type seating and separate workstations for participants. There are separate and adjoining meeting rooms for the different ICS sections to meet in addition to a soundproofed radio and communications room, rest and food areas. While you can find this arrangement in business, it is typically not the case. A business EOC is often a conference room or facility used for other purposes when not required for emergency operations. Trailers or hotel conference rooms/suites are also used for business EOCs.

Both centralize control of response and recovery when multiple units are involved, they both collect and disseminate information, both should be user friendly, support multi shift operations, and provide for noise control. Most governmental EOCs are now organized under the Incident Command System; most businesses are not.

(p. 129)

7. Write a justification to management for the formation of an Emergency Response Team at a low to medium risk facility. Include elements required to develop the program.

*Answer:* Each day we are exposed to the effects of earthquakes, fires, floods, serious injury, and other emergencies that have the potential cause serious and lasting adverse effects to our facilities, operations, good image, and the safety and well being of our
employees. Subsequent to a regional disaster, governmental emergency services (police, fire, ambulance and other medical services) will most likely not be available to us. The formation of a voluntary employee emergency response team to respond to and control emergency before the arrival of public agencies will help to reduce the consequences from the above risks. It will also:

- Intervene and stabilize emergencies with less delay;
- Reduce injuries and loss;
- Prevent adverse publicity;
- Demonstrate management concern and support for the safety of employees;
- Minimize the impact on the environment;
- Help comply with regulatory requirements to mitigate hazardous materials incidents (Fed OSHA, Cal OSHA, Uniform Fire Code, Environmental Protection Agency);
- Become the sole response in a disaster situation when public agencies do not have the ability to respond.

The team would consist of volunteer employees on all shifts and will respond to all emergencies at a basic level of training that include incipient fire response, advanced first, simple chemical spill cleanup and evacuation management. Team members must have the complete support of management for time away from their duties to participate in initial training, on-going training, and meetings and monthly drills.
We intend to organize the team under the Incident Command System that will place the entire tactical direction of emergency operations under the control of a single team member. For the team to operate effectively, management must delegate all operational authority to this individual. Response plans; policies and procedures are developed ahead of time and are subject to your approval.

In addition to the commitment of time, management must approve certain capital and expense budget items to cover start-up costs including radios, vests, recruitment, and other necessary supplies and equipment.

(p. 131)


*Answer*: Jesse Owens, security manager, is designated as the evacuation plan coordinator with Ima Outtahere as his alternate. The coordinator is responsible for the maintenance of this plan and for the training of all personnel in the identification of alarms and evacuation routes. They will ensure that unobstructed escape routes comply with local regulation and to not lead to or through hazardous areas.

Our emergency escape procedures and assignments are designed to respond to many potential emergencies, including:

- Earthquake
• Fire
• Flood
• Civil disorder
• Workplace violence

Floor plans and maps are available and posted at all times to provide guidance in an emergency.

**No Employee is permitted to re-enter the building until advised by Security (after determination has been made that such re-entry is safe).**

No employees are required to remain behind during evacuation to care for critical plant operations.

**Evacuation Wardens are assigned to all floors according to the building management’s plan. Before leaving, these Wardens check rooms and other enclosed spaces in the workplace for employees who may be trapped or otherwise unable to evacuate the area. The wardens will assist with the disabled as required and will ensure that all persons have evacuated.**
Evacuation Guidelines

1. Know the evacuation signal and the evacuation routes for the building. The signal is a loud horn, flashing lights, and loudspeaker announcements.

2. Upon hearing the evacuation signal, immediately evacuate the building. Do not take time to gather any personal belongings, to go back to your office, to finish phone calls, etc.

3. Shut down only those pieces of equipment/machinery that are absolutely essential to be shut down.

4. Evacuate the building using approved evacuation routes.

5. Do not use elevators.

6. Assist others who may need help evacuating (assign evacuation buddies or floor wardens).

7. Go directly to the designated evacuation area (assembly point) and remain there. Do not leave or go back into the building until directed to do so by Security.
8. Account for all individuals (poll floor wardens) and report to the fire or police department if any are missing.

(p. 150)

9. Describe your response to the following situation: A tanker truck crashes just outside your facility and starts to leak a substance that is forming a vapor cloud and the wind is blowing toward one of your buildings. Evacuations have began in the building next to the one affected by the vapor cloud and one of the evacuees has fallen down the stairs and broken his leg. You have a fully trained and equipped Emergency Response Team.

*Answer: Note: The following sample responses are from the text. Other appropriate responses should be acceptable:*

i. **Activate the Emergency Response Team and establish the Incident Command System.** Receive transfer of command if you are not the first responder and someone else has assumed the role of Incident Commander.

ii. **Confirm that emergency services (Fire Department) have been notified and that they are responding a hazardous materials unit.** Request or confirm that an ambulance crew is responding for the broken leg.

iii. **Issue order or approve recommendation from the planning section for operations to issue a Shelter in Place order at the building affected by the vapor cloud.**
iv. Ensure evacuated personnel are sufficiently protected by distance and wind direction from vapor.

v. Receive reports from floor wardens that all have evacuated.

vi. Expand Operations Section into Hazmat and Medical Teams. Establish position of Safety Officer.

vii. Establish and agree on response objectives for each team.

viii. Set up Unified Command with Fire Department IC for Hazmat.

ix. Ensure the Operations Chief has done the following:

x. HazMat Team:

1. Isolate the area and deny access to any unauthorized personnel.

2. Any team members near the spill are wearing the highest level of protective equipment required.

3. Identify the materials, their properties and hazards (this may be a function of the Unified Command).

4. Eliminate ignition sources if a flammable liquid or explosive gas is involved. Stage fire control equipment at appropriate locations (Logistics Section).

5. Determine the size of the area affected and whether additional evacuations are warranted.

6. Do not let material go down a drain, into a waterway, basement, or confined space.

7. Decontaminate responders, facilities, and equipment if necessary.

8. Medical Team:
9. Dispatch personnel to meet and route the ambulance to approach the scene downwind of the vapor cloud.

10. Ensure that the victim is not moved (unless to protect from further hazard)

11. Obtain as much information about the victim’s condition, history, and needs as required

12. Keep those not involved in the emergency away from the area (should have already evacuated).

xi. Monitor progress and information relative to the Fire Department’s cleanup of the spill.

xii. Issue all clear when situation is stabilized and employees can return to the building and end Shelter in Place restrictions.

xiii. Possibly have the Finance and Administration section complete reports and determine cost of incident from lost productivity.

(Chapter 13)


*Answer:* Before September 11, 2001, much attention to emergency response was geared toward handling first aid issues or to putting simple plans in place to meet regulatory requirements. Today, much attention is focused outside the organization
to prepare for and to respond to incidents that are terrorist in nature. A good deal of concentration and resources are directed toward ‘first responders.’

Businesses are now incorporating measures to mitigate against explosive devices, or against the possibility of an aerosol introduced into their ventilation system. Many emergency response plans now include instructions to ‘shelter-in-place.’ Organizations that did not understand today’s risks and that did not incorporate these new threats into their plan were some of the many who succumbed to the intent of terrorists to cause fear and overreaction.

The United States has established The National Response Plan, or NRP, that specifies how the resources of the Federal Government will work in concert with state, local, tribal governments and the private sector to respond to ‘Incidents of National Significance.’ Its purpose is to establish a comprehensive, national, all-hazards approach to domestic incident management across a spectrum of activities including prevention, preparedness, response, and recovery. The NRP is predicated on the National Incident Management System, or NIMS. NIMS consists mainly of a Management System (the Incident Command System), Preparedness (planning, training, exercising, certification, equipment acquisition and publications management), Communications and Information Management, and Supporting Technologies. Together the NRP and the NIMS provide a nationwide template for
working together to prevent or respond to threats and incidents regardless of cause, size, or complexity.

(Chapter 13)

Case Study:

One of your switchboard operators comes to you and says that she just received a call on an outside line by someone who sounded very nervous and very young who said, ‘I have placed a destructive device behind the Building A Northwest Chlorine tank. It is in a brown briefcase and is equipped with a motion detector that will cause a detonation if anybody comes within 20 feet. It is hidden so you can’t see it from the outside. Only I have the capability to disable it. You will deliver $1,000,000.00 to the corner of First and Vine Streets within the next 6 hours. You need to get people out of the area immediately. If I see any cops, I will cause it to explode.’ The receptionist said that she started to ask the questions on her bomb threat questionnaire, but the caller said that he ‘would rather not answer them.’ She also said that she could hear a lot of noise in the background that could have been a party, but was not sure. The call was received just before quitting time and the company is not involved in any controversial products or labor disputes. You are in the process or replacing your contract guard force because of their failure to enforce access controls. You need to decide if the threat is credible and to justify your decision.

Answer: The threat is credible. The fact that the caller had knowledge of the layout of the facility and its processes, took the time to describe the device, used terminology that
indicates a familiarity with bomb making, and has a motivation, indicate credibility.

Additionally, most credible bombers will remain on the call for a relatively longer time (there is a lot of detail in the message) to ensure their message is understood. The caller gave the exact location of the device and it was placed at a time that would minimize injuries (quitting time) if detonated. Poor access control allows for the possibility of someone entering the facility to place the device. There also seems to be some thought process in allowing time to gather the money (although practically speaking, not enough time).

The fact that the caller seemed young is inconclusive and that there may have been a party going on at the source of the call is also immaterial since the receptionist did not indicate that the caller seemed jovial or intoxicated.

(Ch. 13)
Chapter 14: Business Continuity Planning

Learning Objectives

- How the process is defined.
- Justifications for Business Continuity Planning.
- BCP project management.
- Planning methodology.
- Basic strategies.

Presentation Outline

I. Introduction
   A. Business continuity defined.
   B. Distinction between DRP and BCP.
   C. Distinction between a plan and planning.
   D. Importance of the planning process.
   E. Increasing security responsibility.
II. Why Plan?

A. Regulatory requirement.
B. Cost of downtime.
C. Competitive advantage.
D. Retain key employees.
E. Customer requirement.
F. Stockholder liability.
G. Other justifications.

III. Planning Process

A. Initial Steps:
   1. Identify physical or procedural hazards (mitigation).
   2. Prepare to respond to the disaster:
      a. Protect the health and safety of employees.
      b. Minimize damage to the organization.

B. High level BCP planning process:
   1. Identify critical functions.
   2. Rank functions according to their value to the organization.
   4. Develop plan to implement the strategies.

C. Project Management:
1. Consequences and advantages.
2. Process not considered a ‘project.’

D. Planning Steps (overview):
1. Identify the planning coordinator.
2. Obtain management support and resources.
3. Define the scope and planning methodology.
5. Conduct a Business Impact Analysis.
6. Identify critical functions.
7. Develop recovery strategies.
8. Set up recovery teams.
9. Develop team recovery instructions.
10. Collect resource information.
12. Train recovery teams.
13. Exercise the plan.
14. Maintain the plan.

E. Identify the Planning Coordinator:
1. Responsible for project management.
3. Good understanding of the organization.
4. Detail-oriented.
5. May eventually be recovery coordinator.
F. Obtain management support/resources:
   1. Need for management support.
   2. Support communicated to all levels.
   3. Include BCP in goals and objectives.

G. Define scope:
   1. Keep scope narrow.
   2. Starting point dependent on degree of risk.

H. Planning Methodologies:
   1. Publish Planning Standards:
      a. Best when many locations or divisions.
      b. Distribute guidelines, methods and templates.
      c. Training necessary.
      d. Progress monitored.
      e. ‘Basic Plan’ developed at higher level.
   2. Planning or steering committee:
      a. Company or division senior managers.
      b. Advantages.
      c. Disadvantages.
   3. Internal Development:
      a. Facilitation role.
      b. Advantages.
      c. Consultants.
   3. Template plans.
4. Select participants:
   a. Schedule interviews.
   b. Discussion points.
   c. Distribute introductory materials.

I. Conduct risk identification inspections:
   1. Advantages.
   2. What to look for, questions to ask.
   3. Mitigation.

J. Complete Business Impact Analysis.

K. Identify critical functions:
   1. Defined.
   2. Reasons for prioritization.

L. Develop recovery strategies.
   1. Selected by:
      a. Cost-benefit.
      b. Technical feasibility.
      c. BIA.
      d. Recovery Time Objectives.
      e. Strategic vision.
   2. High level for IT and work space.
   4. High availability.
   5. Short- and long-term.
6. Can be reliably implemented.

7. Determine existing strategies.

8. Hot/Cold/Warm Sites:
   a. **Defined.**
   b. **Disadvantages and fees.**
   c. **Planning.**
   d. **Internal hot sites.**

9. Relocation.

10. Work at home.

11. Redundant telecommunications:
    a. Voice and data.
    b. Service and replacement agreements.
    c. Bypass circuits and fax lines.
    d. Divergent routing.
    e. Cellular backup.
    f. Satellite systems.
    g. Hot/cold sites.
    h. Radio systems.
    i. Third-party call centers.

12. Third-party manufacturing.

13. Product from competitors.

14. Underutilized or other data systems.

15. Revert to manual methods:
a. Becoming more difficult due to technology.

b. May need to redevelop.


17. Workforce management.

18. Reciprocal agreements.

19. Equipment rental.

20. Reschedule production.

21. Reallocate resources.

22. Service level or quick ship agreements.

M. Set up recovery teams:

1. Single vs. functional teams.

2. Team leader and alternate:

   a. Duties and responsibilities.

3. Corporate team and responsibilities.

4. Site management team.

5. Continuity Coordinator (Incident Commander).

6. Team members.

N. Develop instructions, resource information and document the plan.

O. Train recovery teams.

P. Exercise the plan.

1. Exercises will:

   a. Validate the effectiveness of strategies.

   b. Ensure the accuracy of information.
c. Increase the preparedness of the team.

d. Reveal gaps in instructions.

e. Identify misplaced or absent assumptions.

2. Proper nomenclature.

3. Must be well-planned.

4. Positive and progressive.

5. Tabletop Exercise:

   a. Discussion based on a scenario.

   b. Responsibilities of a controller.

   c. Note taker.

   d. Scenarios are believable, realistic, relevant.

   e. Single or multiple teams.

6. Call Tree Exercise.

7. Relocation Exercise.


9. Full Scale Exercise.

10. Exercise management and objectives.

Q. Plan Maintenance.
Sample Test Questions

**True or False**

131. Business continuity planning and disaster recovery planning mean exactly the same thing. *Answer: F* (p. 179)

132. Response planning is another term for business continuity planning. *Answer: F* (p. 181)

133. Recovery strategies are agreed upon first before the identification of critical business functions. *Answer: F* (p. 181)

134. Project management skills are not required in business continuity planning, as BCP is not a ‘project.’ *Answer: F* (p. 182)

135. When defining the scope of the project, the selection of a starting point may be dependent upon the degree of risk. *Answer: T* (p. 183)

6. The template plans, when developed by experts, provide the most complete and effective response to a disaster. *Answer: F* (p. 185)

7. An advantage to the recovery team methodology is the ability to respond to both large and limited scale disasters. *Answer: T* (p. 193)
8. The management team should not have an alternate leader.  *Answer: F* (p. 193)

9. Temporarily purchasing materials or product from a competitor is a recovery strategy that will inevitably cause the failure of the business.  *Answer: F* (p. 191)

10. High-availability solutions are devised for processes with low outage tolerance.  *Answer: T* (p. 188)

**Multiple Choice**


   a. Is designed for a worst-case scenario.
   b. Should include a level of detail found in systems or equipment operations manuals.
   c. Should not be modified in any way by the people tasked with its implementation after a disaster.
   d. All of the above.

62. Two goals of response planning are:  *Answer: a* (p. 181)

   a. Protect the safety of employees and minimize damage.
b. Develop and implement strategies to recover operations.

c. Respond to the disaster and recover operations.

d. Prepare employees for disasters and train them to respond to emergencies.

63. The Planning Coordinator:  \textit{Answer: d (p. 183)}

\begin{itemize}
\item pp. Should be a member of management.
\item qq. Should be detail oriented.
\item rr. May become the recovery coordinator.
\item ss. All of the above.
\end{itemize}

64. Publishing planning standards:  \textit{Answer: b (p. 184)}

\begin{itemize}
\item a. Requires no additional training.
\item b. Works well when there are many locations or divisions.
\item c. Removes the flexibility to adapt plans post-disaster.
\item d. Eliminates the need for a steering committee.
\end{itemize}

65. A steering committee:  \textit{Answer: d (p. 184)}

\begin{itemize}
\item a. Is suggested in some regulations.
\item b. Consists of a group of senior managers.
\item c. Can become too bureaucratic.
\end{itemize}
66. It is acceptable to: \textit{Answer: d (p. 187)}

\begin{enumerate}
\item Implement the most effective recovery regardless of cost.
\item Not consider existing strategies.
\item Attempt to move all business functions into a hot or cold site.
\item Have both company global and separate business unit recovery strategies.
\end{enumerate}

67. What is the primary strategy organizations use to protect the integrity and recoverability of their data? \textit{Answer: c (p. 198)}

\begin{enumerate}
\item Subscription to external hot site.
\item Internal hot site.
\item Data backups.
\item Load balancing.
\end{enumerate}

68. The management or corporate recovery team is primarily tasked with: \textit{Answer: a. (p. 193)}

\begin{enumerate}
\item Making strategic decisions.
\item Making tactical decisions.
\item Notification of response team members.
\end{enumerate}
d. Updating team plans.

69. The Business Recovery Coordinator:  \textit{Answer: d} \hspace{1em} (p. 193)

a. Has overall responsibility.

b. Acts as liaison between team leaders.

c. Can activate teams as necessary.

d. All of the above.

70. The important qualities of a team leader include:  \textit{Answer: d} \hspace{1em} (p. 195)

a. Ability to take charge.

b. Familiarity with team’s function.

c. Have no other duties that interrupt focus.

d. All of the above.

71. Duties of a team leader should include:  \textit{Answer: a} \hspace{1em} (p. 195)

a. Planning activation and notification of team members.

b. Tracking the post disaster financial health of the company.

c. Acting as alternate to the Recovery Coordinator.

d. Strategic decision-making.
72. Impacts that define a critical function include: \textit{Answer: d} (p. 187)

- a. Its loss would affect the financial position of the company.
- b. Have a regulatory effect.
- c. Would reduce or destroy public/customer image/confidence or sales. All of the above.

\textbf{Short Answer}


\textit{Answer:} Business continuity planning is a process that identifies the critical 
functions of an organization, develops strategies to minimize the effects of an outage 
or loss of service provided by these functions. (p. 179)

11. List five reasons or justifications for Business Continuity Planning.

\textit{Answer:} Without continuity planning, the organization may lose its competitive 
advantage, valuable employees, and future research. Organizations cannot insure 
against lost customers or a diminished public (customer) image. History consistently 
shows that between 35 to 50 percent of businesses never recover after major 
disasters. Other rationales for continuity planning include:

- Requirement by financial auditors
- Prevent the loss of market share
- Capitalize on the lack of planning by the competition
- Fiscal responsibility
- Stockholder liability
- Regulatory requirement
- Retain key employees
- Prevent the loss of research
- Help ensure the safety of employees
- Preserve customer confidence
- Assist in the overall economic recovery of the community
- Assists in a quick and orderly recovery after a disaster
- Minimize the economic loss (devaluation) to the firm.

(p. 180)

12. A medium-sized manufacturing company owns locations in three States. Their computer system is distributed throughout these locations with excess capacity and floor space at the farthest location. The company has an outage tolerance or recovery time objective of 7 days. They expect no changes to this configuration for at least 5 years. Recommend the most appropriate recovery strategies.

Answer should include at least the following, but not those included in question #4:

- Implement data policy and procedures;
- Source new facilities or bring in restoration services company to repair the damaged facility;
- Use manual methods until data systems are restored (not appropriate for high technology);
- Install UPS systems on critical equipment;
- Enter into service level (replacement) agreements;
- Lower level of communications redundancy;
- Nightly incremental data backup of the server with full weekly backup, and offsite storage of the data;
- Use excess computer capacity at out of state location as the data recovery strategy;
- Use excess workspace capacity at out of state location;
- If production levels cannot be maintained at an acceptable level, consider extra shifts, third party manufacturing, or re-label of competitor’s product.
- Implement a vital records management program and store them off site;
- Develop plans to return to the refurbished site or to a new facility.

(p. 188)

13. How would your recommendations change in the above situation if the recovery time objective is 24 hours? Less than 24 hours?

Answer:
- A higher degree of mitigation (backup generators, telecommunications redundancy, require sole source suppliers to have continuity plans, etc.);
- Consider a subscription to a hot site vendor.
- If less than 24 hours, consider a second data center (mirrored, internal hot site) or other high availability solution if the results of the Business Impact Analysis justifies the cost.

(p. 188)

14. The text outlined steps required to produce an effective plan. Differentiate which of these steps are sequential and why others can be performed concurrently or in a different order.

*Answer:* The identification of the recovery coordinator can occur before or after obtaining management support and resources because either management will initiate the planning process or the planning coordinator will need to obtain the support of management if the project was initiated at a lower level. The scope and planning methodology should follow these steps as they define the remainder of the process. The risk identification and mitigation inspections can be conducted somewhat concurrently with the business impact analysis, or soon after, but the results of both should be included in the business impact analysis report. Conducting the risk identification step after the BIA may necessitate additional
meetings with individuals if additional information or answers to questions are required. A primary purpose of the BIA is to identify critical functions and to cost justify recovery strategies, so this step precedes these elements. Teams can be set up before recovery strategies are developed because the teams are usually formed along the lines of the critical functions (but not always); however, the scripting of team instructions and the collection of most of the resource information should not occur until the strategies are finalized (employee contact information can be collected when the teams are formed, but in practice, the collection of all resource information is often collected in, or just after the BIA). Once this information is collected and the strategies finalized, the team plans can be documented. Non-specific or general portions of the plan can be developed at any point in the process. Once the plans are documented, employees and team members are trained (one could argue that orientation and training for some takes place earlier in the process, such as educating management to the need for the plan, talking participants through the process in the BIA interviews, etc.). Exercising of the plans should follow and maintenance of the plan is usually considered the last and on-going step, but in practice the plan will undergo updating and correcting before it is ‘finalized.’

(Chapter 14)

15. Planning standards can be used for large organizations to effect a more rapid completion of the planning process. Develop instructions to a subordinate advising him or her to avoid certain pitfalls in this planning method.
Answer: Use great caution when using templates or the basic plan; the participants need to adapt them to local conditions and needs and complete the “thought process” necessary to provide the training needed to execute the plan effectively after a disaster. We must still train these persons in the expectations of the project, monitor their progress, and help to implement the plans. Each unit or recovery team must “own” its portion of the plan and become familiar with its contents.

(p. 185)

16. You are a low-level risk management employee who has been assigned the task of developing a business continuity plan. Should you establish a steering committee? Justify your answer.

Answer: Yes. Steering committees work best when the organization or planner has little knowledge of continuity planning principles and strategies or cannot gain an understanding of the operation or needs of the business unit. Since the steering committee is composed of the company’s or division’s top managers, they can better discuss business impacts and select strategies, and they can assign the documentation of the plan to individual functional managers.

(p. 184)
17. List five duties of the corporate or management team.

*Answer:*

- Ensuring the safety of all personnel;
- Making strategic business decisions;
- Directing the recovery process on a regional basis;
- Assisting the site disaster recovery management team to decide if an alternative work site is required;
- Projecting and tracking the financial impact of the disaster;
- Determining the need to review the strategic position of the company based on any change or expected change in financial position, production capacity, corporate image, or sales;
- Working with the public relations director to develop messages and positions, and communicating the necessary management decisions to the public relations;
- Resolving conflicts with the allocation of resource requirements between multiple sites affected by the disaster;
- Ensuring insurance claims are filed in a timely manner;
- Monitoring the recovery operations and recovery expenses;
- Keeping the Board of Directors updated on the position of the company and on the progress of the recovery operations;
- Monitoring and assisting the site disaster recovery management teams, local recovery coordinators, or facilities teams with building restoration, relocation,
and the acquisition of temporary or permanent replacement facilities.

(p. 193)

18. Distinguish a good potential team leader from one that may be a poor selection.

Answer: A good team leader has the ability to oversee the implementation of their teams’ recovery instructions and can take charge in an emergency situation, has familiarity with the operations of the functions to be restored (the duties imposed on the team members by the recovery instructions must closely match their normal skills and scopes of responsibility), and freedom from other significant recovery (or other) duties that may interrupt focus. If team leaders are to perform special functions outside their normal duties, they should have the ability to receive and understand training in these new skills beforehand. For political reasons, the department manager is most often selected as the team leader, but may not always be the best choice unless they match the above criteria. They must have the ability to travel to a hot site or alternate location [this is not specifically mentioned in the text. In practice, only about 20 percent of team members are able to show up at an alternate location if it is some distance from their homes, as is often the case when using a hot site recovery strategy].

(p. 195)
10. Discuss the rationale of using a high-availability solution.

*Answer:* The BIA may indicate that certain business processes cannot be out of service for more than 1 hour (or less) with very little data loss (recovery point objective), but other computer applications can disappear for 1 or 2 days without serious consequence. In this case, a high-availability solution is devised for the processes with low outage tolerance (high RTO); for example, the construction of a second data center at a remote location that receives copies of data as they are processed is on stand-by in case of a disaster. If there is a disaster, the second data center becomes the primary. This helps ensure a minimum of data loss. Copies of the Tier 3 applications are stored at the second data center and loaded on the system. Backup tapes from the Tier 3 applications are obtained and shipped to the second data center (if not stored there) and reloaded within its RTO. Processes are assigned to a tier, and different recovery solutions are devised for the groups to align costs with the need. Data from a Tier 2 application could be sent to the alternate data center by a batch method, wherein the backup data are stored until transmitted all at once, at certain time intervals. High-availability solutions are generally the most expensive. A short RTO and recovery point objective (RPO), or lower outage tolerance, will result in a higher cost of the continuity strategy. Second data centers are generally the best solution if no data loss is an issue, but are usually the most expensive. Third-party hot sites, network storage solutions, load balancing or server clustering (connecting multiple servers that share the processing and storage over a distance), and other information technology strategies are available.
Case Study

You are a newly hired corporate security manager responsible for establishing and managing a new corporate assets protection program. You know that an integral part of that program must be to ensure business continuity. You have found that the corporation does not have a business continuity plan. Identify and explain what steps are needed to produce an effective business continuity plan and provide a high-level outline of such a plan.

Answer: See pages 182 – 198 of the text.
Chapter 15: Business Impact Analysis

Learning Objectives

- Define a business impact analysis.
- Contrast BIA with risk analysis.
- Understand the BIA methodology.
- How to conduct a BIA.
- Data analysis and presentation of the BIA.

Presentation Outline

I. Introduction

A. Business Impact Analysis (BIA):
   1. Establish the value of each business unit.
   2. Determines order of recovery.
   3. Defines the impact of a disruption over time.
   4. Identifies interdependencies.
5. Determines recovery time objectives.
6. Decides which functions are critical.
7. Establishes financial basis for strategies.
8. Provides understanding of the amount of risk to assume, transfer or mitigate.

B. BIA examines impacts over time on:
   1. Service objectives.
   2. Financial position/cash flow.

C. BIA will also:
   1. Identify critical processes and applications.
   2. Establish the value of each business unit.
   3. Identify critical resources.
   4. Gain support for the recovery process.
   5. Increase management awareness.
   6. Meet regulatory requirements.
   7. Reveal inefficiencies in normal operations.
   8. Justify recovery planning budgets.

D. Establishes RTO and RPO:
   1. Outage Tolerance vs. RTO.
   2. Shorter object equates to most costly strategies.
   3. Result of BIA and management agreement.
   4. Can determine escalation point.
5. RPO is amount of acceptable data loss.
6. Often used to determine backup strategies.
7. Timing considerations in RTO, RPO determination.

E. Illustrates business cycle criticality.
F. BIA is a separate planning element.
G. Management time is minimized.
H. Questions often included relate to:
   1. Mitigation and Preparedness.
   3. Resource requirements.
   5. Initial strategy development.

II. BIA vs. Risk Analysis
A. BIA subset of Risk Analysis.
B. Places ‘asset value’ on business processes.
C. Focuses less on hazard identification.
D. Cause of disruption not considered.
E. Goal not to rank criticality of risks.
F. BIA/RA projects managed in similar ways.
G. BIA is a partnership with senior management.
H. Data presented differently.
III. BIA Methodology

1. Project Planning.

2. Data Collection.

3. Data Analysis.

4. Presentation of Data.

A. Project Planning:

1. Management commitment:
   a. Biggest single predictor of success or failure.
   b. Management sponsor.
   c. CFO.
      i. Top down approach.
      ii. Credible data.
      iii. Senior management influence.
      iv. Corporate-wide view.
   d. Agree on scope of analysis.
   e. Determine who should participate.
   f. Prepare list of financial impacts.
   g. Decide on method to collect data.
   h. Schedule interviews.
      i. Include Risk Management, Information Technology.

IV. Data Collection

A. Examine all current business functions.
B. Data collected through interviews.

C. Interviews seek financial and subjective impact information.

D. Formation of questions important.

E. Software programs and questionnaires.

F. Sample Questions.

G. Resource Data Collection:
   1. Short vs. long term needs.
   2. Include:
      a. Employees and consultants.
      b. Internal and External Contacts.
      c. Customers.
      d. Forms and Supplies.
      e. Equipment.
      g. Vital Records.

V. Data Analysis
A. Review of goals of analysis.
B. Criticality not determined solely upon numerical data.
C. Avoid duplication.
D. Do not deduct insurance reimbursement.
E. Validate results.
F. Establish outage tolerance during normal and critical business cycles.
VI. Data Presentation

A. Results presented to senior management.
B. Data must be credible.
C. Presentation short and simple.
D. Financial data better presented graphically.
E. State data as fact where possible.
F. Outline expectations of management.

VII. Updates

A. Reanalyze annually.
B. Reanalyze when strategic direction of company changes.
Sample Test Questions

True or False

136. To survive a disastrous event, a company must recover all of its business functions concurrently.  
    *Answer:* F (p. 200)

137. If a negative impact cannot be stated in financial terms, it should not be included in the business impact analysis.  
    *Answer:* F (p. 199)

138. A risk analysis cannot provide an understanding of the amount of risk to assume, transfer, or mitigate.  
    *Answer:* F (p. 199)

139. The business impact analysis can reveal deficiencies in normal business operations.  
    *Answer:* T (p. 200)

140. Although it is acceptable to ask questions related to hazard identification in the business impact analysis, it is less focused on hazard identification.  
    *Answer:* T (p. 201)

141. Business impact and risk analysis projects are managed in a similar fashion, although the data is presented differently.  
    *Answer:* T (p. 202)
142. A top-down approach to the Business Impact Analysis is the best method. 

*Answer: T (p. 202)*

143. Support organizations like Risk Management or Information Technology are not included in the Business Impact Analysis. *Answer: F (p. 205)*

144. Potential insurance reimbursements should be deducted from the analysis.

*Answer: F (p. 205)*

145. Financial data is best presented graphically. *Answer: T (p. 218)*

**Multiple Choice**

73. A business impact analysis: *Answer: c (p. 201)*

a. Assigns the probability of loss to a business function.

b. Expresses its results in terms of an Annual Loss Expectancy.

c. Assigns an ‘asset value’ to a business function.

d. All of the above.

74. Which of the following is true: *Answer: d (p. 206)*

a. Select those functions for analysis you or your sponsor know are critical.
b. Seek financial data only.

c. Ask straightforward questions such as “How critical is your operation?”

d. Decide on the best method to collect data.

75. The business impact analysis:  \textit{Answer: b (p. 201)}

\begin{itemize}
  \item tt. Returns more accurate data than the risk analysis.
  \item uu. Can be thought of as a subset of the risk analysis.
  \item vv. Is more important than the risk analysis.
  \item ww. Is used strictly for the purposes of business continuity planning.
\end{itemize}

76. A management sponsor:  \textit{Answer: b (p. 203)}

\begin{itemize}
  \item a. Demonstrates the ineffectiveness of the person conducting the analysis.
  \item b. Can help obtain support from other managers.
  \item c. Can slow down the project by adding another level of management.
  \item d. Is the person who makes the final presentation.
\end{itemize}

77. The analyst should use time periods:  \textit{Answer: a (p. 206)}

\begin{itemize}
  \item a. That are meaningful to the company under study.
  \item b. Consistent with other similar companies.
  \item c. Consistent with industry standards.
\end{itemize}
d. It is not important which time periods are used as long as they are consistent from one function to another.

78. A typical business impact analysis project consists of the following steps: Answer: a (p. 203)

a. Project Planning, Data Collection, Data Analysis, and Data Presentation.
b. Needs Analysis, Questionnaire Distribution, Strategy Selection and Justification.
c. Management Support, Data Verification, Strategy Selection and Justification.
d. Management Support, Data Verification, Report Distribution, BCP Project Initiation.

79. The biggest predictor of project success is most often: Answer: a (p. 203)

a. Management commitment.
b. Top-down approach.
c. Valid data.
d. Project funding.

80. Resource information collected in conjunction with the business impact analysis includes: Answer: d (p. 213)

a. Employee contact information.
b. Computer applications.

c. Vital records.

d. All of the above.

81. The criticality of a business process or department is:  \textit{Answer: b (p. 217)}

\begin{itemize}
  \item [y.] Determined by high value, high probability.
  \item [z.] Not determined solely upon numerical data.
  \item [aa.] Is a function of its value to other dependencies.
  \item [bb.] Is completely subjective.
\end{itemize}

82. A common problem encountered in the completion of a business impact analysis is:

\textit{Answer: a (p. 217)}

\begin{itemize}
  \item [21.] Counting the results or value of a function more than once.
  \item [22.] Failure to demonstrate the value of a recovery strategy.
  \item [23.] Completing the project too quickly.
  \item [24.] Arriving at results that conflict with the Risk Analysis.
\end{itemize}

\textbf{Short Answer}

1. List five results or outcomes derived from a business impact analysis.
Answer:

i. Identify which processes and computer applications are critical to the survival of the organization.

ii. Establish the value of each business unit as it relates to the whole, not to itself.

iii. Identify critical resources of the organization.

iv. Gain support for the recovery process from senior management.

v. Increase management’s awareness of the issues and resources required for a workable program, as well as introducing a basic planning structure to the management group.

vi. Potentially reveal inefficiencies in normal operations.

vii. Help to justify or allocate better recovery planning budgets (cost/benefit).

(p. 199)

2. Contrast business impact analysis with risk analysis.

Answer: A business impact analysis is a means of assessing the impact of a disruption in any functional area or on the operations of the enterprise as a whole. It can be considered a subset of a risk analysis, in that it places an “asset value” on business functions and focuses on the criticality of a disruption over various time periods. The source or cause of the disruption, or a detailed understanding of the probability of its occurrence, is relatively unimportant when conducting an impact
analysis and is therefore not considered.

The BIA focuses much less on hazard identification (some say there should be no focus on hazard identification). Listing all the hazards that might befall an operation may be useful in understanding the conditions, environment, and special needs required when selecting recovery strategies (such as the inability to move large pieces of equipment across town after an earthquake, or the amount of time required to remove bodies, complete an on-site police investigation, and remove the carnage after a workplace homicide), but this adds little to the understanding of financial or subjective loss to the operation over time. Outage tolerance is exclusive of its cause. Its goal is not to rank the criticality of risks for planning purposes but to identify the impacts of the loss of business functions over time, to help identify interdependencies, and to prioritize the order of functions to recover. The risk analysis is a more or less solitary experience, while business impact analysis is a top-down partnership with senior management.

(p. 201)

3. List three advantages to working with the CFO.

*Answer:* The CFO is more readily convinced of the importance of the project. This is the person who also may be legally responsible for the protection of certain corporate documents. The CFO is usually high enough within the organization to
drive the project and to help the planner both collect and interpret the data. If the planner has difficulty getting financial data from other managers, a “down and dirty” analysis can be derived from the CFO’s knowledge alone. The results of the analysis must be acceptable to management — everyone must believe that the analysis represents the true impact to the organization. The CFO should provide good insight into how the final report should be presented. The CFO can convince the CEO and other senior managers of the need to commit themselves to the project, and of the value of a top-down approach.

(p. 203)

4. List three ways to ensure the data presented to management is credible.

_Answer:_

- Verify the results with business unit management.
- Verify the results with the CFO.
- Use a top down approach.
- When presenting the results, ensure that figures are accurate and not misleading.
- Distribute a written report that includes supporting data.

(p. 218)
5. List the attributes of a good business impact analysis presentation to management.

*Answer:*

- Must be credible.
- Figures are accurate and not misleading.
- The data and the presentation are short and simple.
- Relationships and financial data are represented graphically.
- State expected occurrences not in terms of probability — state them as a fact.
- Distribute a written report that includes supporting data, the impacts for the individual functions or units, and the combined impacts for the organization.
- Outlines expectations of Management.

(p. 218)

6. The recovery time objectives provided to the Business Impact Analyst by the IT department for the following processes are: Accounting package, 2 weeks. Process control, 5 days. Inventory control, 5 days. Human Resources, 2 weeks. The outage tolerance provided to the analyst by the following departments are: Accounts Receivable (critical time month end), 10 days. Accounts Payable (critical time quarter end), 15 days. Process Control (always critical), 5 days. Inventory control (always and at product rollout), 4 days. and Human Resources (critical time is end of quarter), 2 weeks.
Determine what the recovery time objectives for the IT processes should be and how you could graphically represent it in your report.

*Answer:* [Very often, the IT department does not check with the business units when they establish recovery time objectives. Such is the case in this question.]

**Accounting Package:** 10 days

**Process Control:** 5 days

**Inventory Control:** 4 days

**Human Resources:** 2 weeks

<table>
<thead>
<tr>
<th>Application or Process</th>
<th>Function</th>
<th>Outage Tolerance</th>
<th>Critical Business Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Package</td>
<td>Accounts Receivable</td>
<td>10 days</td>
<td>Month and Quarter End</td>
</tr>
<tr>
<td>Accounting Package</td>
<td>Accounts Payable</td>
<td>15 days</td>
<td>Quarter End</td>
</tr>
<tr>
<td>Process Control</td>
<td>Process Control</td>
<td>5 days</td>
<td>All</td>
</tr>
<tr>
<td>Inventory Control</td>
<td>Inventory Control</td>
<td>4 days</td>
<td>All, Product Rollout</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Human Resources</td>
<td>2 weeks</td>
<td>End of Quarter</td>
</tr>
</tbody>
</table>

(Ch. 15)
7. What is missing from the following Employee resource questionnaire?

Name, Title, Home Address, Home Phone Number, Cellular Phone Number, Pager or Alternate Phone Number

*Answer:* Call or reporting priority ranking (can also be home email address).

(p. 213)

8. Devise a list of subjective impact questions and illustrate what the result would look like in your final report.

*Answer:*

Subjective impacts can include:

- Loss of competitive advantage or market position
- Loss of shareholder confidence
- Increased liability
- Decreased employee morale
- Cash-flow difficulties
- Reduced public image or confidence
- Reduced customer service
- Contractual consequences
Regulatory violations and consequences

Loss of key personnel.

Results may look like:

![Average Severity Graph]

Type of Disruption

(Ch. 15)

Case Study

You are the corporate security manager of a large corporation. Your boss calls you into the office one day and says that the CEO was at an executive management conference where the topic of business impact analysis (BIA) was discussed. The CEO wants to know “what are you doing relative to BIA.” Your boss wants to know what it is and the difference between risk analysis and business impact analysis. Furthermore, your boss wants to know if there are any
advantages if the BIA processes were used instead of, or in partnership with, risk analysis. What answers would you give your boss?

Answer: See pages from the text.

**Case Study #2**

You are in the middle of conducting a Business Impact Analysis when the president of the company gives a speech to a major consumer group and tells the audience and the media that the company’s goal is to ship all orders within 24 hours of the placement of the order without fail. The president later issues an internal memo to the warehouse and shipping departments confirming this goal. Your extensive analysis shows that the warehouse, shipping, distribution, and order entry functions can sustain a recovery period of up to two weeks without significant financial loss or a loss of customers. Every other function identified in your analysis shows similar results or that functions will not show a financial or subjective impact for more than two weeks. All of your work has been reviewed by the Chief Financial Officer (CFO) who agrees that your data is accurate. To be on the safe side, functional managers agree that their recovery time objectives are within a one- to two-week period which will allow for the selection of less costly recovery strategies. What recovery time objectives you would recommend? Justify your recommendations.

*Answer:* The recovery time objective for any function, system, or process that is dependent on shipping an order (including warehouse, shipping, distribution, and order entry) will
have a recovery time objective of not more than 24 hours. We are assuming that the
president meant what he or she said. Although your data and good financial judgment
may indicate a longer RTO, the selection of an RTO is ultimately a management decision.
The remaining RTO can be within the one- to two-week (or more) period.

(p. 200)
Chapter 16: Plan Documentation

Learning Objectives

- Importance of plan documentation.
- Elements of business and governmental planning and plan documentation.
- Recovery team methodology.
- Plan organization and structure.

Presentation Outline

I. Introduction

A. Plan documentation:
   
   1. Help expedite recovery.
   2. Prevent the misuse of resources.
   3. Capture knowledge.
   4. Ensure necessary tasks are completed.
   5. Provide guidance for auditors.
II. Required Elements

A. Must be organized in a logical sequence.
B. Clean and easy to follow.
C. Complete but not overly detailed.
D. Contain a glossary.
E. Facilitate transition from response to recovery.
F. Assign responsibility.
G. Outline specific resources and tasks.
H. Must be flexible.
I. Contain references to other plans or documents.
J. List plan assumptions or constraints.

III. Multi Hazard Functional Planning

A. FEMA format for governmental planning.
C. Task-based planning for requirements or functions, rather than each hazard.
D. Two components to plan:
   1. Basic plan.
   2. Functional annexes.
E. Basic plan:
   1. Outlines overall emergency organization.
   2. Primary audience is executive and managerial level.
   3. Functional annexes are sub-plans that focus on specific functions.
4. Annex may contain its own appendix of tasks.

F. Contents of the basic plan:

1. Introductory material.
2. Purpose Statement.
3. Situation and Assumptions.
5. Organization and Assignment of Responsibilities.
6. Administration and Logistics.
8. Authorities and References.

G. An effective Business Continuity Plan can follow this format.

IV. Plan Organization and Structure

A. Similar Multi-Hazard Functional Plan.

1. Basic plan.
2. Departmental or team plans.

B. Contents include:

1. Policy.
2. Scope.
3. Objectives.
4. Assumptions.
5. Activation authority and procedures.
a. Activation levels.

6. Alternate locations and space allocations.

7. Recovery priorities.

8. Plan distribution.


10. Exercises.

11. Plan maintenance requirements.

12. Appendix.

C. Team recovery plans.

1. Information from the Basic Plan.

2. Overview of functions and strategies.

3. Team member contact list.

4. Team tasks.

5. Resource requirements.
   a. Vendors (internal / external contacts).
   b. Customers.
   c. Equipment requirements.
   d. Forms.
   e. Supplies.
   f. Software and applications.
   g. Vital records.
   h. Other resources.

D. Blank forms.
Sample Test Questions

True or False

146. Business continuity plans can follow a format similar to the multihazard format.

*Answer: T* (p. 223)

147. All recovery teams should have access to the basic plan and copies of all other team plans.

*Answer: F* (p. 229)

148. Plans must be complete but not overly detailed.

*Answer: T* (p. 221)

149. Although it may exist in greater detail elsewhere, company business continuity planning policy is mentioned in the basic plan.

*Answer: T* (p. 224)

150. Nothing from the basic plan is included in the team plan.

*Answer: F* (p. 229)

151. It is not appropriate to include in the section on ‘scope’ items the plan does not cover.

*Answer: F* (p. 224)

152. Recovery strategies should not be outlined in the team plan.

*Answer: F* (p. 229)

153. Blank forms are appropriately appended to the team plan.

*Answer: T* (p. 230)
154. To ensure consistency with governmental planning methodologies, business continuity plans should not follow company standard document formats. *Answer: F* (p. 221)

155. Because of the possibility of the loss of data when it is needed most, business continuity plans should not be distributed in electronic format. *Answer: F* (p. 228)

**Multiple Choice**

83. The following is properly included in a functional annex: *Answer: b* (p. 222)

a. Promulgation document.

b. Search and rescue.

c. Policy.

d. Lines of authority.

84. The plan: *Answer: c* (p. 223)

a. Should not contain references to other documents.

b. Should include all documents and information needed for recovery.

c. Can include references to other documents if necessary.

d. Stands on its own.
85. Parts of a Business Continuity Plan include:  \textit{Answer: a (p. 223)}

a. Basic and Team Plans.

b. Basic Plan and Functional Annexes.

c. Functional Annexes and Team Plans.

d. Basic Plan and Standard Operating Procedures.

86. Which belongs best in a governmental planning document?  \textit{Answer: d (p. 223)}

a. Basic and Team Plans.

b. Prioritization Matrix.


d. Concept of Operations.

87. The plan should include sections that describe:  \textit{Answer: a (p. 224)}

cc. Training, Exercising, and Maintenance.

dd. Preparedness and Mitigation.

e. Emergency Response.

ff. All of the above.

88. Team task instructions: \textit{Answer: a (p. 229)}
25. Can be separated into tasks required in the first 24 hours.

26. Should be directed toward someone who has absolutely no knowledge of how to perform the team’s duties.

27. Should contain the function’s abbreviations and acronyms.

28. Maximize the need to make post-disaster decisions.

89. The entire business continuity plan should be distributed to: Answer: c (p. 227)

   a. Every team member.
   b. Management team only.
   c. A selected few.
   d. Information Technology.

90. Which assumptions can be included in the plan? Answer: d (p. 225)

   a. Buildings are totally destroyed.
   b. Resources will not be available to support all product lines.
   c. Most key personnel will be available.
   d. All of the above.

91. Allocation generally refers to: Answer: d (p. 227)
a. The percentage of business continuity budget the team receives.

b. The team’s share of resources.

c. The amount of time on the server.

d. The number of team members who will report to an alternate site.

92. Which is generally not included in the team plan? Answer: b  (p. 228)

a. Activation procedures.

b. Policy statement.

c. Organization and structure.

d. None of the above.

Short Answer

1. List five justifications for documenting business continuity plans.

Answer:

i. Fundamental to the Business Continuity process.

ii. Lack of a plan will add delays to the organization’s fight to recover.

iii. Lack of a plan can cause the misuse of scarce resources.

iv. Lack of a plan may ultimately set the stage for the failure of the business.

v. May be required by regulations.
2. List five ‘required’ elements of plan documentation.

*Answer:*

- The plan must be organized in a logical sequence.
- It must be “clean” and easy to follow.
- It must be complete but not overly detailed.
- It must contain a glossary defining any terms used.
- It must facilitate a smooth, seamless transition from response to recovery.
- It must assign responsibility for planning to individuals within the organization and describe the emergency lines of authority.
- It must outline specific resources and tasks required to carry out recovery operations.
- It must be flexible enough to address unforeseen events.
- The plan must allow for midcourse correction and adaptation.
- It must contain references to other plans or documents.
- It must state assumptions upon which the plan is based or by which it is constrained.
3. List five categories of resources that are included in team plans.

*Answer:*

- Vendors (internal and external contacts)
- Customers
- Equipment requirements
- Forms
- Supplies
- Software and applications
- Vital records
- Other resources (Model numbers, configurations, floor plans, cabling diagrams, tax tables, milestones, and other due dates, along with both the short and long-term quantities required)

(p. 230)

4. Contrast the differences and similarities between governmental plans and business continuity plan structures.

*Answer: Multi-hazard functional planning is a format the Federal Emergency Management Agency (FEMA) suggests that governmental agencies use to develop their emergency operations plans. An effective business continuity plan follows the*
multi-hazard functional format, especially if a recovery team methodology is used. More recently known as “all-hazard emergency operations planning,” it is based on the premise that although the causes of emergencies and disasters vary, almost three-quarters of them produce common response requirements. The jurisdictions can then develop task-based plans around these requirements or functions rather than around each anticipated hazard. Some hazards do produce unique needs. These needs, requirements, and responses are appended to the “basic plan,” under this methodology. Similarly, business continuity plans are task-based in that instructions in team plans are scripted to implement strategies to recover critical functions, not individual types of disasters (this is referred to as contingency planning).

The main part of the governmental plan — known as the basic plan — outlines the overall emergency organization, its policies, assumptions, activation, and lines of authority. Its primary audience is the jurisdiction’s executive and management level staff. Business Continuity Plans also contain a basic plan, but it is directed to all those involved in the continuity process. It contains similar information, minus certain introductory material such as a Promulgation Document (outlines the authority and responsibility for the plan, usually signed by the chief executive officer), and a Signature Page (demonstrates that all response organizations have participated in its development and are committed to its success), and a section on Authorities and References that highlight enabling laws and the legal basis for emergency operations. Both can contain a dated title and revisions page, distribution list, and Table of Contents. A governmental plan contains a Purpose
Statement, Situation and Assumptions section that describes the scope of the response and the assumptions upon which the plan and response are based. “Situation” refers to a description of the justification or necessity for the plan. Many of these elements are not included in business-oriented plans, although the scope and assumptions section is appropriate for both. Except for coordination with other agencies (in most cases) both types of plans will describe the overall strategy or approach to the response or situation, activation of the plan, and coordination with other agencies (referred to in governmental plans as the ‘Concept of Operations’). A section on Organization and Assignment of Responsibilities that delineates the emergency organization and reporting hierarchy where each position is listed, along with an overview of its duties and responsibilities is appropriate in the All-hazards plan, but a business continuity basic plan can include similar information (some may argue that a discussion of the emergency or continuity organization does not belong in the plan because it is training in nature). A more appropriate section for the governmental plan is a section on Administration and Logistics that defines the general administrative policies, such as financial and purchasing controls and procedures, resource management, and mutual-aid agreements. These elements can be also found in a business continuity plan. A governmental plan should contain information on Plan Development and Maintenance. This section outlines the overall approach to the plan — in contrast to the approach to the response. It explains responsibilities of the planners, the planning process, and includes the requirements for plan maintenance and exercising. Except for the requirements for plan maintenance and exercising, this
information should not reside in a business continuity plan.

Functional annexes are sub-plans that focus on specific functions the jurisdiction will perform in response to the disaster. Shelter management, evacuation, and search and rescue are examples. Each annex may contain its own appendix of tasks and requirements for dealing with the specifics of a particular hazard. Standard operating procedures (SOPs) and checklists may be included in the annex.

Functional annexes are very similar to the individual team plans as they are sub-plans attached to the basic plan but pertain to the recovery of critical functions.

(Ch. 16)

5. Diagram a matrix that illustrates who has plan activation authority.

*Answer:* The answer should look similar to the following:

<table>
<thead>
<tr>
<th></th>
<th>Multiple Plans</th>
<th>Entire Site Plan</th>
<th>Multiple Teams</th>
<th>Individual Teams</th>
<th>Escalation or Hot site Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Team</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Management Team</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Recovery Coordinator</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Team Leader</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Copyright 2006 © Elsevier, Inc. All rights reserved.
6.Compose a brief policy statement to include in the basic plan.

**Answer:** The plan can briefly outline or reference the existence of management’s policy to develop, exercise, and maintain the plan. Ideally, there will be a full policy statement, signed by the CEO. Some planners include a brief description of the responsibilities of separate divisions, sites, or departments for developing their own plans. Although not included in the text, it can include the formation of a steering committee, the allocation of resources, and wording that indicates management support. Reference should be made to the completion of a Business Impact Analysis and that the plan should cover all critical business activities. The following is an example of a brief policy statement that may appear in a basic plan:

XYZ has a policy to implement and maintain a program that identifies natural, technological, and human caused hazards to the business operations, facilities, and employees and that takes reasonable steps to mitigate the effects of these hazards. This program will identify XYZ’s critical business processes, and develop methodologies to implement cost-effective recovery strategies. XYZ will develop plans and procedures to
respond to emergency situations that will maintain or recover operational capability in the shortest appropriate time. The plans detail the firm’s re-establishment of critical business processes and the continued functioning of necessary operations and services. This policy has the full support of the CEO. It is our policy that these plans are exercised on a regular basis.

(p. 224)

7. Criticize the following day-one team task instructions (scripted continuity instructions):

- Decide how best to track, record and report expenses associated with the team’s recovery.

  **Criticism:** This is a decision that should have been made beforehand. A goal of continuity planning is to make as many decisions as possible beforehand.

- Select a team member to report the progress of the recovery to the recovery coordinator.

  **Criticism:** This instruction belongs to the team leader who is responsible for communication with the recovery coordinator or other team leaders. It should reside in a list of tasks for the team leader and not for the team.

- After the MLB of the CTR is completed, re-establish functionality across all systems.
Criticism: Use of acronyms. While common acronyms may be used if they are understood by all, they should be avoided.

- Re-establish operation of the M-1 database on Server #7 using the following procedure: SitSoft is pleased you have purchased our programs to keep your productivity at the highest levels possible. The following chapters will guide you through the installation process. While we strive …

Criticism: Instructions must be brief and to the point, but complete. This instruction should not attempt to replicate the entire installation manual. It should include only the essential points or make reference to the location of the document or its recall procedure from off site storage.

- After the damaged facilities are restored, begin move back procedures.

Criticism: This is typically not a day-one instruction. Students may also mention that this instruction is not sufficiently detailed.

(p. 229)
**Case Study**

Three years ago, your company employed about 50 people in one building. Since then, the company has experienced tremendous growth and now occupies 5 buildings with almost 750 employees. A business continuity plan was developed more than three years ago. You have just been assigned responsibility for business continuity planning. Describe how you will change the existing document.

*Answer:* Since the original plan was developed for a very small company with 50 or less individuals, it most likely used a single team methodology and was likely just a list of phone numbers and simple tasks. Your revised document should include all of the elements outlined in the text.

(Ch. 16)
Learning Objectives

- How to develop a planned approach for dealing with a crisis.
- What steps to take when notified of a kidnap or ransom demand.
- Items to consider when paying a ransom.
- Preventative measures.
- Procedures kidnap victims should know.
- Controlling information.

Presentation Outline

I. Introduction

A. Misunderstanding of term ‘Crisis.’

B. Distinctions between Business Continuity Planning.
II. Threat Identification

A. Branding could represent most valuable asset.
B. Threats can be varied.
C. Risk analysis and scenario planning.
D. Political and personal gain basic motivations for kidnapping.
E. Victims possess common elements.

III. Plan Activation

A. Crisis levels.
B. Pre-planning and analysis.
C. Proactive response.
D. Monitor conditions.

IV. Crisis Management Team

A. Crisis addressed by a crisis management team (CMT).
B. Senior management with decision-making authority:
   1. Consists of least number of individuals.
Chapter 17: Crisis Management Planning for Kidnap, Ransom and Extortion

2. CEO can act as leader.

3. Technical advisors.

4. Record keeping.

C. Duties:
   1. Collect and evaluate information.
   2. Prevent escalation.

D. Not a substitute for Security or Law Enforcement.

E. Use of consultants.

F. Priorities in protection of assets.

G. Involve legal department.

H. Autonomous control over decisions.

V. Initial Contact

A. Immediate notifications.

B. Initial actions may determine the outcome.

C. Discuss recording devices and tracing capabilities beforehand.

D. Training:
   1. Record or write down all data given by the extortionist.
   2. Express cooperation.
   3. Ask questions to lengthen the time of the call.
4. Secure proof that the hostage is being held and unharmed.

5. Call recipient should talk with the hostage:
   a. Give the hostage the opportunity to relay critical information through a prearranged code.

E. Many demands are a written threat:
   1. Protect letters and envelopes from unnecessary handling.
   2. Take steps to identify the source of the document if it was not mailed.
   3. May be necessary to interview all employees immediately.

F. Determine whether the demand is a hoax.
   1. In a kidnap case, establish the whereabouts of the victim immediately.

VI. Ransom Considerations

A. Decision by family and company.

B. Develop policy and the limitations.

C. Not possible to fix categorical limits.

D. ‘Key man’ coverage is a rough standard payment amount.

E. Alternative is to refuse to pay ransom altogether.
   1. Paying a ransom of any type may induce others to try again.

F. Net impact on the enterprise may be smaller than the amount paid.
   1. Cooperation with law enforcement will improve chances of capture and recovery of funds.
   2. Commercial insurance can cover a portion of the ransom payment.
Chapter 17: Crisis Management Planning for Kidnap, Ransom and Extortion

G. Law enforcement authorities will assist in preparing the ransom package.
   1. Plans must be made for availability of funds in appropriate denominations.
   2. It takes considerable time and effort to record currencies used in ransom payments.
   3. Large amounts of small denominations produce heavy, bulky packages.

VII. Preventative Security

A. Capability and awareness of security practices will decrease attempts.
B. Alert executives to the risk.
C. Train executives in personal security.
D. Improve the physical security of executive residences.
E. Instruct children on appropriate precautions.
F. Limit the dissemination of personal information.
G. Secure automobiles.

VIII. Suggestions for Kidnapped Individuals

A. Victim can control an abductor’s actions.
B. Attempt to convince captors that well-being is essential to their success.
C. Develop a relationship with the abductors.
D. Give information through prearranged code words, phrases, or verbal mannerisms.
E. Almost no circumstances in which an escape attempt is recommended.
IX. Media Control

A. CMT reviews methods to communicate to public.

B. Present a consistent, coordinated response.

C. Establish and communicate media policy.

D. Consequences.

E. Importance of accurate information.

F. Coordination with media:
   1. Locations.
   2. Separation of victims.
   3. Resources.
   4. Control of information.
Sample Test Questions

True or False

156. Although the terms *crisis management planning* and *business continuity planning* are synonymous, their planning is very different. **Answer: F** (p. 231)

157. Brand name identification can represent the company’s greatest asset. **Answer: T** (p. 233)

158. A business impact analysis is best used to identify threats against the organization that could become a crisis. **Answer: F** (p. 233)

159. The two basic reasons for executive kidnappings are personal gain and political purposes. **Answer: T** (p. 234)

160. A crisis management plan can stand on its own, apart from a business recovery plan. **Answer: T** (p. 234)

161. The crisis management plan must resolve the fixed elements of a crisis, so as to require the CMT to make only those decisions during a crisis that are affected by immediate variables. **Answer: T** (p. 234).
162. The CMT should consist of the least number of individuals possible. \textit{Answer: T (p. 235)}

163. The CMT must be given autonomous control over decisions the corporation must make during a crisis, consistent with an advance plan approved by the board of directors. \textit{Answer: T (p. 237)}

164. In a kidnap case, the whereabouts of the alleged victim must be established immediately. \textit{Answer: T (p. 238)}

165. Paying a ransom in small bills has many advantages both to the kidnappers and to the company. \textit{Answer: F (p. 239)}

166. Law enforcement agencies will decide if a ransom should or should not be paid. \textit{Answer: F (p. 239)}

167. The amount of a kidnap victim’s life insurance policy should never be considered when evaluating a ransom demand. \textit{Answer: F (p. 239)}

168. It is inappropriate to include the immediate families of executives in kidnap and ransom plans. \textit{Answer: F (p. 238)}
169. A company’s demonstrated crisis-response capability and an awareness of personal and corporate security practices will decrease the chances of a kidnap or extortion attempt. **Answer: T (p. 240)**

170. The Public Relations Department, not the Crisis Management Team, decides what information is released to the public. **Answer: F (p. 241)**

**Multiple Choice**

93. Crisis management planning: **Answer: a (p. 232)**

   a. Can conform to the comprehensive emergency management model.
   b. Because of the variables, is best when addressed on an ad hoc basis.
   c. Applies mostly to kidnap and ransom.
   d. All of the above.

94. Kidnap or extortion victims generally possess one or more of the common elements:

   **Answer: d (p. 234)**

   a. Money.
   b. Power.
   c. High public visibility.
   d. All of the above.
95. An executive’s chances of being kidnapped are increased if: *Answer: d* (p. 234)

a. His industry is often victimized by terrorists or extortionists.
b. His company has a history of paying ransom demands.
c. His company does business in an area prone to kidnapping.
d. All of the above.

96. Knowledge of the types of adversaries encountered: *Answer: d* (p. 237)

a. Is not important, since all are handled in the same manner.
b. Is provided to the CMT by the security director or security consultant.
c. Is impossible to obtain.
d. Is best obtained through local law enforcement.

97. A result of the failure to plan, or to pre-approve actions and limitations by the board of directors, could be: *Answer: d* (p. 237)

a. Stockholders’ and employee negligence suits.
b. Insurance cancellations.
c. Expropriations of assets by foreign governments.
d. All of the above.
98. Persons who may potentially receive a telephoned kidnap or extortion demand should be trained to: \textit{Answer: a} (p. 238)

a. Secure proof that the hostage is being held and is unharmed.

b. Understand the CMT process.

c. Negotiate the person’s release.

d. Reassure the victim.

99. Which is most important when notification of a kidnapping is first received? \textit{Answer: a} (p. 238)

a. Determine whether the demand is a hoax.

b. Contact the FBI or other Federal authorities.

c. Place the bank on notice.

d. Decide if the ransom demand will be met.

100. If a decision is made to pay a ransom, the net impact on the enterprise is: \textit{Answer: a} (p. 239)

a. Much smaller than the amount paid.

b. Much larger than the amount paid.

c. Ransom should never be paid.

d. Impact cannot be determined.
101. The victim in a kidnapping case should: \textit{Answer: b} (p. 240)

\begin{itemize}
\item gg. Remain passive, as he or she has no control over the situation.
\item hh. Attempt to convince his captors that his or her well-being is essential to their success.
\item ii. Attempt to escape immediately.
\item jj. None of the above.
\end{itemize}

102. Which of the following is good advice for kidnap victims? \textit{Answer: b} (p. 240)

\begin{itemize}
\item 29. Take survival classes to ensure their safety after escape.
\item 30. Develop a relationship with the abductors.
\item 31. Flash international distress signals to outsiders.
\item 32. None of the above.
\end{itemize}

\textbf{Short Answer}

1. Design a short training program (list topics or subjects) for executives to prevent kidnappings.

\textit{Answer:}

\begin{itemize}
\item i. Alert the corporation and its executives to the level of danger
\item ii. Physical security of executive residences
\end{itemize}
iii. Instruct children on appropriate precautions

iv. Limit the dissemination of personal information

v. Secure automobiles

vi. Suggestions for kidnapped individuals

vii. Prearranged code words, phrases, or verbal mannerisms

viii. Don’t appear to jeopardize the abductors’ plan

ix. Develop a relationship with the abductors

x. Avoid escape

(p. 240-241)

2. What steps would you take specific to the receipt of a written ransom demand?

*Answer:*

- The letter and its envelope should be protected from unnecessary handling and preserved for fingerprints, handwriting, printing and typewriting examinations, as appropriate.
- Identify the source of the document if it was not mailed.
- Interview all employees immediately in order to develop information leading to the identity of the person who delivered the communication.

(p. 238)
3. Discuss the pros and cons of refusing to pay a ransom demand.

*Answer:* If ransom is not paid, you avoid the question of how much to pay, the danger of losing the ransom in transit, avoid shareholder liability if the executive approving or making the ransom payment did not act legally, did not have corporate authorization, or if the payment of ransom or any other action taken in response to the extortion demands was itself a violation of local criminal law. It has been suggested that paying a ransom of any type may induce others to try again, that the possible individual loss of life is a necessary cost.

However, at least within the United States and Canada, the business community and the general public may not accept the above position and its potential cost.

If a decision is made to pay a ransom, the net impact on the enterprise may ultimately be much smaller than the amount paid, for two reasons. First, active cooperation with law enforcement from the very beginning will improve the chances of capturing the kidnappers and recovering all or part of the money. Second, commercial insurance can be purchased to cover a portion of the ransom payment actually made.

(p. 239)

4. Speculate on the effects of a response to a kidnap and ransom demand without using a Crisis Management Team.
Answer: Decisions for the entire corporation during a crisis might be made on an ad
hoc or poorly considered basis, potentially with a large unit that is generally
incapable of reaching decisions quickly and who may not have the ability to develop
alternative strategies after gathering information and analyzing threats under
rapidly changing crisis conditions. Decisions that affect the company directly and
require corporate decisions or responses or partnerships with law enforcement may
be less effective. Publicity and public information may be mishandled or not
properly controlled. The lack of a team may equate to the lack of corporate
leadership. The response to a demand requires a team approach. The CMT will
require the assistance of its legal counsel to examine such issues as employee and
stockholder rights vis-à-vis the legal standing of the company regarding various
strategies and monetary payments to extortionists. Information from the financial
arm of the corporation is needed to develop the monetary base for CMT operations,
and its assistance is needed to set the corporate strategy and limitations regarding
ransom of any particular corporate employee. Every action to be taken by the
company not dependent on the specific nature of the crisis should be rehearsed,
much like a fire drill; only the variable decisions will then have to be handled. This
would be difficult without a specific team. The lack of a team may increase
considerably the probability of loss through matters growing out of the original
crisis, such as stockholders’ suits, employee negligence suits, wrongful-death suits,
insurance cancellations, and expropriations of assets by foreign governments
irritated by the way in which a corporation handled a problem. Inadequate action
or improper action by the corporation leading to death or injury of an employee might result in claims against the corporation for damages by the employee or his family. This is particularly true if there were no contingency plans and the injured employee was exposed chiefly because of his corporate employment.

A company’s demonstrated crisis-response capability and awareness by executives of personal and corporate security practices will likely decrease the chances that a corporation or its executives will become victims of a kidnap or extortion attempt, thus increasing the chances if the team did not exist.

(Ch. 17)

5. You are a plaintiff’s attorney for a family member of an executive that was killed overseas in a kidnap and ransom attempt. Outline points that may help you show liability on the company’s part.

*Answer:*

- Failure of the company to identify the risk;
- Lack of advance planning by the corporation;
- Failure to develop crisis management skills;
- Failure to form a crisis management team;
- Poor decision making by management or by the team;
The plan did not fix corporate objectives and limitations;

The plan was not designed to be effective when the CMT is operating under the emotional strain of responsibility for human life;

The plan did not have sufficient flexibility to enable the CMT to develop alternative strategies;

A trained hostage negotiator was not working in conjunction with law enforcement personnel to act as the intermediary between the extortionist and the victim company;

The corporation had little knowledge of the types of adversaries encountered;

Lack of assistance from the corporate legal department;

Provisions for gathering personal data, family biographical sketches, as well as medical and other requirements of the employee and his family, were not incorporated into the plan or methods to make this data readily available during the crisis period did not exist;

Responses to the media were not coordinated with law enforcement officials to avoid premature release of information that may have jeopardized the victim’s life;

The CMT was not given autonomous control over decisions the corporation must make during a crisis, or their decisions were not consistent with an advance plan approved by the board of directors;

The actions, methods, and procedures were not ‘rehearsed’ by the CMT;

The CMT did not work with, or worked with the host country in such a manner that they became uncooperative;
- Law enforcement, the CMT or responsible management was not notified of the incident in a timely manner;
- Details of the threat were not maintained or handled in a manner that could have provided information on the safety, conditions, or whereabouts of the victim;
- Failure to interview the person who received the initial threat;
- The person receiving a telephoned threat did not attempt to talk with the hostage or to give the hostage the opportunity to relay critical information through a prearranged code;
- The person who received the call did not end the conversation in a manner that allowed additional contacts with the extortionist before a ransom is paid;
- Following receipt of a written threat, steps were not taken to identify the source of the document, to protect it or to develop additional identifying information;
- The decision to pay or not pay ransom was mishandled;
- Payment was delivered improperly;
- Failure of the company to take preventative measures such as physical security;
- Victim was not trained in how to survive and manage the situation.

(Ch. 17)
Research

2. Research a corporate kidnapping case. Discuss the payment of ransom, how the company reacted and what the public relations ramifications were. Was there a rescue attempt? Does your research show if any outside agencies participated?

Many references on the Internet or published material.

Case Study

In today’s international business environment, corporate executives are traveling around the world. Some of the places they travel are more dangerous than others. However, the threat of kidnapping, ransom, and/or extortion is always a possibility, regardless of the location.

To be prepared to deal with such events, the corporate security manager should take the leadership role in establishing a crisis management team in the event such an incident occurs. In a briefing to your corporate executive management team, you explain the need for such a team. Assume you are providing that briefing. Explain the rationale behind the formation of such a team, its makeup, and give a detailed example of an incident that would require the activation of the team and what steps they would take in dealing with the crisis.

Answer: See pages 235-240 of the text.
Case Study #2

Your company runs a day care center for employee’s children that took a group of 12 on a field trip to the local zoo. You are in the parking lot returning from lunch, and notice a TV news reporter conducting a live interview with a secretary about the shooting and kidnapping of some children at the zoo. Your company has recently been the target of animal rights demonstrations. What actions need to be taken?

Answer: See chapter and appendix for answers.
Chapter 18: Monitoring Safeguards

Learning Objectives

- Students are introduced to the concept of system testing.
- Different testing methods are introduced.
- The reasons behind and importance of testing are discussed.

Presentation Outline

I. Introduction

   F. A system will prove to be either adequate or inadequate in meeting objectives.

II. Monitoring or Testing Existing Systems

   A. Periodically monitoring or testing the existing system determines adequacy.

III. The Scientific Method
A. The scientific method is a basic problem-solving approach that gathers data to confirm or reject a developed hypothesis.

B. People and procedures must be tested in a number of scenarios.

C. To be effective, testing must be an ongoing process.

D. Testing is the only way the integrity of any system or procedure can be proven before catastrophe strikes.

E. Testing should be included in every designed security system, large or small.

IV. Five Basic Types of Testing

A. There are five basic types of testing:

1. Functional testing determines if CCTV or electronics access control system will do what it was designed to do.

2. Safety testing determines if the object or procedure can be used without causing injury, loss, or harm.

3. Performance testing validates conformance to timing, resource usage, or environmental constraints.

4. Stress testing checks a person’s or object’s tolerance to abuse or misuse under deliberately introduced stress.

5. Regression testing applies to an object, system, or procedure that has been altered to perform a new function while still performing some of its original functions.
B. Testing can apply equally to persons, systems, procedures, methodologies, and objects.

C. Testing must have a specified objective.

D. Other questions that should be answered are:
   1. Are the tests adequate?
   2. Are the results valid?
   3. Can this type of test uncover a weakness or flaw that might otherwise remain hidden?

E. The best time to prepare a hardware or electronics equipment test is during design.

F. Tests can be broken down into component segments.
   1. Desirable to conduct functional and performance tests this way.
   2. Testing a complex system at one time is more difficult and expensive.

V. Avoid Predictable Failure

A. Any system that is not periodically tested will eventually fail.

B. The testing concept is consistent with the objective of reducing risk by diminishing uncertainty.

C. Testing is often not completed due to its expense.

VI. Some Audit Guidelines

A. Test expense can be reduced by basic audit techniques:
   1. Statistical sampling.
2. Restricting the value of input parameters or limiting the scope or field of inquiry.

3. Scheduled testing.

B. Every test shortcut has potential risk.

C. Almost total absence of a general, accepted set of practices for testing security systems.

D. Testing techniques used by other disciplines can be used.

E. Attributes of an effective measurement (test) system (safety):
   1. Administratively feasible.
   2. Adaptable to the range of characteristics to be evaluated.
   3. Constant.
   4. Quantifiable.
   5. Sensitive to change.
   6. Valid in relation to what it is supposed to represent.
   7. Capable of duplication with the same results from the same items measured.
   8. Objective, efficient, and free from error.

F. The Auditing field sets forth the following guidelines:
   1. An audit is part of management control.
   2. Management is the planning, organization, direction, and control of activities to achieve desired goals.
   3. It is necessary in a successful business process to set policy, establish procedure, assign responsibility, institute an accountability system, and measure performance.
   4. Exceptionally good levels of security performance are achieved when risk control is perceived as an important and integral part of planning, organization, direction, and control.
5. Risk-control management systems must be integrated into the mainstream of all management functions.

6. There is a noticeable difference between issued policy and procedure and what actually occurs.

7. Seldom is an activity as effectively managed as those responsible for it say it is.

G. Auditing risk control (security) programs can serve as an appraisal of management’s performance.

H. The basic objective of the audit (test) is the qualitative analysis of the existing security system(s) to determine whether performance is effective and acceptable.

VII. Develop Plan of Action

A. Suggestions to develop a plan of action for submission to management include:

1. Review the existing test procedures, if any.

2. Identify kinds of tests conducted, by whom, when, and where.

3. Determine if tests cost-effective and proven to reduce (eliminate) risks.

4. Ensure records of past tests are maintained for future use.

5. Investigate the existence of better, less expensive tests that can be adapted at your facility.

6. Eliminate tests that are no longer functional or effective.

7. Identify high-risk areas within the organization that are not being tested (audited).

8. Develop a suggested test program for management’s review and approval.

9. Decide if outside help or a second opinion is necessary for complicated tests, audits
or surveys.

10. Evaluate your capability to develop and implement formal testing policy and guidelines.

B. Performance examination is a necessary element of the security professional’s job description.
Sample Test Questions

True or False

171. A system should be periodically tested to determine if it is still doing the job for which it was designed or installed. Answer: T (p. 245)

172. The scientific method is the gathering of data to be used to confirm or reject a developed hypothesis. Answer: T (p. 246)

173. If the results of a test are positive, it need not be periodically repeated. Answer: F (p. 247)

174. Safety testing: a test to determine if the object or procedure can be used without causing injury, loss, or harm. Answer: T (p. 246)

175. Testing does not necessarily need to have a specified objective. Answer: F (p. 247)

176. Tests can be broken down into component segments. Answer: T (p. 247)
177. One suggestion to developing a plan of action for submission to management is to determine if records of past tests conducted are being maintained for future use. **Answer: T (p. 249)**

178. According to audit control guidelines, risk-control management systems must be integrated into the mainstream of all management functions. **Answer: T (p. 249)**

179. In the security profession, there are specific standards used to test and evaluate security systems and processes. **Answer: F (p. 248)**

180. Testing is often not completed due to its expense. **Answer: T (p. 248)**

**Multiple Choice**

103. A system, upon review, will prove to be what in meeting the client’s objective?

**Answer: a (p. 245)**

a. Adequate or inadequate.

b. Functional or underutilized.

c. Properly designed or under-designed

d. Tested or untested.
104. The type of testing that usually applies to an object, system, or procedure that has been altered to perform a new function and must still perform some of the functions for which it was originally designed is: \textit{Answer: d} \hspace{1em} (p. 247)

a. Functional testing.

b. Performance testing.

c. Stress testing.

d. Regression testing.

105. Testing that is normally concerned with conformance to timing, resource usage, or environmental constraints is: \textit{Answer: b} \hspace{1em} (p. 246)

xx. Functional testing.

yy. Performance testing.

zz. Stress testing. Regression testing.

106. The best time to prepare a hardware or electronics equipment test is: \textit{Answer: a} \hspace{1em} (p. 247)

a. During the design phase.

b. After it has been in operation for 6 months.

c. When it is near capacity.

d. Just after repair and maintenance.
107. Attributes of an effective measurement (test) include: Answer: d (p. 248)

   a. Verifiable, measurable, consistent.
   b. Professional, validated, repeatable.
   c. Standardized, audited, validated.
   d. Constant, quantifiable, sensitive to change.

**Short Answer**

6. Why do managers tend to not test their processes and systems?

   *Answer: While routine testing is both time-consuming and costly, testing complex systems can be enormously expensive in terms of time and money. A routine fire evacuation drill in a manufacturing plant, for example, can cause thousands of man-hours lost to production.*

   (p. 247)

7. Testing is the only way the integrity of any system or procedure can be proven or, conversely, system flaws detected before catastrophe strikes. Explain.
Answer: From the standpoint of achieving a totally functional security system, one that can be counted on to work when it is needed, testing of safeguards (countermeasures) in a production environment is probably the critical area that is most likely to be overlooked. This is in sharp contrast to the scientific and engineering fields, where testing is usually taken as an article of faith. People and procedures must be tested in a number of scenarios, and testing, to be effective, must be an ongoing process. Any system that is not periodically tested will eventually fail.

(Ch. 18)

8. How can testing apply equally to persons, systems, procedures, methodologies, and objects?

Answer: All of these elements must operate properly to ensure an adequate system that meets the needs and objectives (protection of assets) of the client or security manager.

(Ch. 18)

9. Correlate the five testing methods according to the best method to use when evaluating security systems.
Answer: Functional testing: a test to determine if a procedure, CCTV, or electronics access control system will do what it was designed to do. A common correlation is a system walk test that will show all sensors are in working order and that they operate within their specification. Safety testing: a test to determine if the object or procedure can be used without causing injury, loss, or harm. It does not have wide application in security systems from the manager’s point of view since all components and systems should have a UL or other safety rating. Performance testing: normally concerned with conformance to timing, resource usage, or environmental constraints (a good example is an anti-intrusion alarm). This can be used to test the operator’s response to system alarms. Stress testing: checks a person’s or object’s tolerance to abuse or misuse under deliberately introduced stress, and also does not have a great deal of application from the security manager’s point of view, as this should be a function of the manufacturer. A manager might want to do this type of testing in a busy, well-used area prior to purchase of a component. Regression testing: usually applies to an object, system, or procedure that has been altered to perform a new function and must still perform some of the functions for which it was originally designed.

(p. 246 and Ch. 18)

10. You have been asked to test the effectiveness of a small- to medium-sized security system. Decide which audit or testing technique you will use and justify your selection over the others.
Answer: The guidelines used in the auditing field are probably the best to use because they can be used as is and will evaluate most all components of the system including managerial performance. Statistical sampling, restricting the value of input parameters or limiting the scope or field of inquiry, and scheduled testing should probably not be used because the size of the system does not require such time and expense tradeoffs. The Safety testing method does not seem to cover managerial issues.

(Ch. 18)

Case Study

As the corporate security manager responsible for the corporate assets protection program, you know that it is imperative that periodic tests are conducted to ensure that the assets are adequately protected. Explain the five basic types of testing that can be used and give an example as to when you would use each of them.

Answer: See pages 246-247 of the text.
Chapter 19: The Security Consultant

Learning Objectives

- Why companies benefit or don’t benefit from using consultants.
- Brief history of consulting.
- How to justify and use consultants.
- Elements of writing proposals.
- Criteria to use to evaluate proposals.

Presentation Outline

I. In-house versus Outside Advice

B. Some companies benefit from outside advice; others do not.
   1. Employees may be resentful and secretive.
   2. First task is to learn the intricacies of the client company’s processes, procedures, and operations.
3. Some managers defend status quo.

4. Salespersons that represent themselves as consultants are under pressure to sell products rather than cost-effective solutions.

5. Use solid business judgment and standards in selecting a security consultant.

C. History of Security Consulting.

1. Origins in the insurance industry.

2. Spurred on by secret defense projects and defense industry just prior to WWII.

3. Original emphasis on perimeter protection, access control, and document classification.

4. Requirements for defense security were contractual in nature.

5. Greatest growth in 1970’s.

6. Design engineering now more common and requires knowledge and education of an experienced consultant.

D. Mistakes can be costly – may be necessary to use team approach.

1. No consultant expert in all security disciplines.

2. Team approach reduces time and expenses.

II. “Why Do I Need Outside Advice?”

A. Consultant can furnish objective opinions without prejudice, internal pressure or politics.

B. Can furnish a second opinion.

C. Loyalty.
III. “How Can I Justify the Cost of a Consultant on a Limited Budget?”

A. Most surveys are a full-time task.
B. Consultants have resources usually not available to the security practitioner.
C. Consultants less limited in scope of knowledge and experience.
D. Most consultants more experienced with finance and negotiation.

IV. “Will an Outside Consultant Provide Assistance in Setting Up the Recommended Program?”

A. The presence of the consultant can materially contribute to the final success of the project.
B. The consultant assists the client by drawing up minimum specifications and requirements.
   1. Consultant can assist the client in reviewing the bids and selecting the best service.
   2. The consultant can inspect, guide, and provide administrative oversight.
   3. The consultant can critique the implementation or installation of the service.
   4. Key role is to function as the client’s representative.

V. Security Proposals (Writing and Costing)
A. A security survey can range from a simple telephone call to a one-day on-site review with verbal conclusions and recommendations, to a full field study.

B. Client and consultant should establish the specifications of the tasks to be performed.

C. Client and consultant must have a basic understanding as to the problem or problems to be solved.

D. Five basic elements are common to proposals are: introduction, proposal, management, cost, and summary.

1. Introduction section identifies the client and the problem in very broad terms.
   a. Also identifies the consultants and the firm that is submitting the proposal.

2. Proposal section must:
   a. Clearly state the need to be fulfilled.
   b. Set forth in specific terms the problem and the proposed manner to solve the problem and meet the client’s needs.
   c. Later serve as a general planning outline for the consultant.
   d. Basic subject areas to develop this part of the proposal include:
      i. Four prime security objectives that will be developed during the evaluation of a facility: the risk assessment, vulnerability assessment, criticality assessment, and the security function.
      ii. Losses.
      iii. Security Organization.
      v. Guard Force.

viii. Utilities.


x. Security Hardware.

xi. Alarm Systems.

xii. Communications.

xiii. Surveillance.

xiv. Security and Fire Safety Hardware.

xv. Procurement.

3. Management section identifies and describes details of the consulting organization, experience, personnel, and references.


   a. Cost figures are the best-guess estimate of the consultant doing the job.

   b. Request for Proposal.

   c. The cost proposal will generally include the following factors:

      i. Direct labor (manpower) cost.

      ii. Travel and expenses.

      iii. Miscellaneous cost, if any.

      iv. Overhead rate (usually in percentage).

      v. General and administration (includes reports).

      vi. Total estimated cost.

      vii. Profit.

      viii. Total proposal cost.
d. Contingency fee, based on the total cost figure for:
   i. Potential delays on site.
   ii. Meetings before, during, and after the on-site work commences.
   iii. Responding to follow-up inquiries after the final report is submitted.
   iv. Other unanticipated cost connected with the project.

5. The summary is used to highlight the details of the proposal. It should:
   a. Contain total cost of the proposed project.
   b. Identify the benefits the survey hopes to accomplish.
   c. Leave the reader with a positive feeling.
   d. Be prepared in a timely, efficient, and professional manner.

VI. Evaluating Proposals and Reports

A. Apply the following criteria to evaluate proposals and reports prepared by consultants:

1. The report (proposal) should fully satisfy the purpose for which the evaluation was made.
2. The objective(s) of the evaluation should be identified and achieved.
3. The scope of the evaluation must be consistent with the purpose and objective(s).
4. The methodology used must be stated and must ensure that all significant information is collected, collated, and analyzed.
5. The documented qualifications of the consultant must be adequate to perform the task.

6. Application of appropriate standards, acceptable practice and/or experience.

7. Credible estimates of comparative risk (probability/time) and potential damage/loss.

8. Recommendations for abatement of risk must be appropriate and effective in regard to priority and cost.

9. Estimated reduction of risk and potential damage.

10. The proposal should set forth a reporting procedure.
Sample Test Questions

True or False

181. The first task of a consultant is to learn the intricacies of the client company’s processes, procedures, and operations.  
   Answer: T (p. 251)

182. Security consulting can trace its origins to the advice and services provided by police department crime prevention units.  
   Answer: F (p. 252)

183. A professional security consultant is expected to be expert in all security disciplines.  
   Answer: F (p. 253)

184. A disadvantage to the team approach is the increase in time and expense.  
   Answer: F (p. 253)

185. The greatest growth in security consulting occurred just prior to WWII.  
   Answer: F (p. 252)

186. Because of the expense involved, consultants are rarely used to provide a second opinion.  
   Answer: F (p. 253)
187. Consultants have resources usually not available to the security practitioner.  

   Answer: T (p. 254)

188. Most consultants are more experienced with finance and negotiation than security managers in general.  

   Answer: T (p. 254)

189. Professional security consultants consider the addition of a 10 percent contingency fee over the total cost of the proposal to be unethical.  

   Answer: F (p. 258)

190. A project reporting procedure is not appropriately disclosed in the proposal. 

   Answer: F (p. 260)

Multiple Choice

108. Which is an example of a difficulty a consultant may face?  

   Answer: d Page (p. 251)

   a. Employees may be resentful and secretive.  
   b. Some managers defend status quo.  
   c. Salespersons that represent themselves as consultants.  
   d. All of the above.
109. To avoid misunderstanding the parameters of the task to be performed: Answer:

a (p. 255)

a. Both client and consultant should establish the specifications at the outset.
b. The consultant should ask for clarification.
c. A professional consultant will know what the client needs.
d. Submit the tasks to your lawyer or legal department.

110. The five basic elements common to most proposals are: Answer: a (p. 255-258)

aaa. Introduction, proposal, management, cost, and summary.
bbb. Scope, qualifications, references, cost, and attachments.

111. The cost proposal will generally include the following factors: Answer: d (p. 258)

a. Direct labor (manpower) cost.
b. Travel and expense.
c. Overhead rate (usually in percentage).
d. All of the above.
112. The original emphasis on security consulting was for: *Answer: d* (p. 252)

a. Perimeter protection.
b. Access control.
d. All of the above.

113. Cost figures are: *Answer: a* (p. 258)

a. The best-guess estimate of the consultant doing the job.
b. Subject to determination by very specific formulas.
c. Not discussed until after the award of the proposal.
d. None of the above.

114. The four prime objectives that will be developed during the evaluation of a facility are: *Answer: b* (p. 256)

a. Current practices, conditions, systems, and recommendations.
c. Utilities, systems, procedures, and policies.
d. Proposal, acceptance, recommendations, and review.
115. RFP means:  \textit{Answer: a (p. 258)}

\begin{itemize}
\item[a.] Request for proposal.
\item[b.] Recommendations from Professionals.
\item[c.] Risk, Frequency, Probability.
\item[d.] Return or Forward Proposal.
\end{itemize}

116. Recommendations for abatement of risk must be appropriate and effective in regard to:  \textit{Answer: a (p. 260)}

\begin{itemize}
\item[kk.] Priority and cost.
\item[l.] Client acceptance.
\item[mm.] Proposal limitations.
\item[nn.] Cost.
\end{itemize}

117. A team approach to consulting:  \textit{Answer: a (p. 253)}

\begin{itemize}
\item[33.] Is sometimes required.
\item[34.] Demonstrates the consultant’s lack of experience.
\item[35.] Is more difficult than herding cats.
\item[36.] Is not accepted well by most clients.
\end{itemize}
Short Answer

1. Discuss how a consultant can help to implement their recommendations.

*Answer:* Consultants can continue to be employed to the extent that they and management feel is necessary to achieve the level of protection necessary to solve the problems identified during the survey. Risk assessment is at best a matter of opinion, with much uncertainty. The continued presence of the consultant with input at the implementation or installation stages can materially contribute to the final success of the project. Once the service is accepted, the consultant can inspect, guide, provide administrative oversight, and critique the implementation or installation of the service.

(p. 254)

2. What can the proposal process demonstrate to the client? What fears may the client maintain as a result of the proposal process?

*Answer:* It should identify the benefits the survey hopes to accomplish in terms that even the most recalcitrant, bottom line–oriented, bean-counting executive can understand. It must leave the reader with the positive feeling of having just read a proposal prepared in a timely, efficient, and professional manner. A late, poorly prepared, and disjointed proposal is a reflection of what the future holds regarding
the primary task. Don’t expect more or less from a consultant’s proposal than you would expect to receive for the principal task.

(p. 258)

3. Justify the need to use outside advice (consultants):

*Answer:* Companies have benefited from the experience and knowledge that consultants can bring to bear on problems encountered during surveys. Using the team approach to consulting assignments can reduce time and expenses for most large projects. Often it is the only way some large projects can be adequately handled, because of the many specialty areas encountered in these environments. An independent consultant can furnish objective opinions without prejudice and without regard to internal pressures or politics. The outside consultant furnishes a “second opinion” that reinforces the initial opinion, especially regarding cost-effective solutions to complicated problems. Assuming that the in-house professionals are fully employed at their day-to-day occupations, they may not find the time to conduct a meaningful audit or survey. Professional consultants usually have available to them library and research assistance unavailable to the average security practitioner. Few security professionals have developed the depth of knowledge necessary to do risk assessment in a multi-disciplined environment. An outside consultant can also discern the financial aspects of the necessary manpower and hardware solutions and then negotiate these cost factors with management. Not
every in-house security professional is schooled in the financial and negotiating
techniques necessary to sell program changes. Most consultants are.

(Ch. 19, mostly pages 253-254)

4. The XYZ Corporation has sent you a RFP to test the operation of their newly installed
alarm and access control system at their National City facilities. National City is a 4-hour
airplane flight away from your location. The RFP contains a list of specific items to
check; they anticipate this will require about 4 hours of your time. They are also
requesting a written report of your findings and recommendations. Your billing rate for
this type of work is $125.00 per hour. Write your proposal to XYZ to complete this
project.

Answer: The proposal should contain at least the following elements:

- An introduction that identifies the client and the problem in very broad
terms. It also identifies the consultants and the firm that is submitting the
proposal.

- Proposal section that clearly state the need to be fulfilled, most often
expressing it as a statement of work or scope. It sets forth in very specific
terms both the problem and the proposed review or study that will be
undertaken to gather the data necessary to solve the problem and meet the
client’s needs. It will also later serve as a general planning outline for the consultant doing the work.

- Management section of the proposal that will identify and describe the consulting organization, its experience, its personnel, a sampling of client companies that may be used as references. In any event, management, administration resources, and capabilities should be spelled out in some detail and should fully qualify the consultant and firm for the task at hand. Usually included in this part of the proposal are biographical sketches of the consultants who will actually be performing the survey.

- Costs. While the text includes: Direct labor (manpower) cost, Travel and expenses, Miscellaneous cost, if any, Overhead rate (usually in percentage), General and administration (includes reports), Total estimated cost, Profit and Total proposal cost, we are accepting a simple cost structure in the response. The cost should include 8 hours of travel, hotel and meals (or a per diem), 8 hours of consulting (4 hours inspection, 2-4 hours meetings, misc.), and the 2:1 ratio of report time to site hours. A 10 percent contingency fee should be added. This totals and should be listed as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Hours</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site visit and inspection</td>
<td>8</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Report and Recommendations</td>
<td>16</td>
<td>$2,000.00</td>
</tr>
<tr>
<td>Travel</td>
<td>8</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Per Diem (Meals, hotel, misc.)</td>
<td>1 day</td>
<td>$130.00</td>
</tr>
</tbody>
</table>
Sub Total: $ 4,130.00

Contingency $ 413.00

Total $ 4,543.00

The per diem was derived from the text, but is obviously higher than the amount appropriate at the publish date.

- Summary of the report and costs.

You may note that we did not include the cost of a preliminary survey in the calculation.

(p. 254-258)

5. Evaluate the proposal submitted by one other student in response to the above RFP.

*Answer:* The instructor should consider removing identifying material (student name etc, substituting a number or other identifier). The evaluation should consider the following criteria:

- The proposal should fully satisfy the purpose for which the evaluation was
made.

- The objective(s) of the evaluation should be identified and achieved.
- The scope of the evaluation must be consistent with the purpose and objective(s).
- The methodology used must be stated and must ensure that all significant information is collected, collated, and analyzed.
- The documented qualifications of the consultant must be adequate to perform the task.
- Costs and time are appropriate.
- Meets the elements for the answer to number 4 above.

(p. 254 – 260)

Note: An alternate question may involve the distribution of three of the proposals produced in question #4 with the instruction to the students to act as the security manager of XYZ Corporation and select the consultant they would use for the project. They must justify their selection over the other two.

Case Study

As a corporate security manager, you may not have experienced or sufficient staff to perform a security function (e.g., risk analysis or other needed security task). You have contemplated
hiring a security consultant. As the corporate security manager, explain the process you would go through in making a determination as to whether or not to hire a security consultant.

**Note:** Your answer should include, as a minimum, a discussion about:

- In-house versus outside advice.
- An explanation that you can provide to your boss as to why you need an outside security consultant.
- How to justify the costs of a security consultant.
- What you expect from the security consultant.

**Answer:** See pages 251-255 of the text.