

# CRM | CONTROL OF RISK

L E A R N I N G   G U I D E



**RISK & INSURANCE**  
EDUCATION ALLIANCE





# Control of Risk

---

## THE CERTIFIED RISK MANAGER PROGRAM

Principles of Risk Management

Analysis of Risk

Control of Risk

Financing of Risk

Practice of Risk Management

Risk & Insurance Education Alliance

© 2024 by Risk & Insurance Education Alliance

Published in the United States by

Risk & Insurance Education Alliance

P.O. Box 27027

Austin, Texas 78755-2027

**Telephones: 512.345.7932**

**800.633.2165**

[RiskEducation.org](http://RiskEducation.org)

Disclaimer:

This publication is intended for general use and may not apply to every professional situation. For any legal and/or tax-related issues, consult with competent counsel or advisors in the appropriate jurisdiction or location.

Risk & Insurance Education Alliance and any organization for which this seminar is conducted shall have neither liability nor responsibility to any person or entity with respect to any loss or damage alleged to be caused directly or indirectly as a result of the information contained in this publication.

Insurance policy forms, clauses, rules, court decisions, and laws constantly change. Policy forms and underwriting rules vary across companies.

The use of this publication or its contents is prohibited without the express permission of Risk & Insurance Education Alliance.

# Contents

---

A Letter from William J. Hold, President/CEO .....	vi
To the Participant.....	vii
Program Overview .....	viii
How to Use This Learning Guide.....	xi

## **Section 1: Risk Management Concepts.....1**

What is Risk? .....	2
Key Risk Management Terms .....	4
The Steps of the Risk Management Process .....	7
The Impacts of an Effective Risk Management Program.....	20
Total Cost of Risk (TCOR) .....	24
Summary.....	28
Section 1 Self-Quiz.....	29
Set Yourself Up for Success! .....	32

## **Section 2: Risk Control and Mitigation – Human Resources.... 33**

Introduction .....	34
The Purpose of Risk Control .....	34
The Root Causes of Accidents and Injuries.....	37
Accident Prevention.....	40
Safety and Health Programs.....	44
Ergonomics .....	60
Manual Material Handling.....	67
Substance Abuse in the Workplace .....	73
Workplace Violence.....	79
Summary.....	84
Section 2 Self-Quiz.....	85
Set Yourself Up for Success! .....	88

**Section 3: Risk Control and Mitigation –  
Property and Liability .....89**

Employment Practices Liability Exposures ..... 90

Fleet Hazards and Controls .....104

Property Exposures and Hazard Control Programs ..... 113

E-Business and Cyber Activity..... 118

Cyber Risk Exposures.....121

Contractual Risk Transfer ..... 131

Summary..... 138

Section 3 Self-Quiz..... 139

Set Yourself Up for Success! ..... 143

**Section 4: Crisis and Disaster Planning ..... 145**

Defining Crises and Other Key Terms .....146

Crisis Management, Business Continuity, and Disaster Recovery..... 151

Crisis Management Goals and Principles ..... 155

Crisis Management.....158

Reputation Management During a Crisis..... 174

Summary..... 182

Practical Exercise ..... 183

Section 4 Self-Quiz..... 189

Set Yourself Up for Success! ..... 192

**Section 5: Claims Management ..... 193**

Defining Claims Management ..... 194

The Claims Management Process.....200

Evaluation .....203

Types of Claims Management Plans.....218

Claims Audits.....230

Third-Party Administration (TPA) Selection..... 235

Selecting Defense Counsel ..... 243

Summary.....	247
Section 5 Self-Quiz.....	248
Set Yourself Up for Success! .....	252

<b>Appendix.....</b>	<b>253</b>
Preparing for the Final Exam.....	253
Glossary of Terms.....	255

## A Letter from William J. Hold, President/CEO

I trust this Learning Guide finds you well and eager to embark on a transformative journey with our esteemed risk management and insurance courses. As the President of Risk & Insurance Education Alliance, it is both an honor and a privilege to welcome you to this unparalleled learning experience.

In our ever-evolving world, the importance of risk management and insurance cannot be overstated. This industry is the backbone of organizational resilience, ensuring that businesses and individuals can navigate the complexities of today's dynamic landscape. I commend you for recognizing the significance of this expertise and taking the initiative to invest in your professional development.

At Risk & Insurance Education Alliance, our philosophy revolves around the belief that every individual has untapped potential waiting to be realized. This course is not just about acquiring knowledge; it is a platform for you to own your potential. We are here to guide, support, and empower you to discover the depths of your capabilities, enabling you to excel in the realm of risk management and insurance.

As committed professionals, you are not merely participants in a course; you are integral members of a community dedicated to excellence. Our team of expert instructors, industry practitioners, and support staff are equally committed to your success. Throughout the program, you will benefit from their wealth of experience and knowledge, gaining insights that extend beyond textbooks to real-world applications.

"Own Your Potential" encapsulates the ethos of our educational approach. It encourages you to take charge of your learning journey, embrace challenges as opportunities, and emerge as a confident and proficient risk management and insurance practitioner.

As you embark on this course, remember that your commitment to professionalism sets you apart. The skills and insights you gain here will not only elevate your individual career but contribute to the advancement of the entire profession.

I am confident that, armed with the knowledge and skills imparted in this course, you will become a committed professional who not only understands the intricacies of risk management and insurance but also actively shapes the future of these industries.

I look forward to witnessing your growth, learning, and success in the coming weeks. The journey ahead is both challenging and rewarding, and I encourage you to embrace it with enthusiasm and dedication.

Best wishes for a fulfilling and transformative learning experience.

Sincerely,



William J. Hold, M.B.A., CRM, CISR

President/CEO

# To the Participant

Welcome to Control of Risk, part of the Certified Risk Manager designation program. This program will provide you with the core knowledge and tools you need to support your clients with analysis of their business risks and forecasting future losses. A Certified Risk Manager (CRM) is recognized as someone capable of analyzing risks, policies, forms, and claims data and communicating that understanding clearly to clients, carriers, and colleagues.

As a participant in Risk & Insurance Education Alliance (RIEA) program of study, it is expected that you will not only gain knowledge that will give you greater success in your work, but that you will be challenged to make Risk & Insurance Education Alliance's core values of integrity, innovation, inspiration, and imagination part of your daily practice. As experts in their fields, RIEA faculty, consultants, and academic directors—each with a commitment to assisting you in your efforts to achieve standards of excellence—have contributed to the content of this course. In this course, you can expect:

- engagement in the learning process
- clear learning objectives supported by essential content
- activities designed to strengthen understanding
- exposure to real-world examples and contexts

As representatives of Risk & Insurance Education Alliance (RIEA), we take great pleasure in welcoming you to this program and to our organization. We are committed to helping you become a successful Certified Risk Manager.

# Program Overview

This program overview provides an at-a-glance view of the contents of this Learning Guide. Here you will find section goals as well as specific learning objectives for every section.

## Section 1: Risk Management Concepts

### Section Goal

In this section, you will be introduced to common terminology used in discussions of risk management. In addition to becoming familiar with key terms and concepts, you will identify the five steps of the risk management process and describe how those steps help build a comprehensive risk management program.

### Learning Objectives:

- 1.1 Define risk, including the distinction between pure and speculative risk.*
- 1.2 Define other key risk management terms.*
- 1.3 Explain risk management and the five steps of the risk management process.*
- 1.4 Apply the five techniques of risk control to a given scenario.*
- 1.5 Describe the impacts of an effective risk management program.*
- 1.6 Describe the components and uses of Total Cost of Risk (TCOR).*

## Section 2: Risk Control and Mitigation – Human Resources

The goal of this section is to provide you with a review of risk control, including the purpose and importance of risk control for organizations. Insight into and information about the various exposures that can be found in the human resources general classification of risk are discussed along with appropriate risk control measures.

- 2.1 Describe why organizations should focus on risk control and the importance of involving all members of an organization in the risk control process.*
- 2.2 List the root causes of accidents and injuries.*
- 2.3 Apply the six basic steps of accident prevention.*
- 2.4 Develop recommendations for a health and safety program based on the eight elements of an effective program.*



- 2.5 Define the term “ergonomics” and describe the risk control methods associated with ergonomic issues.*
- 2.6 Identify the risk factors and risk control measures associated with manual material handling and lifting.*
- 2.7 Describe the benefits and possible legal problems associated with a workplace substance abuse program.*
- 2.8 Name the risk factors and risk control measures used to prevent or reduce workplace violence.*

### **Section 3: Risk Control and Mitigation – Property and Liability**

In this section, you will learn about the various property and liability exposures organizations face and explore risk control methods to mitigate and address these concerns.

- 3.1 List the common sources of employment practices liability exposures and the risk control measures used to address those exposures.*
- 3.2 Apply risk control measures to the common types of fleet exposures and hazards.*
- 3.3 Define key property exposure terms and describe the corresponding property hazard control programs.*
- 3.4 Explain the common cyber exposures faced by businesses and the risk control methods that could mitigate those risks.*
- 3.5 Describe the four types of contractual risk transfers and the three types of hold harmless agreements.*

### **Section 4: Crisis and Disaster Planning**

This section focuses on how a crisis or disaster can arise and its potential impact on the operations and livelihood of an organization. Crisis and disaster planning techniques and the four phases of crisis management will be explored. In addition, best practices in crisis communications are reviewed.

- 4.1 Define a crisis, its characteristics, its phases, and the potential impacts it may have on an organization.*
- 4.2 Describe the terms crisis management, business continuity, and disaster recovery, and explain the relationship between the three terms.*
- 4.3 Describe the principles of an effective crisis management program, including general crisis management goals.*

- 4.4 *Explain the four essential steps of the crisis management process.*
- 4.5 *Describe the important considerations of reputation management during a crisis.*
- 4.6 *Use the principles of crisis management to respond to a hypothetical crisis scenario.*

## **Section 5: Claims Management**

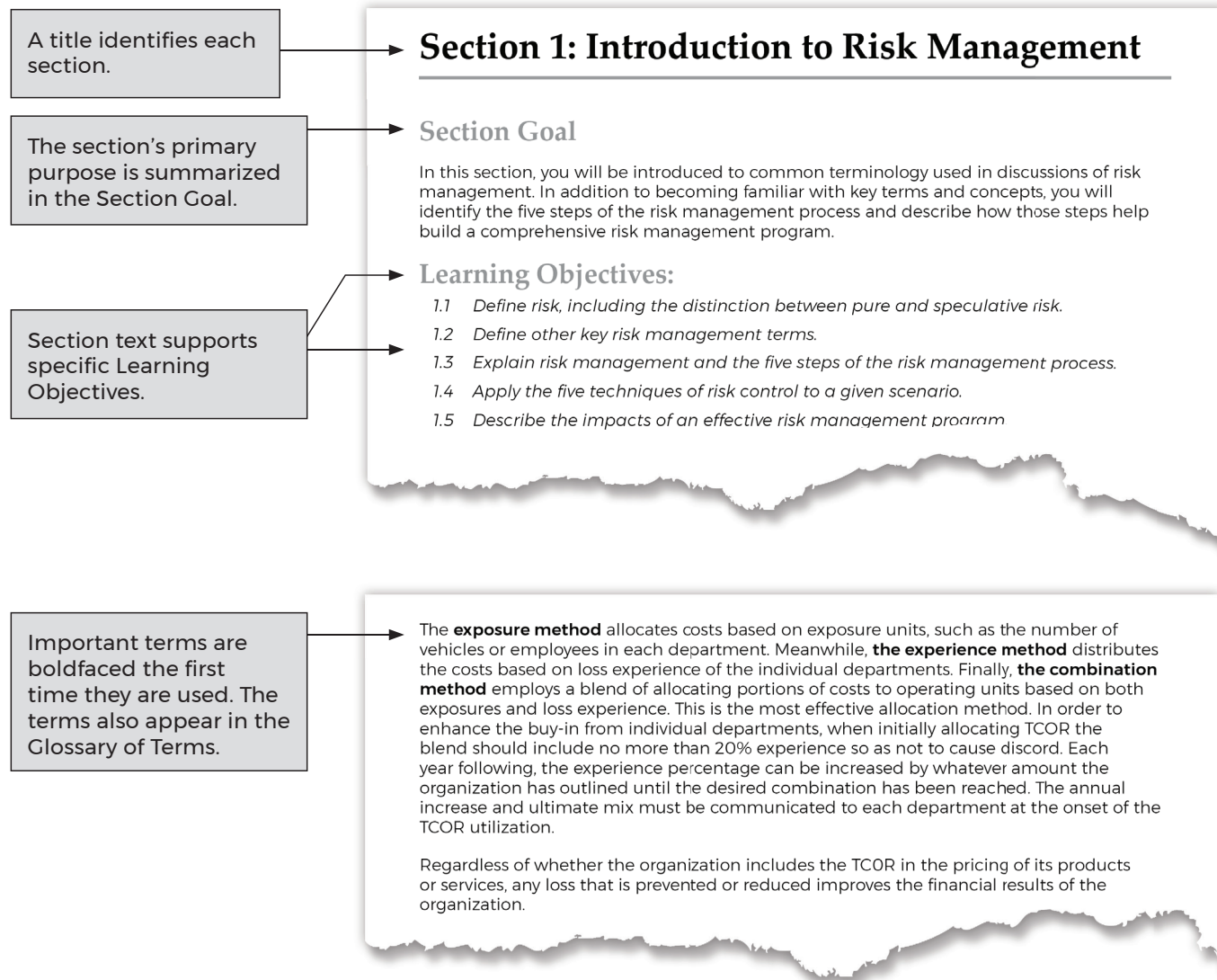
In this section, you will learn about one of the risk manager's key responsibilities—the process of managing claims. In addition, alternative dispute resolution (ADR) will be discussed as an alternative to litigation. Finally, the considerations that should be made when selecting a third-party claims administrator and defense counsel will be reviewed.

- 5.1 *Describe claims management and how it supports the risk control program.*
- 5.2 *Describe the actions and considerations for the investigation phase of the claims management process.*
- 5.3 *Explain the evaluation step of the claims management process, including how damages and reserves can be calculated and set.*
- 5.4 *Discuss the resolution step of the claims management process, including the four types of alternative dispute resolution (ADR) methods.*
- 5.5 *Analyze the three types of claims management plans and the considerations that should be made when selecting a plan.*
- 5.6 *Describe the components, requirements, and possible findings of a claims audit.*
- 5.7 *Explain the role of a third-party administrator (TPA) and the major considerations of the selection process.*
- 5.8 *Explain the considerations when selecting defense counsel for an organization.*

# How to Use This Learning Guide

The Learning Guide you are using in this course is like all the learning materials published by Risk & Insurance Education Alliance; it has been written and authenticated by industry experts.

Each section in this learning guide shares the same features.



expected to occur, will determine the number assigned. The higher the assigned number, the greater the impact or likelihood of an event. Each risk is plotted on the map based on the assigned value, which assists an organization with risk prioritization.

### Heat Map Risk Matrix



Visuals such as diagrams, graphs, and tables support the text.

### Summary

Individuals and organizations set goals for their futures, and effectively predicting, preparing for, and managing risks can help them to achieve these goals. While risk may be inevitable, it is manageable with assistance from insurance and risk management professionals who thoroughly understand the terminology, forms of risk, and steps or actions their clients can take to avoid or minimize financial loss.



Each section concludes with a summary.

Examples describe real-world-style scenarios to enhance your understanding of the concepts presented.

- Severity** – Severity is the dollar amount of a single loss or the total value of all losses in a given time period.



For an insurance company, the total dollar amount of homeowners insurance claims in a single year is an example of severity, while the total number of homeowners claims is an example of frequency.

- Expected Losses** – Expected losses describes a prediction of the frequency and severity of losses based upon loss history distributions and statistics.
- Risk Appetite** – Risk appetite refers to an organization's willingness to accept or tolerate risk.
- Risk-Taking Ability** – Risk-taking ability is an organization's financial capacity for assuming risk.

Check-Ins and Knowledge Checks help you test your understanding before moving forward.

### Check-In



Richard is a welder in an equipment manufacturing facility. One day, he sees the CEO walking on the work floor without a hard hat or safety glasses. Richard promptly turns off and puts down his torch and walks over to the CEO and reminds him that he must follow the safety rules which are established for all employees. Which element of the safety program made Richard comfortable in correcting his CEO?

- ☐ Management Leadership
- ☐ Accountability, Responsibility, and Authority
- ☐ Employee Participation
- ☐ Hazard Assessment and Control

### Element 5 – Employee Information and Training



Employees need to know they are responsible for their own health and safety program, and they need the information necessary to fulfill their responsibilities with

### Knowledge Check



**Directions:** Respond to the question below.



Mr. Smith operates a local bakery. Historically, his business has not offered delivery services. With the hope of increasing his revenue, he hires two part-time delivery drivers and purchases two vans. Explain the speculative risk and at least one pure risk associated with his decision.

**Speculative Risk:**

Each section closes with a quiz to help you assess your learning.

## Section 2 Self-Quiz

**Directions:** Select the best answer for each of the following questions.

1. Why is it important to involve all members of an organization in the risk control process?
  - ☐ Lack of employee involvement in a safety program can upset shareholders.
  - ☐ Employee involvement in safety decisions is a legal requirement.
  - ☐ Individual employees are needed to help identify unsafe behaviors and hazards.
  - ☐ Employees should be involved only because their involvement boosts workplace morale.

A Glossary of Terms puts the Learning Guide's special vocabulary in one, easy-to-use location.

## Glossary of Terms

### Section 1: Introduction to Risk Management

**accident** - an unexpected and unintentional event that tends to result in damage or injury

**avoidance** - eliminating an activity or exposure, thereby removing the chance of a loss

**claim** - a demand for payment or an obligation to pay as the result of a loss. Claims can be paid by the insurance company or an individual/organization.

**duplication** - a risk control technique that aims to reduce the overall severity of a loss by using back-ups for critical systems or operations

# Section 1: Risk Management Concepts

---

## Section Goal

In this section, you will be introduced to common terminology used in discussions of risk management. In addition to becoming familiar with key terms and concepts, you will identify the five steps of the risk management process and describe how those steps help build a comprehensive risk management program.

## Learning Objectives:

- 1.1 Define risk, including the distinction between pure and speculative risk.
- 1.2 Define other key risk management terms.
- 1.3 Explain risk management and the five steps of the risk management process.
- 1.4 Apply the five techniques of risk control to a given scenario.
- 1.5 Describe the impacts of an effective risk management program.
- 1.6 Describe the components and uses of Total Cost of Risk (TCOR).

Risk (and risk management) is inherent to everyday life. It presents itself in every activity and decision and is continually evolving as circumstances in the world change. On a personal level, there are risks associated with many common decisions:

- An employee may be considering changing professions. Although they would take a pay cut in the short term, the change would increase their future earning potential.
- A frequent driver ponders whether purchasing an expensive electric vehicle would be a sound financial investment due to rising fuel costs.



In each of these situations, the individual is considering the circumstances surrounding the decision. They identify and analyze available facts so they may manage and control their own risks and feel comfortable moving forward.

On a business level, organizations face uncertainty concerning the risks and losses that affect their operations. They may face potential losses to buildings and property due to fire, theft, natural disasters, and even global political circumstances. Other losses can stem from personnel issues within the organization itself.

Resignation, disability, or death of essential employees can have cascading impacts on a company. Risk management exists to support an organization in moving forward with a particular strategy, project, decision, or activity. This occurs through a systematic process





## Section 1: Risk Management Concepts

targeted at mitigating the impact of events that might otherwise impede the organization's strategy. Consider the following scenario:



Wilson Widgets (WW) suspects that the cost of a rare earth metal it uses in manufacturing will increase significantly due to military conflict in its primary sourcing country. Since it has the financial ability to do so, WW chooses to stockpile large amounts of this key raw material to avoid losses due to supply chain shortages and the increasing cost of raw materials. In the long run, WW has had a successful fiscal year as it is one of the few manufacturers in its industry not to experience significant disruptions due to the shortage.

Risk management is the best way for businesses to internally control costs to increase profits. It should be employed by organizations of all shapes and sizes operating in all stages of life across all industries. Risk & Insurance Education Alliance's CRM (Certified Risk Manager) program is designed to provide you with the tools to apply this vital process to any type of organization.

# What is Risk?

## Learning Objective:

1.1 Define risk, including the distinction between pure and speculative risk.

In the risk management arena (including the insurance world), risk is defined differently depending on an individual's job function or area of expertise. To an underwriter, the risk is the entity or person being insured. To some agents or brokers, the risk may be the insured or the **exposure**, such as a building or vehicle. Alternatively, the risk could be a **peril** (wind, fire, etc.) or a **hazard**, such as poor safety standards on a construction site.



- In risk management, several definitions of risk are used, each for a specific purpose. **Risk**, as defined for the purpose of this course, is **the possibility of a positive or negative outcome arising from a given set of circumstances**. Risk can be further divided into two broad categories: pure risk and speculative risk.

## Pure Risk

**Pure risk** involves a situation whose only outcome can either be loss or no loss. Pure risks include threats to property and people, as well as liability for injuries to others. Insurance usually addresses pure risk.

Examples of pure risk include:

- The possibility of Peter having an auto accident on the way to work; either Peter will be in an accident, or he won't.
- The possibility of lightning striking a building and resulting in a fire loss





## Speculative Risk

Like pure risk, **speculative risk** presents the possibility of loss or no loss. However, it also presents the chance of a gain. This combination of both positive and negative uncertainty reflects the full definition of risk.

- Speculative risk is usually associated with business or financial risk. For example, speculative risk includes positive and negative changes in a company's stock value and positive and negative changes in a market that affect the demand for a company's manufactured goods. Speculative risk is also considered when determining if an organization should develop a new product or service, utilize/create new technology, alter its strategic direction, adjust its supply chain, and any other decision that creates, enhances, and/or supports its competitive advantage.



Examples of speculative risk include:

- Launching a new formulation of an existing product with the hope that it will draw greater market share
- Locking in a mortgage rate with the hope that rates won't go lower

## ►► Knowledge Check



**Directions:** Respond to the question below.



Mr. Smith operates a local bakery. Historically, his business has not offered delivery services. With the hope of increasing his revenue, he hires two part-time delivery drivers and purchases two vans. Explain the speculative risk and at least one pure risk associated with his decision.

**Speculative Risk:**

---

**Pure Risk:**

---

# Key Risk Management Terms

## Learning Objective:

### 1.2 Define other key risk management terms.



Individuals within every industry or profession share a special vocabulary or jargon. A clear grasp of this vocabulary allows for effective communication. There are 13 critical terms common to the insurance and risk management industry. Developing a solid understanding of these terms gives insurance and risk management professionals the foundation they require to work successfully with clients and insurance companies. A key skill employed by successful risk managers is the ability to communicate effectively while also translating these concepts to the client in practical terms that can be easily understood.

1. **Loss** – Loss is a decrease in the value of an asset (valuable property owned by a person or company). Losses include physical property damage, such as a fire damaging a home, or injury to an employee or customer. Here’s an example:



Ezekiel delivers hardware using a company truck. While working, an ice storm causes him to crash into a barrier. The truck requires repair, and Ezekiel is taken to a hospital, where it is discovered that he has fractured his right leg.



What kind of losses have occurred? Injury to Ezekiel and the physical property damage to the barrier and truck have certainly occurred. Losses can also be indirect. For example, it is possible that since Ezekiel can’t make deliveries, his revenue will be reduced, and/or he may have to hire a driver at additional expense.

2. **Exposure** – Exposure is a situation, practice, or condition that may lead to a loss. Activities, resources, and assets are also viewed as exposures.



Consider a restaurant. The building is an asset that is susceptible to various exposures for the owner, like damage from perils such as a fire or a windstorm. What other types of exposures could be found in a restaurant? Bodily injury to employees and customers could occur due to perils such as food poisoning of customers, knife cuts to chefs, and customers falling on slippery surfaces.

3. **Peril** – Peril is the cause of loss—why it happened. Examples of perils include fire, lightning, auto accidents, theft, heavy snow, hurricanes, and tornadoes.
4. **Hazard** – Hazard is a condition or circumstance that makes a loss from a given peril more likely or more severe. Think, for example, of storing cardboard boxes up against the furnace in the storeroom. The choice of storage location is a hazard that increases the likelihood of the peril of fire.



## Section 1: Risk Management Concepts

5. **Incident** – An incident is an unplanned event that may lead to a loss or a claim. For example, George is rushing to get to a meeting and bumps into a desk. He stumbles but does not fall or sustain injury.
6. **Accident** – An accident is an unexpected and unintentional event that tends to result in damage or injury. An accident always occurs at a specific time and place. In the example above, if George falls and is injured because he bumped into the desk, it is an accident. Similarly, if his back starts to hurt later in the day, the stumble becomes an occurrence.
7. **Occurrence** – An occurrence is an accident without the time constraint; it happens over an extended period of time. For example, consider occupational injuries. An employee who typically lifts heavy boxes throughout the day may suffer back strain. There is no specific date and time that the injury occurred. These types of injuries are often described as cumulative—building over time. 
8. **Claim** – A claim is a demand for payment or an obligation to pay—whether paid by the insurance company or an individual or organization—as the result of a loss. Most people are familiar with the concept of a claim. Some examples are auto accident claims and property insurance claims (fire, lightning damage, etc.)
9. **Frequency** – Frequency describes the number of incidents, accidents, occurrences, or claims in a given time period, usually a policy year or calendar year.
10. **Severity** – Severity is the dollar amount of a single loss or the total value of all losses in a given time period. 

For an insurance company, the total dollar amount of homeowners insurance claims in a single year is an example of severity, while the total number of homeowners claims is an example of frequency.
11. **Expected Losses** – Expected losses describes a prediction of the frequency and severity of losses based upon loss history distributions and statistics.
12. **Risk Appetite** – Risk appetite refers to an organization's willingness to accept or tolerate risk.
13. **Risk-Taking Ability** – Risk-taking ability is an organization's financial capacity for assuming risk.



## Knowledge Check



**Directions:** Respond to the questions below.

1. Phillip's company owns an old office building in Memphis, TN. The risk manager has been lobbying for retrofitting the structure to withstand potential perils. He explains that the building sits on the New Madrid Fault Line. Identify the exposure, peril, and hazard the risk manager is concerned about.

---

---

---

2. Callie works on a manufacturing line assembling small tools. Her wrists are often sore by the end of the day. Callie goes to a doctor, who advises her that she has a work-related injury. Callie reports this to her supervisor. Which risk management terms are applicable?

---

---

---

With a clear understanding of risk and its technical language comes the ability to examine risk management. As mentioned previously, everyone is a risk manager to some degree. Individuals attempt to avoid accidents and injuries where possible and take steps to preserve their assets. In the same way, businesses take specific steps through various risk management efforts to reduce their potential for losses.

# The Steps of the Risk Management Process

## Learning Objective:

1.3 Explain risk management and the five steps of the risk management process.

**Risk management** describes the process of implementing actions that reduce or eliminate the likelihood of a loss that would affect an individual or organization's assets, profitability, or objectives. Every industry faces risk and has opportunities to manage those risks. For example, the costs associated with workers compensation losses can be managed. In this case, a risk manager would employ strategies and procedures to prevent and reduce the number of workplace accidents and the impact those accidents have on employees. This could be accomplished through the **risk management process**.



## The Five Steps of the Risk Management Process

The risk management process consists of five steps, and each step is necessary for a risk management program to be effective. The five steps are:

1. **Risk Identification**
2. **Risk Analysis**
3. **Risk Control**
4. **Risk Financing**
5. **Risk Administration**

This section will examine each step in the process separately. The process is best imagined as a cycle, as risks constantly evolve and emerge as companies expand or venture into new markets. Every major change within an organization brings the possibility of new and additional risks. The graphic that follows demonstrates the continuous cycle of risk management.



## Step 1. Risk Identification



The first and most important step in the risk management process is **Risk Identification**, during which a risk manager identifies and examines all an organization's exposures, perils, and hazards. The identification process could also include some of the following considerations:

- The economic climate an organization operates in, such as market trends and the status of its competitors
- An organization's strategic objectives
- An organization's internal governing principles such as risk appetite, risk ability, and desired reputation

A failure to identify exposures can subject organizations to negative financial consequences. Consider the following scenario:



Don manages a manufacturing plant where employees frequently use heavy machinery. Failure to identify the dangers inherent in operating a piece of heavy machinery could result in not having insurance for an injury stemming from operating the equipment. If this were to occur, Don would be responsible for paying for the claim with his own financial resources.





A software company stores its information on an internal server. Failure to identify the exposure and potential losses from a power outage could result in data loss, crippled operations, and immense costs.

In both cases, failure to identify risks results in unplanned losses. These losses are the most dangerous as they must still be paid, ultimately at the expense of the budget. Without proper identification, risks cannot be analyzed, controlled, financed, or administered.

There are several ways risk managers can identify risks. One way is to make a physical inspection by walking around the premises to determine if everything is in order and safe. Another way to identify risks is to look to the past. While the past is not always a predictor of the future, a risk manager can get a sense of what losses might occur and how an organization can plan accordingly.

## Step 2. Risk Analysis

Once risks are identified, they can be analyzed to assess the potential impact exposures may have on an organization. **Risk Analysis** provides the information that enables an organization to make decisions about how risks can be controlled or financed. There are two broad forms of risk analysis: quantitative and qualitative.



### Qualitative Risk Analysis

Not all information is easily translated into mathematical measurements. **Qualitative risk analysis** is used to examine possible risks and how they might impact an organization. For example:



A manufacturer of athletic wear is picking a new celebrity spokesperson. Bad behavior on the part of the celebrity can negatively impact the company's reputation and harm sales. The impact is not measurable, but the exposure is there.

In this case, the risk manager could send surveys to internal personnel to understand the potential impact of an adverse event related to the celebrity. Ultimately, this information would be used to address two critical questions:

- Should we implement this course of action?
- What potential impact will that have?

### Quantitative Risk Analysis

A risk manager undertaking **quantitative risk analysis** uses numerical values to predict the likelihood and severity of a risk. One benefit of quantitative analysis is that since it relies on concrete numerical data, it can be easier to compute and interpret than more abstract risk measures. There are several acceptable methods for calculating the statistical and financial impacts of risk. These methods include loss projections or forecasts, cost-benefit analyses, and total cost of risk calculations and analyses. Review the following example of a **cost-benefit analysis**:

## Section 1: Risk Management Concepts



A hospital is considering the purchase of equipment to lift and transfer patients at a cost of \$100,000. The risk manager believes this will reduce the cost of workers compensation claims for back injuries. The risk manager can consider how long the equipment typically lasts before needing to be replaced and determine the reduction in claims the hospital would need to achieve to make the purchase worthwhile. The risk manager is weighing the cost of the equipment against the potential benefit (a reduction in claims).

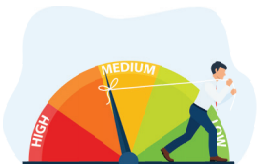


Qualitative and quantitative analyses work together to predict risk. Risk managers use qualitative measurements to understand risk and quantitative measurements to assign value to them. The challenge for the risk manager and the organization is that no clear-cut “right” answer exists. The course of action taken often depends on many variables, including the risk appetite of the organization, the financial capability of the organization, the credibility and quality of the data utilized, and the social responsibility of the company.

### Step 3. Risk Control

#### Learning Objective:

1.4 Apply the five techniques of risk control to a given scenario.



The third step in the risk management process includes any action to minimize the probability, frequency, severity, or unpredictability of a loss. **Risk control** is a people process, and all parts of an organization must be involved in a risk control program for it to be effective.

#### General Theories on How Losses Are Caused

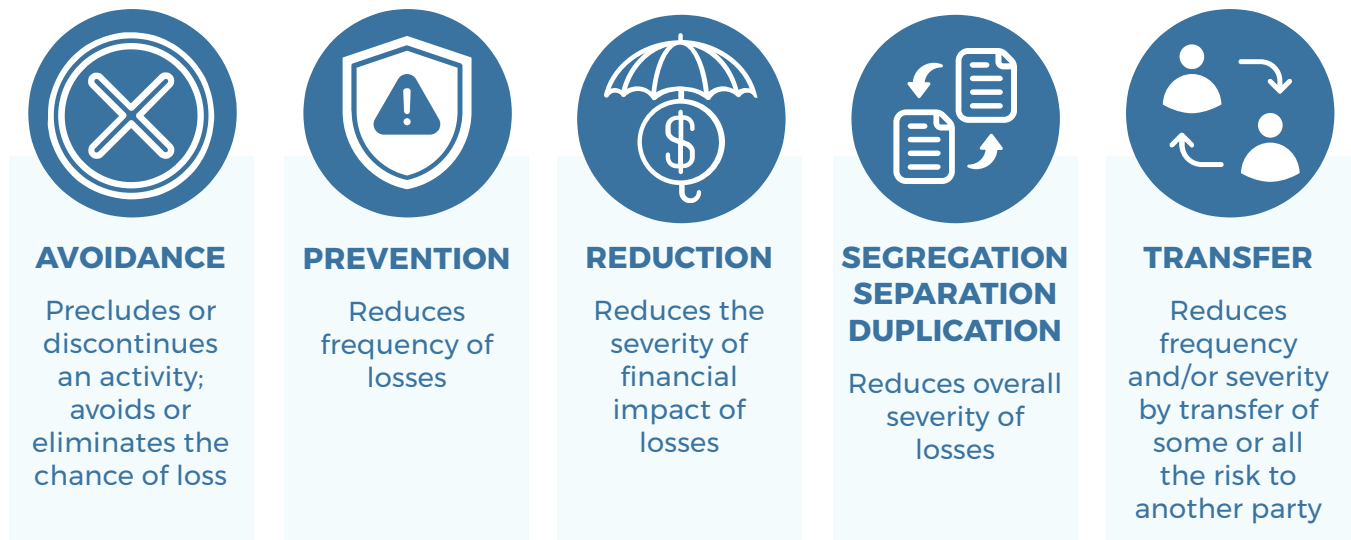
This section focuses on three theories that attempt to explain how losses are caused. These three theories include:

- **The Human Approach:** This view states that accidents occur because of negligence or the deliberate acts of a person. In this case, risk control measures attempt to change employee behavior.
- **The Engineering Approach:** This view is based on the concept that objects cause accidents, such as a piece of malfunctioning equipment injuring an employee. Risk control in this approach would focus on improving the safety of the equipment that is used.
- **The Systems Approach:** This final approach emphasizes the role that internal system failures or weaknesses play a part in the occurrence of accidents. Failure to monitor or implement correct policies and procedures, as well as negligent supervision, are viewed as the causes of loss. Here, risk control measures would modify internal processes to reduce accidents.



## Five Techniques of Risk Control

A risk manager has a variety of risk control methods available. Often, more than one may be used to address a particular category of loss. The following graphic summarizes how the various techniques can be used to control risk.



The following pages will discuss each technique of risk control in more detail.

### Avoidance

**Avoidance** eliminates an activity or exposure, thereby removing the chance of a loss.



Fun Toys Manufacturer sells a popular brand of children's toys. It is discovered that a toxic chemical was used in the toys that resulted in several children falling ill. The manufacturer discontinued the sale of the product.

In this example, avoidance may not totally control exposure to loss as the discontinued product is still in the hands of consumers. Even if they recall and stop the sale of the toy, the product could still result in damages for which the company is ultimately held liable.

Another limitation of the avoidance technique of risk control is that it may be difficult to sell to management for several reasons:

1. Entirely avoiding the risky activity may conflict with an organization's goals and profit motives.
2. The risky activity may be inherent to the organization's identity or mission.
3. The risk manager may lack the appropriate decision-making authority to discontinue the risky activity.

Consequently, avoidance may not always be the most viable or readily available risk control technique.

### Prevention

**Prevention** attempts to reduce the frequency of types of claims that cannot be eliminated. Risky operations can continue but with measures in place to reduce loss exposures. For example, individuals working with dangerous chemicals might wear personal protective equipment or machine guarding may be used to prevent injuries among those who work with dangerous machines.



### Reduction

**Reduction** attempts to reduce the severity or financial impact of losses that are not prevented. Reduction measures can be implemented pre-loss or post-loss. An example of a pre-loss reduction measure would be installation of a fire suppression system (sprinkler); it will not prevent the fire from happening but will help control its spread and the damage it causes. Post-loss reduction measures would be applied after a loss, including prompt claims administration, early intervention, and rapid claims closure.

### Segregation, Separation, Duplication

Segregation, separation, and duplication are a set of techniques geared toward reducing the severity of a loss:

- **Segregation** involves isolating an exposure from other exposures, perils, or hazards. If a company's operations depend on physical computer servers, the company would need to "segregate" the servers into a separate room equipped with firewalls and fire suppression systems. If the main building catches on fire, the servers are protected. Similarly, a company that uses flammable chemicals might store them in a cinderblock building away from the main operations.
- **Separation** is the process of spreading exposures, activities, or assets over several locations. This way, if one of the locations suffers a loss, the other location will still have sufficient capacity to meet the organization's needs. For example, an online retailer may have separate warehouses in different locations to ensure that a loss at one location will not completely shut down the organization. The key to separation is ensuring that the locations are far enough apart to ensure they are not susceptible to the same loss.
- **Duplication** is the creation of asset back-ups. Asset duplication may minimize business interruptions should an unexpected event occur. A company may backup sensitive data so that duplicates can be easily retrieved if the original copies are lost. Another common example of duplication is the spare tire in a car. If one of the other tires is damaged or flat, the driver has a duplicate tire.



### Transfer

**Transfer** attempts to reduce risk to the organization by transferring some or all of it to another party. A company might hire a delivery service for its products rather than maintaining a fleet of delivery trucks and having delivery drivers. Another good example is a hospital pharmacy. Those services are frequently “farmed out” to a third party and not offered directly by the hospital. The hospital has transferred the risk of incorrectly dispensing drugs to another party. In both situations, there has been a physical transfer of an operational function or exposure to an outside source.


Risk can also be mitigated through contractual transfer, where the responsibility for payment of losses arising from certain liabilities is shifted to another party. There are three common types of contractual transfer: a waiver of subrogation, an exculpatory agreement, and a hold harmless or indemnification agreement.

1. A **waiver of subrogation** is a pre-event agreement that prevents an insurance carrier from recovering payments it makes to its insured for a claim caused by a third party.
2. An **exculpatory agreement** is a pre-event exoneration of one party for events that may result in any loss or a specified loss to another party.
3. A **hold harmless agreement** or **indemnification agreement** is an arrangement whereby one party assumes the liability inherent in a situation, thereby relieving another party of that liability.

Examples of these types of contractual transfers are reviewed in Section 3 of this Learning Guide.

Risk Control Technique Examples

Review the following tables for examples of the application of the various risk control techniques discussed.

Avoidance
<ul style="list-style-type: none"><li>• Drug manufacturing Company A terminates the manufacturing of a medication due to its adverse side effects.</li><li>• Homebuilder B ceases to purchase wooden trusses used in home construction from an international supplier due to the collapse exposure.</li><li>• Hoverboard Manufacturing Company C ceases the sale and distribution of its highly popular hoverboard product line due to an explosion hazard.</li><li>• Producer Grower D recalls tomatoes from grocery store shelves due to a Listeria outbreak.</li><li>• Destination Resort E closes its beaches due to a seasonal shark infestation endangering its guests.</li><li>• Concert Management Company F cancels a concert due to the threat of terrorism that could potentially injure thousands of patrons.</li><li>• Restaurant Chain G ceases the sale of alcoholic beverages near college campuses.</li><li>• Toy Store H discontinues importing and selling a popular wooden doll house painted with lead paint.</li></ul>


### Prevention

- Long-haul Trucking LLC hires an expert driver training company to conduct comprehensive driver training for all drivers.
- Highway Construction LLC inspects and conducts maintenance checks of heavy equipment to ensure that it is operational and safe.
- Boom Fireworks LLC labels products to thoroughly explain safe use and safety hazards.
- Fun Time Amusement Park installs signs and fencing to deter public entry to unsafe areas of the park.
- A machine works company requires employees to use personal safety equipment (i.e., eye goggles, hard hats, safety shoes, etc.) from the time they clock-in to work until they clock-out.



### Pre-Loss Reduction Activities

- A retail strip center installs firewalls throughout buildings to reduce the spread of fire.
- Candy Wholesale LLC installs fire suppression systems in their warehouses.
- A youth hockey organization requires coaches and players to wear helmets with eye shields while on the ice.

### Post-Loss Reduction Activities

- A large company activates crisis management procedures that include evacuation plans, communication protocols, securing property, etc.
- A homeowner puts a tarp over a hole in their roof to prevent further damage to the interior of the house.



## Section 1: Risk Management Concepts

### Segregation

- A computer room is designated as a high-risk exposure and is located on the bottom floor of the building with controlled access.
- A spa manufacturing plant builds a storage building 500 yards away from the main manufacturing building to store flammable cleaning solvents.

### Separation

- A school district decentralizes storage of its fleet of buses by setting up three separate garage locations in different parts of the city.
- An appliance store splits unsold inventory between two separate warehouses 200 miles apart.

### Duplication

- Heavy Equipment Rentals LLC keeps an inventory of spare parts in readiness for equipment breakdowns.
- Many organizations store duplicate copies of computer backups off-site or in the cloud.

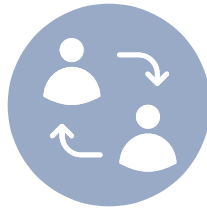


### Physical Transfer

- A manufacturing company uses a common carrier to distribute manufactured goods rather than buying trucks to transport products.
- An organization leases employees rather than hiring them directly.
- Window Distribution LLC hires independent contractors to install windows rather than hiring employees.

### Contractual Transfer

- **Hold harmless or indemnity agreements** – A tenant agrees to hold the landlord harmless for any damage to the building the tenant causes. These types of agreements are discussed further in Section 3.
- **Exculpatory agreements** – Malyssa and Robert are neighbors. Robert's tree drops leaves into Malyssa's pool. Robert is concerned that if he takes down the tree, limbs may fall and damage Malyssa's fence. Malyssa agrees that she will not hold him responsible for damage to the fence caused by limbs.
- **Waivers of subrogation** – A business owner may require a waiver of subrogation from individual subcontractors who work at the job site. This protects the owner from liability for claims made by or against the subcontractors.



Risk control involves more than the use of one single risk control technique. The reality is that a combination of control techniques may be needed to address an exposure or activity. The most successful risk control programs incorporate elements of all five techniques.



## Knowledge Check



**Directions:** Read the scenarios below. For each scenario, identify two techniques of risk control that could be used and explain how those techniques would help mitigate the exposure described in the scenario. If needed, research some possible solutions.

1. Rapids Waterpark recently unveiled a new water slide. Over the course of the next few months, several patrons of the park were injured when riding the new slide.

---

---

---

---

2. ABC Software Company has been the target of phishing and attempted ransomware attacks. They are worried that a bad actor will gain access to their software code and servers and demand a ransom payment.

---

---

---

---

3. Austin Antiques refinishes and restores antique furniture. Once they complete their process, they ship the finished product to the customer. They currently use their own delivery fleet. After several bad traffic accidents, they are concerned about safety issues.

---

---

---

---



The focus of risk control should be on solutions that will prevent or reduce actual harm or the cost of loss. Providing funds to be paid in compensation is addressed in the following step – Risk Financing.

### Step 4. Risk Financing

Risk financing involves acquiring funds to pay for losses that an organization experiences. These funds can be obtained internally (within the organization) or externally. When clients rely on insurance to pay losses, they pay premiums in exchange for promises of compensation for specified losses. Those losses are paid using external funds because they came from outside of the organization.



The use of internal funds to pay for losses is referred to as retention. There are two types of retention:

**active** (planned) or **passive** (unplanned). In active retention, a company may decide it is willing to accept a specific financial amount of risk knowing that if a loss occurs, payment will be made from the company's assets. For example, Company A may decide it is willing to retain losses of \$10,000 in the event of a fire and will use its own financial resources if such a loss were to occur.

Passive retention is unplanned. For example, imagine if Company A purchases a new building but fails to obtain property insurance. If the building is damaged in a fire, Company A would have to use its own funds to pay for the cost of repair or reconstruction. This example illustrates why risk identification is so important. Without identification, risks cannot be analyzed, controlled, financed, or administered correctly.

### Step 5. Risk Administration

The final step is Risk Administration, which involves two key steps:

- The implementation of the risk management program's policies and procedures; and
- the ongoing monitoring of their success. Adjustments are made to policies and procedures as needed, based on the results of the monitoring process.



The most effective risk management programs are extremely flexible and are therefore able to adapt to the ever-changing operational landscape—whether it be new regulations, technology, environmental and/or social viewpoints, market forces, or any combination thereof.

## ▶▶ Knowledge Check



Nancy is the risk manager at Risk and Insurance University and is conducting her annual review of the risk management program throughout the day. State which step in the risk management process is being executed.

1. Nancy's first meeting of the day includes the university's insurance broker and chief financial officer as various insurance policies and retention options are reviewed.  

---
2. Before lunch, Nancy tours the campus along with building managers, maintenance professionals, and grounds keepers to ensure that various safety protocols are being followed and all safety mechanisms are functioning properly.  

---

## The Impacts of an Effective Risk Management Program

### Learning Objective:

*1.5 Describe the impacts of an effective risk management program.*

An effective risk management program will produce several positive impacts on the program-implementing organization. A successful risk management program helps an organization consider the full range of risks it faces. It also examines the relationships between risks and the impact they could have on an organization's strategic goals. It allows the organization to select appropriate risk control and risk financing methods. As the program progresses, it can have several impacts on an organization.



## Increase in Profitability

An effective risk management program helps to increase profitability. This is done primarily through reducing costs but also through maintaining and even increasing revenues. Effective risk management programs may also result in reduced claims (lowering insurance premiums, deductibles, and other retention costs while increasing risk transfer opportunities) and managing non-insurable risks/opportunities, including reputation, process improvements, new technology development, and other avenues that create or support a competitive advantage.



## Helps Identify Exposures, Opportunities, and Associated Risks

An effective risk management program helps an organization identify exposures and opportunities and the risks associated with each. The organization can then direct resources to support the success of the opportunities while attempting to prevent and reduce the costs associated with losses, all while spreading the financial risk of each across the organization. Essentially, risk management programs help organizations to reduce the frequency and severity of losses and more accurately predict and prepare for the financial impact of those losses.

## Protect Cash Flows and Assets

Effective risk management programs protect cash flow and assets. Ultimately, any prevented losses increase the bottom line and avoid cash flow disruptions that may occur if cash is otherwise diverted to loss payments, which can have immediate and long-lasting negative implications. Consider the scenario:



Wilson's Widgets (WW) is set to launch a new product intended to compete with rival products already in the marketplace. The new product requires a large amount of funding reserved for this purpose during the prior fiscal year.

Prior to the launch, a hacker takes control of WW's entire system, freezing the organization out and demanding a ransom payment to release it. WW failed to finance this type of loss by securing the proper insurance coverage, so they are forced to pay the ransom and have no choice but to use the funds set aside for the new product.

Outcome: The product launch is ultimately delayed, and replacement funds must be secured. WW falls behind its competitors in terms of market share.



## Check-In



**Directions:** Read the paragraph below and respond to the question.

How could an effective risk management program been used at Wilson's Widgets to address the potential losses for cyber exposures such as those detailed in the scenario?

---

---

---

---

## Improves Workforce Morale and Productivity

Effective risk management programs improve workforce morale and productivity through fewer injuries, efficient return-to-work programs, and improved communication from management. Better communication will help management be more responsive to the needs of the workforce, all of which lead to lower employee turnover. Maintaining skilled and motivated employees is always more productive and cost-effective than continually searching for and onboarding new employees. Ultimately, this can lead to greater productivity and increased revenues for the company, assuming there is demand for its products.



## Improves Quality, Processes, and Technology

Effective risk management programs often focus on improving quality, processes, and technology. This can enhance supply chain efficiency and create or support a competitive advantage. The efficiencies will decrease costs while revenues increase as more units are produced, locations are opened, consumers are reached, and products are developed.



Henry Ford's creation of the assembly line revolutionized manufacturing as production costs were slashed while the number of available units skyrocketed. Ford's innovations established an entirely new market as the expanded inventory and reduction in costs meant automobiles were no longer strictly for the uber-rich, but could now be afforded by a much wider segment of the population. More modern examples include utilizing information technology systems and data analytics, automation and robotics, vertical integration and just-in-time manufacturing, and using foreign labor.

## Safeguards Brand and Reputation

Effective risk management programs safeguard the organization's brand and reputation. This is one of the most difficult tasks for any organization to accomplish because once a reputation is tainted, it is extremely difficult to repair it completely. If the nature of the event and/or the results are severe enough, it can forever remove the brand from the market. For example, if a company is discovered to be involved in controversy and scandal, its reputation will suffer, resulting in lost revenues. Review the following case study to see how risk management can mitigate the damage from scandals and help an organization recover its reputation after a major incident.



### Case Study – Reputation Management



Johnson & Johnson (J&J) faced a dire situation in the early 1980s, which could have led to the demise of the Tylenol brand (and, more importantly, to more human fatalities) should it have been handled less skillfully. In the fall of 1982, seven people in the Chicago area died after taking cyanide-laced capsules of Extra-Strength Tylenol, the drug maker's best-selling product. Although it was determined that the capsules were being tampered with after they arrived on the drugstore shelves and not at J&J's manufacturing facility, J&J notified the public and recalled 31 million bottles while offering a replacement product in the safer tablet form free of charge. J&J still experienced a staggering drop in market share from 37% to 7%, and experts at the time predicted that the Tylenol brand would never recover. Two months later, Tylenol was back on the market with a new tamper-proof package (designed by J&J) reinforced by a widespread media campaign, and one year later, had climbed its way back to 30% market share. J&J was successful in restoring the Tylenol brand image because it made its customers' safety the top priority, revolutionized the packaging of medicines to address the initial problem, and, most importantly, communicated honestly, clearly, and consistently with the public throughout the process from the initial warning notification of the incidents in Chicago to the marketing campaign supporting the re-launch of the newly packaged product.

Overall, an effective risk management program does more than reduce accidents, injuries, and losses; it positively impacts the organization. From preserving its reputation to driving dollars to the bottom line, an effective risk management program benefits all levels of the organization.

## ▶▶ Knowledge Check



Provide an example of current events where a miscalculation or inaction on the part of an organization resulted in damage to its reputation—from which the organization might or might not have recovered.

---

---

---

---

## Total Cost of Risk (TCOR)

### Learning Objectives:

1.6 Describe the components and uses of Total Cost of Risk (TCOR).

One important calculation that all risk managers need to understand is the **Total Cost of Risk (TCOR)**. TCOR calculations and analyses determine the sum of all costs and expenses associated with risks and risk management within an organization. In response to the question, “What is the total cost of risk within your organization?” a risk manager might respond, “It is the cost of an organization’s insurance premiums.” However, the actual total cost of risk is much more complicated. These costs include insurance costs, risk management department salaries, outside services, insurance **deductibles** (what the organization pays before the insurance company contributes its share), and retentions.



TCOR is a tool used to help inform risk management decisions, establish accountability in the workplace, and develop more precise budgets. By calculating and analyzing the TCOR, organizations can improve safety measures and control losses. TCOR can also help organizations better predict and budget for risk, as well as enhance their risk management processes.

## Basic TCOR Calculation – Five Elements

Traditionally, organizations track only insurance premiums and deductibles. TCOR is the calculation of all measured costs and expenses connected with the risk management function of an organization:

$$\begin{array}{l} \text{(1) Insurance costs} \\ + \text{(2) retained losses} \\ + \text{(3) risk management department costs} \\ + \text{(4) outside service costs} \\ + \text{(5) indirect costs} \\ \hline = \text{TCOR} \end{array}$$

The calculation itself is straightforward, but the development and implementation of the metric can be more complicated. Organizations vary greatly, and as a result, there is no definitive method that determines which costs are measured in which category. Consequently, organizations will develop their TCOR calculations differently and should use them as internal metrics. What follows is a breakdown of each component of the TCOR calculation.

### 1. Insurance Costs

These costs are the most easily quantified. This category includes premiums, premium taxes, letters of credit, deposits, collateral, and interest on financed premiums.

### 2. Retained Losses

This includes deductibles and active and passive retentions. It can also include other self-funding costs such as accruals, bonds, surety costs, funded reserves, and the costs associated with handling retained losses or claims, including legal expenses, medical case management fees, third-party claims administrator fees, and so on. Passive retention can be accounted for here, but it is difficult to accurately measure since even the most prepared organizations will likely suffer some unplanned retention.



### 3. Risk Management Department Costs

This covers payroll and related costs, risk management information system costs, and administrative costs. It could also include other risk management department costs, like travel, education, conferences, and any other costs the organization deems appropriate to charge to the risk management department.

### 4. External Service Costs

These costs include fees for any outside expertise the organization deems necessary in mitigating risk. For example, if the risk manager hires a consultant to perform safety training, the consultant's fees would fall into this category.

### 5. Measurable Indirect Costs

These are costs that arise because of the loss but are not directly related to the loss itself. If an employee is injured on the job and cannot return to work for quite some time, the employer may have to pay overtime to other employees who are covering the workload. This is a measurable indirect cost—it has nothing to do with the injury itself.

## Benefits of Allocating TCOR

When used as a universal organization metric, TCOR utilization can improve the risk culture of an organization. However, allocating TCOR to individual departments or locations will produce optimal results. When TCOR is assigned to individual departments, an organization can determine where costs, such as retained losses, originate. This enhances accountability as each location, division, etc., becomes responsible for its own cost of risk. Bonuses, salary increases, and evaluations can be linked to the outcomes of TCOR. Doing so allows employees to become more aware of the costs related to losses, exposures, and other TCOR elements. This modifies the behavior of all employees as they become risk owners. In turn, this encourages all employees to participate in loss control and concentrate on mitigating the frequency and severity of losses.





## ▶▶ Knowledge Check



Lucy is the risk manager for Pinnacle Products. She is reviewing a TCOR report prepared by the risk management intern. Lucy is concerned that the intern may not have a good understanding of the elements of TCOR. Which of the items in the report below support Lucy's concern?

- \$300,000 – insurance premiums for all lines of coverage
- \$20,000 – repair of office equipment damaged by an employee's negligence
- \$55,000 – settlement of a general liability claim paid by the insurer and billed back to the insured
- \$10,000 – safety consultant hired to perform physical inspections at each of the locations
- \$4,000 – the recovery of damage to a company-owned vehicle from a negligent driver's insurer
- \$65,000 – salary of the Director of Marketing, including her benefits
- \$15,000 – overtime paid to an employee who covered for another employee who was out of work while recovering from a work-related accident

---

---

---

## Summary

Individuals and organizations set goals for their futures, and effectively predicting, preparing for, and managing risks can help them to achieve these goals. While risk may be inevitable, it is manageable with assistance from insurance and risk management professionals who thoroughly understand the terminology, forms of risk, and steps or actions their clients can take to avoid or minimize financial loss.



A thorough understanding of risk management depends partly on an understanding of common terms. For example, the term “risk” has four definitions used in the risk management field in differing circumstances. For the purposes of this course, risk is defined as **the possibility of a positive or negative outcome arising from a given set of circumstances**. Pure risks involve situations or incidents whose only outcomes can either be loss or no loss. In other words, there is no possibility of gain. Speculative risk, on the other hand, involves the possibility of loss or no loss and includes the chance of a gain. Risk managers use a specific set of terms in their work. Many of these terms have differing meanings to agents, brokers, and underwriters. Those terms include exposure, loss, and peril.

**Risk management** describes the process of implementing actions that reduce or eliminate the likelihood of a loss that would affect an individual or organization’s assets, profitability, or objectives. The risk management process involves five steps: Risk Identification, Risk Analysis, Risk Control, Risk Financing, and Risk Administration. Each step in the process presents potential benefits for clients.

To manage the risk management process effectively, the risk manager must know the Total Cost of Risk of the organization. The TCOR comprises all costs related to an organization’s risk management program, including those that fund losses or fund the implementation and monitoring of the risk management process.

## Section 1 Self-Quiz

**Directions:** Respond to the questions below.

1. One example of an industry that is basically immune to risk is the restaurant industry.

True

False

2. Which one of the following statements is correct?

- ☐ Chemicals Inc. frequently ships toxic chemicals. This is a speculative risk.
- ☐ Jeremiah purchases stock in a new company. This is a speculative risk
- ☐ A restaurant opens a new location to increase sales. This is a pure risk.
- ☐ A store launches a loyalty program to improve customer retention. This is a pure risk.

3. Paul is a long-time employee of Stonework Masonry. After decades of lifting heavy bricks, he has developed two herniated discs in his spine. This is an example of an

\_\_\_\_\_.

- ☐ incident
- ☐ accident
- ☐ occurrence
- ☐ incident that became an accident

4. An insurance carrier tracks the total dollar amount it paid in claims after an unusually severe hurricane season. They are calculating the \_\_\_\_\_ of their losses.

Frequency

Severity

## Section 1: Risk Management Concepts

**Directions:** Use the word bank to complete questions 5-10.

loss	exposure	expected losses	peril	claim
	hazard	risk-taking ability	risk appetite	

1. The projection of the frequency or severity of losses based on loss history is the \_\_\_\_\_.
2. A(n) \_\_\_\_\_ is a factor that increases the likelihood that a loss will occur.
3. Fires, lightning, riots, and automobile accidents are all examples of \_\_\_\_\_.
4. A graphics design firm recently had to pay a legal settlement due to copyright infringement. This is an example of a(n) \_\_\_\_\_.
5. A chemical manufacturing company routinely handles hazardous chemicals. This is an example of a(n) \_\_\_\_\_.
6. \_\_\_\_\_ refers to a company's willingness to accept a risk, whereas \_\_\_\_\_ refers to the organization's financial capacity for assuming that risk.
7. Which answer below defines any conscious action or inaction to minimize (at optimal cost) the probability, frequency, or severity of loss?
  - ☐ Risk Control
  - ☐ Risk Analysis
  - ☐ Risk Administration
  - ☐ Risk Financing
  - ☐ Risk Identification

## Section 1: Risk Management Concepts

8. A company recently decided to invest in enhanced cybersecurity measures to protect its data and servers from ransomware attacks. Which technique of risk control did the company employ?
- ☐ Reduction
  - ☐ Transfer
  - ☐ Avoidance
  - ☐ Prevention
9. Which of the following statements describe a benefit(s) of an effective risk management program? **(Select all that apply.)**
- ☐ Improved quality, processes, and technology
  - ☐ Improved workforce morale and productivity
  - ☐ Protected cash flow and assets
  - ☐ Increased demand for a company's products
10. A company's insured building suffers a fire loss of \$50,000. The company pays a \$2,500 deductible to activate the coverage. Under TCOR, the deductible would be categorized as follows:
- ☐ Insurance costs
  - ☐ Retained losses
  - ☐ Risk management department costs
  - ☐ Indirect costs

# Set Yourself Up for Success!

## Visit the “Resources” Webpage at [RiskEducation.org/RCresources](https://RiskEducation.org/RCresources)

For valuable reinforcement, be sure to visit the “Resources” webpage. This webpage contains a variety of materials that will help you absorb the course material *and* set you up for success on the Final Exam. You’ll find:

### Study Guide

Download a copy of the Study Guide. It contains all the Check-In questions, Knowledge Checks, and Self-Quizzes contained in this Learning Guide in a format that makes it easy for you to practice and check your answers.

### Flash Cards

Play an interactive vocabulary game with a study set of digital flashcards to enhance your learning of the insurance and risk management terms used in this course.

### Review Game

Use a fun, trivia-style review game to test your knowledge and prepare for the Final Exam.

### Review Activity

Explore a fun simulation activity to learn more about phishing exposures.

## In Addition...

### Appendix

The Appendix of this Learning Guide contains a Glossary of terms as well as tips for study techniques and sample test questions that will help you prepare for the Final Exam.

## Section 2: Risk Control and Mitigation – Human Resources

---

### Section Goal

The goal of this section is to provide you with a review of risk control, including the purpose and importance of risk control for organizations. Insight into and information about the various exposures that can be found in the human resources general classification of risk are discussed along with appropriate risk control measures.

### Learning Objectives:

- 2.1 *Describe why organizations should focus on risk control and the importance of involving all members of an organization in the risk control process.*
- 2.2 *List the root causes of accidents and injuries.*
- 2.3 *Apply the six basic steps of accident prevention.*
- 2.4 *Develop recommendations for a health and safety program based on the eight elements of an effective program.*
- 2.5 *Define the term “ergonomics” and describe the risk control methods associated with ergonomic issues.*
- 2.6 *Identify the risk factors and risk control measures associated with manual material handling and lifting.*
- 2.7 *Describe the benefits and possible legal problems associated with a workplace substance abuse program.*
- 2.8 *Name the risk factors and risk control measures used to prevent or reduce workplace violence.*

## Introduction

Once an organization's exposures to loss have been identified and analyzed, an effective risk control program should be created. This program is essential to the financial health of the organization. Reducing claims severity and frequency drives dollars to the bottom line, allowing the organization to grow and meet strategic objectives. Ultimately, an effective risk control program will require company-wide support and will engage all members of the organization in the risk control process.

## The Purpose of Risk Control

### Learning Objective:

*2.1 Describe why organizations should focus on risk control and the importance of involving all members of an organization in the risk control process.*

### Who should be involved in a risk control program?

As previously discussed, risk control is any conscious action or inaction to minimize, at the optimal cost, the probability, frequency, severity, or unpredictability of loss. The focus of risk control is on finding and implementing solutions to prevent or reduce actual harm and the total cost of risk. The focus is not on securing finances to pay for a loss—that is the role of risk financing.

An effective risk control program should engage all individuals within the organization. For risks to be identified, individuals from across the organization are required to provide input about ineffective or dangerous processes and procedures, faulty machinery, and many other types of risks that exist in their areas of operation. Risk control is no different. Any attempts by an organization to adopt measures to control identified risks are unlikely to succeed without the participation of people within the organization. Only when people are involved and engaged in the safety procedures will risk be controlled.



### Why should organizations focus on risk control?

#### It's good business.

First and foremost, the primary objective of a responsible organization should be "safety comes first." Productive businesses do not want to cause harm to anyone, whether they are employees, customers, or third parties. Effective risk control programs are good business that create a "win-win" situation for all parties associated with the organization, thereby protecting the





organization's reputation and brand. In addition, when accidents are prevented, there is no need for any other part of the risk management process (e.g., risk identification, risk analysis, risk financing, risk administration.) This ultimately reduces the total cost of risk.

### Risk control can reduce costs.

When there is no accident, no additional cost is added to the total cost of risk, which is good for the organization's bottom line. The cost of losses arising from damages and/or injuries is a key component of any organization's total cost of risk, either directly through retentions or deductibles, or indirectly through future insurance premium increases due to adverse claims experience—not to mention negative publicity, potential loss of reputation, and lost productivity.

### Risk control may be needed for compliance.

Organizations must implement risk control practices to fully comply with federal and state regulations set by organizations such as the Occupational Safety and Health Administration (OSHA). Despite extensive regulations and the significant enforcement authority assigned to OSHA, some company executives and managers fail to take compliance obligations seriously. The reasons are simple. First, they argue, it is the government, and the likelihood of an OSHA visit and/or inspection is almost non-existent since there are not enough inspectors.



Second, OSHA fines may seem to be an insignificant portion of the total cost of risk. However, in addition to the usual fines and penalties, OSHA can impose daily fines and even jail sentences on flagrant violators.

Outside federal and state OSHA laws, there are other sources of legislation that organizations must comply with. Statutes, including safety and workers compensation, differ by state. To ensure that they are following the law, employers must refer to their states' statutes to determine their exact legal requirements. The Department of Labor maintains a website that outlines the list of benefits by state ([www.osha.gov/stateplans](http://www.osha.gov/stateplans)).

### Risk control protects employees' safety and an organization's reputation and brand.

Employees who know that their employer is concerned for their safety and that there is a robust safety program in place will be more satisfied in the workplace. Morale is heightened, and performance and production are improved<sup>1</sup>.

Furthermore, by maintaining a safe workplace for employees, an employer avoids the negative press and damage to their reputation and brand which are often the product of serious employee injuries



<sup>1</sup> SafeStart. "The Correlation Between Workplace Morale, Productivity, and Safety." SafeStart. Accessed June 12, 2023. <https://safestart.com/news/the-correlation-between-workplace-morale-productivity-and-safety/>.

or extraordinary property losses. A continuous record of safe operations strengthens the organization's brand and reputation.

### ▶▶ Knowledge Check



**Directions:** Review the scenario and complete the chart below

A hurricane struck Florida's Gulf Coast, causing significant damage to a five-star hotel. The hotel has a golf club, golf course, and a separate parking structure. The hotel maintains a fleet of minivans and employs drivers to shuttle guests to and from the airport.

During the storm, it was necessary to evacuate guests and employees using the shuttles, and injuries were reported. After the storm, the property required extensive repairs as a result of wind damage and flooding. Plus, water damage made it necessary to replace the hotel's fleet of golf carts and two minivans.

Knowing the extent of the damage, what risk control measures should the hotel have taken prior to the loss? Write your answers in the chart. Below the chart, explain how these measures would have benefited the hotel.

<b>Avoidance</b>	
<b>Prevention</b>	
<b>Loss Reduction</b>	
<b>Segregation</b>	
<b>Transfer</b>	

# The Root Causes of Accidents and Injuries

## Learning Objective:

2.2 List the root causes of accidents and injuries.

A general understanding of the causes of accidents is helpful if a risk manager is to successfully determine which risk control techniques will be most practical or valuable. Some common root causes of accidents include:

- Unsafe acts or behaviors
- Unsafe conditions
- Lack of awareness or training
- Uncontrollable events



Most unsafe behaviors and conditions are observed one or more times before an accident occurs. Unsafe behaviors and conditions left unchanged will eventually result in an accident or injury. Root cause analysis lays the foundation for preventing future accidents and injuries.

## Unsafe Acts or Behaviors

There are many reasons why employees may work in an unsafe manner:

1. Unsafe work may be faster, more convenient, or more comfortable.
2. Unsafe behavior rarely results in injury on any single occasion.
3. People may take risks when rewards are quick and certain, and the risk of an accident is low.

In circumstances like these, employees may not receive regular reminders regarding the importance of safety or feedback about their behaviors. In fact, workplace conditions can sometimes encourage unsafe behavior.

It's not surprising then that employees often think if everyone else is demonstrating a particular behavior, the behavior must be okay. In some cases, unsafe work behaviors are viewed as more convenient, more comfortable, or help employees accomplish their goals in less time. Consider an example:



Employees on a construction site object to wearing hard hats. In addition to this, they tend to avoid using cumbersome safety equipment as it slows them down. The behavior is widespread among employees.



This is where managers—and risk managers—must ensure that all personnel understand that employee safety is in everyone’s best interest. There must also be a clear expectation that safety requirements will be enforced without exception. Unsafe behaviors rarely result in injury on any single occasion, but at some point, an accident will occur if unsafe behaviors are not addressed. The goal of a risk manager is to alter or prevent unsafe behaviors.

### Unsafe Conditions

Unsafe conditions are a second major reason for employee accidents. This factor includes everything from commonplace tripping hazards to more specific hazards inherent in dangerous occupations, such as underwater welding. For the manufacturing industry, additional unsafe conditions could include using a machine where the guarding shield has been removed, or the dead-man’s switch has been disabled.



While some unsafe conditions are simply inherent to the nature of specific operations, it is also frequently the case that management permits some unsafe conditions to continue. There have been many lawsuits over unsafe conditions permitted by management. Unsafe conditions are occasionally allowed because they increase the speed of a production line or enhance efficiency in some other manner. Sometimes, management knowingly disregards a manufacturer’s safety recommendations for these very reasons.

### Lack of Awareness or Training



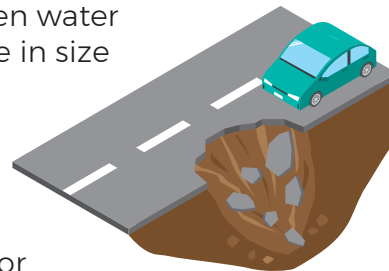
Another very common and preventable cause of accidents is that employees are unaware their behaviors are unsafe. In many cases, this lack of awareness is because no one in the companies where an employee works has ever identified and addressed unsafe behaviors. Employees may not have had any training on safer ways to accomplish the same objective. Too often, personnel, including managers, become too involved in their other roles and responsibilities, leaving safety and training to take a back seat.

### Uncontrollable Events

There may be causes of accidents or injuries that are unavoidable. These uncontrollable events are usually thought of as catastrophic natural events like earthquakes. These events can have devastating effects on both people and property, but an event need not be catastrophic to be uncontrollable. Consider sinkholes.



Sinkholes are cavities below the ground that form when water erodes an underlying rock layer. The cavities may range in size from several feet to hundreds of feet in diameter. Unobserved from the surface, the collapse is entirely unexpected. In 2020, a sinkhole in China swallowed an entire bus, killing several passengers and injuring many others. Sinkhole activity is an uncontrollable event, even though it does not have the same impact or disastrous nature as a hurricane.



### Knowledge Check



**Directions:** Conduct your own research and comment about your findings.

Since the industrial revolution, there have been many large-scale industrial disasters. Research one of these disasters and determine if the root cause was unsafe acts or behaviors, unsafe conditions, lack of awareness or training, or an uncontrollable event.

**Explain the root cause (or causes) for the event you select.** Some potential choices of disasters could include:

- 2023 Ohio train derailment
- Fukushima Daiichi nuclear accident
- 2010 Deepwater Horizon oil spill
- Bhopal disaster
- Triangle Shirtwaist Factory fire

---

---

---

---

# Accident Prevention

## Learning Objective:

*2.3 Apply the six basic steps of accident prevention.*

Accidents are part of an organization's total cost of risk and can prove costly. When an accident occurs, an organization must pay either through retention or deductibles. Accidents may also have indirect costs, such as the increased price of future premiums. As discussed previously, accidents can also damage an organization's profitability and reputation. Consequently, accident prevention directly protects an organization's bottom line.

Earlier, the root causes of accidents were discussed. All accidents can be traced back to four root causes:

- An individual committing an unsafe act or behavior, negligently or intentionally
- The existence of unsafe conditions
- A lack of training regarding safe practices
- Uncontrollable natural or economic events that cause accidents

Estimates of the number of incidents, accidents, and losses that arise from each of these four root cause vary widely. However, the National Safety Council estimated that workplace fatalities, injuries, and illnesses resulted in \$171 billion in damages in the United States alone in 2019. Establishing an accident prevention program and encouraging workplace safety can directly reduce losses for an organization<sup>2</sup>.

## Accident Prevention Basics

To help mitigate the root causes, the organization can use the six Accident Prevention Basics: eliminating the hazard, substituting a less hazardous substance or process, using engineering controls, administrative controls, personal protective equipment, and implementing training programs.



<sup>2</sup> Occupational Safety and Health Administration (OSHA). "OSHA Business Case." Accessed June 12, 2023. <https://www.osha.gov/businesscase>

# ACCIDENT PREVENTION BASICS



**1** Eliminating the Hazard



**2** Substituting a less hazardous process



**3** Engineering Controls



**4** Administrative Controls



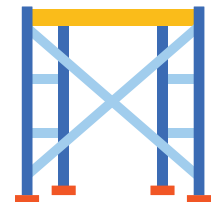
**5** Personal Protective Equipment



**6** Training

## 1. Eliminating the hazard

Eliminating the hazard is like the risk control technique of avoidance; it attempts to avoid or eliminate the hazardous activity. For example, ladders are one of the largest sources of employee accidents and deaths in the construction industry. Many construction companies have eliminated this hazard by requiring the use of various types of lifts. Employees are not provided with ladders, nor are they allowed to use them.



## 2. Substituting a less hazardous substance or process

The second method of accident prevention is substituting a less hazardous substance or process for an existing one. For example, many companies use non-toxic alternatives for substances commonly used in the workplace that contain chemicals that can cause employee injuries. Think about what occurred in the Roundup® litigation's aftermath, where landscapers and homeowners are now moving to use organic weed control methods. To briefly summarize, the second method of accident prevention is finding safer alternatives to processes or substances used in the workplace.

## 3. Engineering controls

Another accident prevention technique is using engineering controls to modify designs physically. For example, a hedge trimmer manufacturer learns that homeowners are sustaining hand injuries because the product was designed to leave one hand free. The manufacturer redesigns the product to require two-handed operation. This physical modification ensures that the free hand will no longer be at risk of injury.

#### 4. Administrative controls



Administrative controls consist of rules or activities that management undertakes, such as safety meetings, supervision, or safety procedures and manuals aimed at reducing the likelihood of accidents or injuries.

A good example would be establishing whether employees are allowed to use their phones while driving company vehicles.

#### 5. Personal protective equipment (PPE)

Personal protective equipment is exactly what it sounds like, e.g., safety goggles, steel-toed shoes, gloves, hard hats, respirators, and similar gear worn or used by workers that prevent or reduce injuries.

A welder's helmet is an example of PPE. It protects a welder's face and eyes from sparks and burns. It also offers eye protection from the electromagnetic energy an arc or flame gives off, commonly referred to as radiant energy or light radiation.



#### 6. Training

Training is education meant to instruct individuals on the appropriate behavior or actions they should take.

Employees must be aware of safe work habits and procedures. Many companies have “toolbox talks” on a regular basis. Toolbox talks are informal safety meetings typically lasting five to seven minutes and held at the beginning of a shift or workday. These talks focus on specific safety topics and can be as simple as brief reminders to stay hydrated while working outdoors in the summer.





# Knowledge Check



Over the past three years, a national landscaping company has experienced an increase in the frequency of work-related accidents. They have recorded back injuries, workers falling out of trees, limbs falling on employees and vehicles, and chipper accidents. Most recently, two fatalities resulted from accidents during tree-trimming operations. Using the six-step accident prevention process you just learned, make two suggestions accident-prevention actions you could take under each step.

Eliminating the hazard	Substituting the hazard	Engineering controls
Administrative controls	Personal protective equipment	Training

# Safety and Health Programs

## Learning Objective:

2.4 *Develop recommendations for a health and safety program based on the eight elements of an effective program.*

## Safety and Health Standards

To promote safety and health in the workplace, standards were developed through legislation, administrative laws and rules, and industry agencies and organizations. Employers are responsible for providing a healthy and safe workplace and must comply with all applicable Occupational Safety and Health Administration (OSHA) standards.



OSHA, a part of the U.S. Department of Labor ([www.osha.gov](http://www.osha.gov)), was formed to “assure the safety and health of America’s workers by setting and enforcing standards; providing training, outreach, and education; establishing partnerships; and encouraging continual improvement in workplace safety and health.” The OSHA General Duty Clause states “each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees.

OSHA also stipulates that the employee has a responsibility to work safely: “each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.” The General Industry Standards are listed in Title 29 of the Code of Federal Regulations Subpart B Part 1910 (29 CFR Part 1910). The Construction Safety Standards can be found in 29 CFR Part 1926. OSHA enforces these regulations through inspections and citations or fines.

Many states have also elected to establish their own agencies to administer federal OSHA standards through delegated authority. Authorized state OSHA programs are required to implement health and safety standards at least as stringent as federal requirements and may be more extensive if authorized by state legislatures.



Despite extensive regulations and significant enforcement authority assigned to OSHA, some company executives and managers fail to take compliance obligations seriously. The reasons are simple. They may view OSHA inspections as unlikely to happen. Furthermore, executives and managers may view OSHA fines as an insignificant part of the total cost of risk and ignore the excessive fines and even jail time that can result from severe OSHA violations.

Consequently, risk managers must continuously educate managers and supervisors on the importance of documenting all OSHA compliance activities. Not only is documentation in and of itself a compliance obligation, but failure to maintain required records specified by regulation makes it difficult, if not impossible, to prove that required compliance measures have been implemented.

## Section 2: Risk Control and Mitigation - Human Resources

In addition to federal and state OSHA laws, there are other sources of legislation. The Mine Safety Health Administration (MSHA) is also a part of the U.S. Department of Labor, with jurisdiction over the mining industry. According to the MSHA website, their mission is “to administer the provisions of the Federal Mine Safety and Health Act of 1977 (Mine Act) and to enforce compliance with mandatory safety and health standards as a means to eliminate fatal accidents; to reduce the frequency and severity of nonfatal accidents; to minimize health hazards; and to promote improved safety and health conditions in the nation’s mines.”

The U.S. Department of Transportation (DOT) oversees federal highway, air, railroad, maritime, and other transportation administration functions. The DOT’s top priority is to keep the traveling public safe and secure, increase mobility, and maintain a transportation system that contributes to the nation’s economic growth.

The Office of Workers’ Compensation Programs (part of the U.S. Department of Labor, Employment Standards Administration) administers four major disability compensation programs that provide wage replacement, medical treatment, vocational rehabilitation, and other benefits to certain workers or their dependents who experience work-related injury or occupational disease.

These programs, the Energy Employees Occupational Illness Compensation Program, the Federal Employees’ Compensation Program, the Longshore and Harbor Workers Compensation Program, and the Black Lung Benefits Program serve the specific employee groups covered under the relevant statutes and regulations. They also serve taxpayers and employers by mitigating the financial burden resulting from workplace injuries.



## Section 2: Risk Control and Mitigation - Human Resources

Other agencies and organizations also have significant involvement in employee health and safety and are listed in the table:

<b>The National Institute for Occupation Safety and Health (NIOSH)</b>	Certifies respiratory protective devices and air sampling detector tubes recommends occupational exposure limits for hazardous substances, and assists OSHA and MSHA in occupational safety and health research
<b>The American National Standards Institute and Safety Products (ANSI)</b>	Tests and certifies types of personal protective equipment, such as hard hats, steel-toed boots, etc.
<b>The National Fire Protection Association (NFPA)</b>	An international organization that promotes fire protection and prevention. The NFPA 101 Code, also known as the “Life Safety Code,” addresses those construction, protection, and occupancy features necessary to minimize danger to life from fire, including smoke, fumes, or panic.
<b>The American Conference of Governmental Industrial Hygienists (ACGIH)</b>	Publishes a schedule of recommended biological and chemical exposure limits for the workplace. These limits are called threshold limit values (TLVs) and typically include exposure limits based on short-term exposures and time-weighted averages for an entire work shift. Although TLVs do not have the regulatory force of OSHA standards, they are based on the most current research from NIOSH and others. They can be updated much more rapidly than OSHA standards, which require extensive rule-making and approval by Congress.

Risk managers should be aware of these different organizations and the various ways that specific regulations may impact their organization’s health and safety programs.

## Qualities of an Effective Health and Safety Program

### **Eight Elements of Effective Health and Safety Programs**



Good safety and health programs require the implementation of eight key elements:

### **Element 1 – Management Leadership**

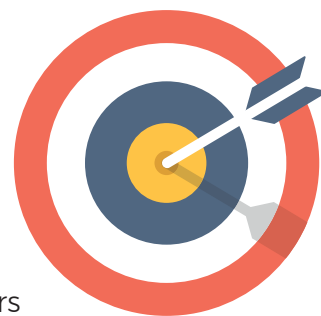
The safety policy is foundational to the success of any risk management program, so it must be incorporated into a company's mission statement. The safety program must be in writing and must identify safety policies, goals, and objectives. It is critical that the CEO or leader of the organization include a signed statement that the organization's senior management expects cooperation and compliance with this program. This demonstrates that the management team is fully committed to safety standards.



Responsibilities and accountabilities should be clearly defined for managers, supervisors, and employees. The written safety program should provide authority, information, training, and resources to fulfill these responsibilities. Management must “walk the walk” to show that safety is a matter of “do as I do,” not just “do as I say,” thereby integrating safety into the business process. For example, if the safety policy requires a hard hat and safety glasses at a job site, the CEO and all accompanying persons who visit the job site must wear the required gear. Safety must be an integral part of the business process; it should be part of the company culture.

### Element 2 – Accountability, Responsibility, and Authority

The safety goals and objectives should be included and properly weighted in performance reviews and employee compensation. They should be both activity-oriented and results-oriented. Safety responsibilities should be defined for all positions, whether an employee works in organizational safety, risk management, purchasing, maintenance, operations, human resources, or any other area of the organization. There should be enforcement of responsibilities with authority assigned to appropriate individuals. The program must stress individual accountability for actions and behaviors from all employees, whether top management or front-line workers. Read the scenario for an example of an accountability structure for supervisors.



A machine shop supervisor has the goal of maintaining a safe facility and encouraging employees to follow safe work practices. If there is a reduction in employee injuries (elimination is unlikely) over the course of the evaluation period as compared to the previous one, he earns a stronger rating for that goal on his performance evaluation.

Similarly, the supervisor could be charged with accident investigation, determining the root cause of the accident, and taking steps to reduce or prevent recurrence.

### Element 3 – Employee Participation



If the safety program is to succeed, every employee must participate and support it. There are many opportunities for employees to participate, from establishing the initial program to its implementation and even to evaluating the safety program’s effectiveness.

One potential way for employees to participate is a safety committee. A safety committee is focused on ensuring the workplace is safe for everyone. It should involve members from across the organization and conduct regular meetings where safety program results are reviewed. In some states, safety

committees are mandated by law, but even in those states without mandates, safety committees should be a vital part of the risk control program. The safety committee should have a charter or be recognized by its top management as crucial to the organization and

its employees. It should have cross-departmental participation with equal representation from management and front-line employees.

The designated safety coordinator should not be the chair of the committee. The chair should be another employee so the committee generates and implements new ideas. There should be regular meetings with agendas, minutes should be maintained for future reference, and action items with parties responsible should result from each meeting.

Employees should also be involved in safety inspections because they are more familiar with the operation than either management, the risk management department, or even outside experts. There should be regular communication between management and employees covering workplace safety and health issues. Furthermore, employee participation can be fostered by:

- Allowing employees to have access to relevant safety and health information.
- Involving employees in exposure assessment and control.
- Allowing employees to report injuries, illnesses, and occupational exposures.
- Accepting recommendations from employees regarding appropriate controls.
- Responding promptly to reports and recommendations from employees.

Management should not act in any way to discourage employee participation in the safety program. The safety program should allow reporting of unsafe conditions and actions directly and anonymously, without fear of any repercussions.

### Element 4 – Hazard Assessment and Control



As previously stated, many accidents are caused by unsafe behaviors or acts rather than unsafe conditions. For example, about 80 out of every 100 accidents are caused by the person involved in the accident, and unsafe acts or behaviors cause four times as many accidents & injuries as unsafe conditions. Uncontrolled events (such as natural disasters) cause only about 2% of accidents. In other words, 98 percent of all accidents are caused by unsafe behaviors, unsafe conditions, or a combination of both, and all these behaviors or conditions can be controlled.

Employees often behave in an unsafe manner because they are unaware their behavior is unsafe. Due to a lack of training, they are unaware of how to perform their

duties safely. When employees work unsafely, they typically do not receive regular reminders and feedback from their supervisors. Also, workplace conditions may encourage unsafe behavior. If management's emphasis is on increasing production at any cost rather than working safely and avoiding accidents, employees will develop slipshod behaviors that lead to accidents.



## Section 2: Risk Control and Mitigation - Human Resources

A key component of risk control is recognizing why employees take risks and get injured. In many situations, the workplace naturally rewards unsafe behavior because it can be faster, more convenient, and more comfortable to work unsafely. Consider the example:



Paul works the assembly line in the widget factory. He can produce widgets much more quickly if he does not use a machine guard because he does not have to move the guard or reach around it to take the finished widget off the machine.



As a result, his unsafe behavior is reinforced because he is able to make more widgets.

Unsafe behavior rarely results in injury on a single occasion, so when rewards are certain, and risks are low, it is relatively easy for a worker to take a risk. However, regular unsafe behavior virtually ensures that injuries will occur. Unfortunately, there is no way to predict when unsafe behavior will result in an injury or who will be injured.

An effective safety program will aim to stop workers from taking risks. One potential method would be to make the risks outweigh the reward through the use of punishment. However, punishment produces minimal compliance and lowers overall employee morale. As a result, punishment should only be used as a last resort.

The preferred option would be to reward safe behavior. Rewards tend to result in extra effort from employees and higher morale. The best way to reward behavior is particular to an organization, but some non-monetary rewards could include:

- legitimate praise
- a certificate
- a pin or button, or a t-shirt or hat.

Regardless of the reward, it is essential that employees are recognized and celebrated for following property safety procedures when performing their job duties.



As shown above, unsafe behaviors and conditions cause accidents, and there is usually time to correct unsafe conditions before an accident occurs. In fact, most unsafe behaviors and conditions are observed at least once prior to an accident. This is why systematic identification and assessment of workplace hazards lead to safer working conditions for all employees. This identification and assessment can be performed in several ways:

### 1. Physical Inspections

These can uncover unsafe working conditions.

### 2. Audits

These may review management practices regarding safety.



### 3. Job Safety Analysis (JSA)

A JSA will identify unsafe work practices.

### 4. Behavior-Based Safety

Behavior-based safety aims to change the behaviors of employees in order to improve safety in the workplace. The employees are observed performing their jobs, and recommendations for improvements are made. This can help pinpoint unsafe acts.

### 5. Accident Investigations, Incident Investigations, and Trending

These investigations can identify unsafe acts and unsafe conditions, work methods, and management practices that lead to losses.

#### Check-In



Richard is a welder in an equipment manufacturing facility. One day, he sees the CEO walking on the work floor without a hard hat or safety glasses. Richard promptly turns off and puts down his torch and walks over to the CEO and reminds him that he must follow the safety rules which are established for all employees. Which element of the safety program made Richard comfortable in correcting his CEO?

- ☐ Management Leadership
- ☐ Accountability, Responsibility, and Authority
- ☐ Employee Participation
- ☐ Hazard Assessment and Control

## Element 5 – Employee Information and Training



Employees need to know they are responsible for their own health and safety program, and they need the information necessary to fulfill their responsibilities within that program. Every employee should receive specific training for each exposure associated with their position and job responsibilities, which should include the nature of the exposure and how to recognize it, any control measures (such as machine guards) and protective procedures the employee must follow, and any provisions of applicable standards or regulations.

Training should begin immediately when an employee is hired and before the initial work assignment. Periodic training should take place to maintain competency and awareness. Additional training should occur when there is a change in a workplace exposure or procedure or a change in a job assignment.

An effective training method is to pair a new employee with a highly experienced, safety-minded coworker so the new person can become familiar with the workplace, learn the

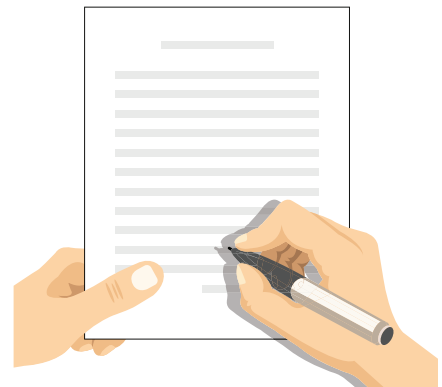
skills needed, and observe someone following proper safety procedures and correctly using safety equipment. This approach teaches the new employee that working safely is expected and routinely accomplished and that shortcuts are not tolerated.

### Element 6 – Incident and Accident Reporting, Investigation, and Analysis

In Section 1, the distinction between an incident and an accident was discussed, but it is crucial to recall the difference between these two terms. Simply put, an incident is an event that disrupts normal activities and can potentially become a loss or a claim; it is a “near miss.”

An accident is an event resulting in injury or damage to a person or property that has or will become a loss or claim. Accidents also occur at a particular time and place.

Accidents, like history, are often repeated. Consequently, it is important to investigate accidents to identify the causal factors involved and to determine any changes that need to be implemented, whether they are related to employee behavior or physical property/equipment.



Investigating accidents also leads to a reduction in employee and equipment downtime and expenses. All accidents that cause bodily injury or property damage, all OSHA recordable injuries, all first-aid cases, and all close calls or near misses should be investigated. It is essential that management makes it clear to everyone that the purpose of investigating accidents is not to assign blame but to protect employees. The management team sets the tone.

#### Investigation Guidelines



When investigating an accident, a standardized reporting form should be used so that all investigations are conducted in a consistent manner. The best time to investigate an accident is immediately afterward, as the facts are more easily discerned and the details are fresh. Accident reports should be completed within the first 24 hours of the event.

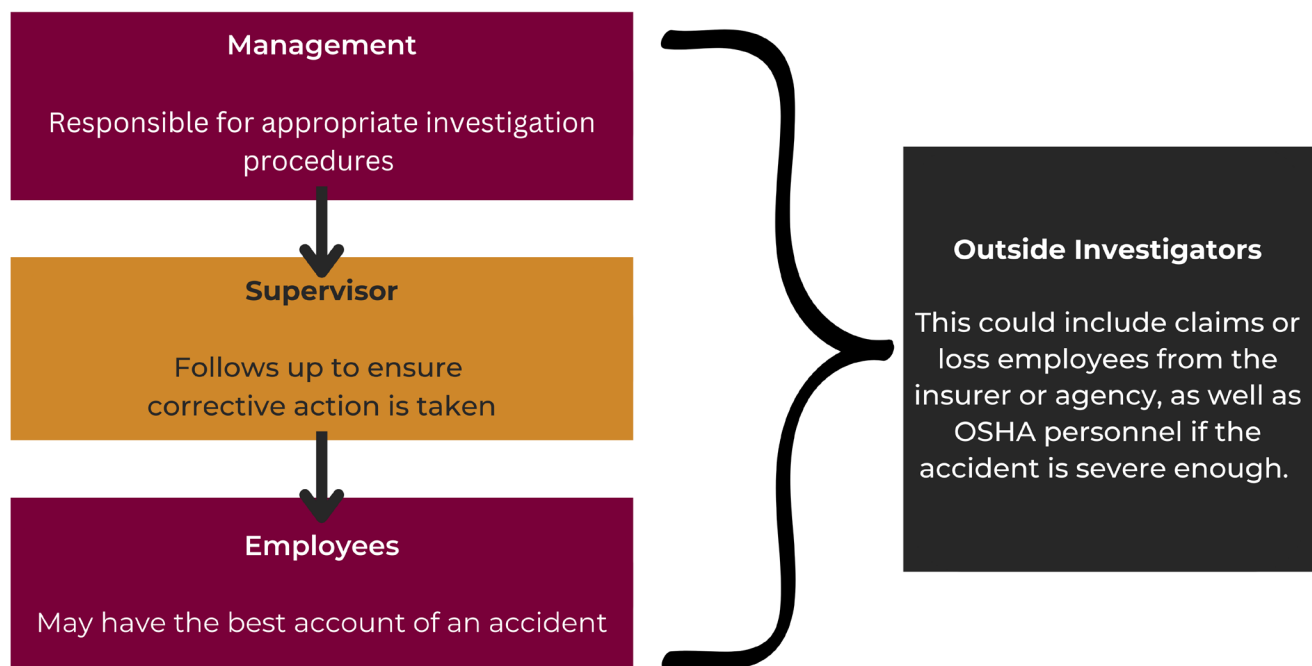
This ensures that the causes of the accident and any witnesses are available. In addition, it limits time for gossiping, creating excuses, changing narratives, and assigning blame. Also, if an accident occurred outdoors, it provides a greater potential for any evidence at the accident site to be unaffected by weather conditions. The actual accident site should be secured as soon as possible after all necessary emergency actions have been taken, and someone should be assigned to take photographs to document the details.

### Parties in the Investigation

Depending on the severity of an accident, there may be multiple individuals or groups involved in the investigation. The supervisor has intimate knowledge of job conditions and procedures in the department and is responsible for promoting and enforcing safe behavior. The employee or fellow employees may have the best account of the accident, but those accounts might be misleading to avoid discipline or to maintain relationships. That is why management should make it clear to all employees that the purpose of investigations is not to place blame but to determine and correct the cause(s).



The Safety Committee or Accident Review Committee is charged with having an unbiased perspective on the accident and can include multiple areas of expertise to determine the cause(s). The supervisor should follow up to ensure corrective action is taken. Management is ultimately responsible for appropriate, credible, and defensible investigation procedures. Outside experts with specialized knowledge may be called in for more complex situations. This could include claims or loss control representatives from the agent/broker or insurance carrier.



OSHA may investigate the accident depending on how severe it is. OSHA may also become involved if the accident involves a fatality or an employee files a complaint. In some jurisdictions, OSHA agencies have a consulting division to assist employers with identifying compliance needs, provided the employer is committed to corrective action.

### Interviewing Witnesses

When conducting interviews, the first step would be to identify who should be interviewed. In general, an investigation should interview the following individuals:

## Section 2: Risk Control and Mitigation - Human Resources

- Anyone who saw the events leading up to the accident
- Eyewitnesses who were involved in the accident or who saw it happen
- Individuals who came to the scene after the accident
- Anyone with information about the work habits of the injured employee
- Any employees with knowledge about the equipment involved in the accident

When these individuals are identified and interviewed, it is important that all witnesses are interviewed privately. Always begin accident/incident investigation interviews positively by emphasizing the purpose—not to find fault or assign blame but to identify ways to prevent the reoccurrence of situations in which employees might be injured.



It is also important to remember the limitations of interviewing witnesses. There is an old story of several blind men and an elephant. Each man observed the elephant by holding a different part (a leg, a tail, an ear, and so on) and pictured an entirely different animal based on their limited perspectives. Similarly, individual witnesses may not be able to provide a complete picture for several reasons. Most witnesses are not trained observers and may have only

seen a few details and imagined the rest. Some witnesses may intentionally give the wrong information to protect themselves or a fellow employee. The witness's own personality and perspective may also distort their account of an accident. For these reasons, only after the entire investigation has been conducted and the evidence is compiled can an accurate picture of what happened be ascertained.

When conducting the interview, it should be done with the perspective this may be the only chance to speak with the witness; therefore, the interviewer should be prepared beforehand with pertinent questions to gather the most accurate information in the allotted time. Avoid asking "why" questions because these questions can lead to a defensive attitude. It is better to ask open-ended questions that cannot be answered with a simple "yes" or "no," but it is also important not to lead or influence the witness. Finally, ask the witness for suggestions to prevent future incidents and conclude the interview positively by re-emphasizing the need for prevention and not finding fault.



### Final Investigation Report



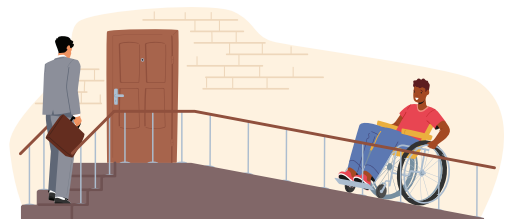
The final investigation report should be complete and thorough. Entries should be clearly stated and provide insight into the cause of the accident. Recommendations for prevention could include engineering controls, administrative controls, human resources' hiring and placement procedures, as well as training and discipline recommendations.

There should be a documented follow-up mechanism that provides for auditing by management or risk management, including the content of the report and the recommended remedies.

To recap, the benefits of a well-performed investigation are numerous. To mention a few, the investigation demonstrates concern and commitment on behalf of the organization and its management. It also identifies the root causes and can reduce or prevent future accidents by pinpointing flaws in the safety program. It improves current job procedures, and it certainly reduces the economic impact of accidents.

### Element 7 – Post-injury Management

Post-injury management is essential to reduce healthcare and workers compensation costs, reduce lost work time, provide for an early evaluation of the injury, and improve employee morale. It is also important for addressing any legal issues that may develop from the Americans with Disabilities Act (ADA), Family Medical Leave Act (FMLA), or any other governmental regulation dealing with employee injuries. Post-injury management enables the employer to maintain contact with the injured worker and ensure the worker's return to light, transitional, or modified duty as soon as possible. It is an important tool for making sure the injured worker does not feel abandoned or neglected after an injury.



A team that includes the supervisor, management, medical provider, claims adjuster, and injured employee should be involved in the post-injury management. A written policy and procedure should be developed that includes chapters on return-to-work (with coordinator or administrator and supervisor involvement) and ongoing employee training that includes instruction on workers compensation benefits, accident reporting procedures, established/approved medical providers if law permits, and return-to-modified-duty procedures. It is valuable to be able to direct care of injured employees to a designated medical provider because the provider can develop a familiarity with the organization's operations, understand the organization's treatment and return-to-work philosophy, and can assist the organization with disability management. Insurers sometimes require the use of their own approved medical providers.



In most organizations, the insurance company, a third-party administrator, or an in-house claims adjuster handles the claims. Regardless of who handles the claim, elements of successful claim handling include communication about claim status, physician referral, addressing the organization's return-to-work philosophy and availability of modified duty, medical cost containment activities, and recovery or subrogation from negligent third parties. There should be continuous communication among the employee, the medical provider, and the claims handler, particularly with respect to physical therapy, vocational counseling, and disability management.

## Check-In



An employee slipped and fell down a flight of stairs at work. He broke his leg and is in a cast and on crutches. The employee's office is upstairs in the building, but he has frequent meetings on the ground level. He goes to a printing and filing room multiple times per day. What available job accommodations might a risk manager provide for the employee to be able to return to work sooner?

---

---

---

---

## Element 8 – Evaluation of Program Effectiveness

The risk manager must make sure the program is effective and appropriate for workplace conditions. This should be a formal evaluation process with documented results. Either internal or external resources could be used. Financial information and incidence rates from insurers and other sources, such as OSHA, can serve as the statistical measurements used to evaluate the program's effectiveness. This could include examining premium credits and debits and analyzing insured losses per exposure unit and claim frequency and severity.



### Measurements

Insurance and information, such as credits/debits, experience modifiers, loss rates, and frequency/severity, may be available on an industry-wide basis. OSHA or U.S. Bureau of Labor Statistics (BLS) incidence rates are easily accessible for comparison. Some measurements used by both OSHA and the BLS can be calculated with the following formulas.

The **Total Recordable Injury Rate (TRIR)** applies to any work-related injury beyond first aid and is calculated with the following formula:

$$\frac{\text{\# of cases of injury and illness} \times 200,000}{\text{\# of hours worked by all employees in a given year}}$$

**Days Away, Restricted, and Transfer Rate (DART)** is a BLS statistical measure of injury and illness cases involving days away, restricted duties, or transfer to other duties during the return-to-work phase. It is calculated with the following formula.

$$\frac{\text{\textit{\# of DART cases} \times 200,000}}{\text{\textit{\# of hours worked by all employees in a given year}}}$$

**Note:** DART is an acronym for **D**ays **A**way from work, **R**estricted duty, and days of job **T**ransfer due to injury or illness. The data used to calculate the formula is found in columns H and I of OSHA Form 300a. OSHA publishes DART rates from its statistics so employers can compare their DART rates to others.

[The Bureau of Labor Statistics also provides a calculator and comparison tool on its website.](#)

### ▶▶ Knowledge Check



**Directions:** Read the scenario described on the left. In the right column, identify the element of a health and safety program that should be addressed, and provide a recommendation to remedy the situation.

1. A construction company has established the required PPE needed to enter the job site and has posted signage at the entrance to the job site instructing workers what to wear. Management is frequently seen wearing improper PPE.	
2. An auto parts manufacturer has an established safety protocol. However, it is unclear who is responsible for enforcement. There is rarely any consequence for employees operating outside the safety guidelines.	
3. Upper management at the auto parts manufacturer, dismayed at the high rate of incidents on the job, decides to implement a new safety protocol. After walking the floor, high-level management independently comes up with a new safety protocol. Despite the new rules, employee accidents continue.	



## Section 2: Risk Control and Mitigation - Human Resources

<p>4. A worker is injured during their shift at a chemical factory. They are out for weeks, but their injury has improved. The employee is unsure when they will return to work and what their role will be as they recover.</p> <p>Following the injury, the chemical factory implements a strict, zero-tolerance policy regarding the use of proper PPE. Any employee seen not wearing the appropriate equipment is reprimanded immediately. Management notices that workers are frustrated and are not sure that individuals are complying when management is not around.</p>	
<p>5. A widgets factory recently purchased a new piece of machinery to speed up production. Employees are somewhat comfortable with the new equipment, but the manager observes several employees using the machinery in unsafe ways.</p>	
<p>6. A construction company is investigating a serious accident where a worker fell from a scaffolding and became disabled. When interviewing individuals, management emphasized the serious nature of the accident and that people who are at fault will be held accountable. After interviewing several individuals, management still lacks a clear picture of how the accident occurred.</p>	
<p>7. A company has implemented a new health and safety program. So far, they have noticed a reduction in accidents but want to use a metric to compare their rate of accidents to other similar workplaces.</p>	

# Ergonomics

## Learning Objective:

2.5 Define the term “ergonomics” and describe the risk control methods associated with ergonomic issues.

In addition to health and safety, ergonomics is another important aspect in controlling the frequency and severity of losses an organization must address. Over time, this has become an increasingly significant human resource exposure.

The word “ergonomics” is derived from the Greek words *ergon* (work) and *nomy* (laws). Thus, ergonomics are the “laws of work.” The *American Heritage Dictionary* further defines ergonomics as:



“Design factors, as for the workplace, intended to maximize productivity by minimizing operator fatigue and discomfort.”

In simpler terms, ergonomics involves studying human characteristics for the most appropriate design of the living and work environment. Stated another way, it is fitting the physical work environment to the person rather than expecting the person to adapt to the work environment.

The cost to employers for injuries due to inappropriate workplace designs is disproportionate to the cost of adapting the workspace. The number of ergonomic injury cases and resulting costs are increasing at an alarming rate.



## Ergonomic Risk Factors and Control Methods



Ergonomic injuries usually result from long-term exposure to repetitive or forceful actions and generally cause injuries to muscles, nerves, and tendons. These types of injuries are also known as musculoskeletal disorders. The risk factors most likely to cause these ergonomic injuries are performing repetitive tasks, using excessive force, performing work in an awkward posture, static loading (maintaining a tense, still posture), working in an extreme temperature environment, and vibration. The following table looks at each risk factor and potential control methods that could be used to address various ergonomic risks.

Potential Issues	Risk Control Methods
<b>Repetitive Tasks</b>	
Repetitive tasks are motions repeated throughout the work shift. The highest risk factors are found in jobs in which there are 2,000 or more repetitions per hour. This can be compounded in a job that allows few or no breaks because there is no recovery time for the muscles and tendons. Employees who work at least 50% of a work shift in this type of environment are at an increased risk of injury.	Automation, scheduling more frequent short breaks, and encouraging stretching and exercise are risk control measures to reduce repetitive task injuries.
<b>Excessive Force</b>	
This risk factor can affect small and large muscle groups as well as isolated tissues. This occurs when a high amount of physical energy is required to complete a task, such as pulling or pushing a heavy load.	Measures that reduce or spread the force provide relief for affected muscle groups. To minimize injuries related to this risk factor, mechanical aids can be substituted when possible. The workplace can also be redesigned, and the worker can be encouraged to minimize reaching, bending, and/or overhead lifting.
<b>Awkward, Deviated Position</b>	
This risk factor arises from employees working while their bodies are deviating from a neutral position in their wrists, arms, trunk, neck, shoulders, legs, or feet. As the angle of deviation increases, discomfort and injury potentially increase. Two common sources of awkward posture are overhead and extended reaching.	Awkward posture can be resolved with the use of stepping stools, ladders, raising or lowering surfaces, or a redesign of the workplace. Reaching, bending, and/or lifting overhead should be minimized, if possible.
<b>Static Loading</b>	
This is a sustained exertion of the muscles that causes decreased blood flow to the muscles and leads to general fatigue and discomfort. This can result from maintaining a constant posture or position or trying to use hands as a fixture or tool. Applying pressure to certain points of the body, such as at the wrists, is a type of static load.	Saloon keepers and pub operators learned long ago that patrons would stay longer and purchase more products if they could stand with one leg slightly elevated: hence, the bar rail. Risk control measures for this risk factor include a possible redesign of the workplace, use of footrests, arm and wrist rests, use of fixtures for holding and gripping, and less reaching, bending, and/or overhead lifting, if possible.

Potential Issues	Risk Control Methods
<b>Personal Risk Factors</b>	
These are physical attributes that contribute to ergonomic injuries. They include characteristics like an employee's physical condition, age, weight, disability, flexibility, general health, outside activities, proper work methods, education, and stress.	Ensure the height of the work surface accommodates the employee's height. Job rotation will allow an employee to rest between periods of intense activity. Employers can ensure an employee's fitness for duty by providing the employee's physician with a Job Safety Analysis and typical physical demands.
<b>Extreme Temperature Environments</b>	
Both high and low temperature extremes can give rise to employee injury and illness. High extremes can give rise to dehydration, heat exhaustion, and heat stroke, as well as excessive perspiration that can cause grips to slip. Low extremes cause muscles to contract and hypothermia or frostbite to occur.	Workers should be trained to recognize risk factors associated with extreme temperatures and be aware of proper work methods and incident reporting procedures when an incident does occur. They should be sure to take breaks and continuously monitor the work environment to proactively identify the risk factors.

The following graphic summarizes the various ergonomic risk factors. Take some time to review them.

## GENERAL ERGONOMIC RISK FACTORS



### **Repetition**

Performing the same motion or task over and over again, usually for hours at a time, with no breaks or a cycle time allowing limited recovery, further increases the likelihood of injury.



### **Excessive Force/Excessive Load**

When a high amount of physical effort is required to complete a task, such as lifting heavy loads, pushing heavy loads with a hand truck, or pulling hard to loosen a bolt, etc., the likelihood of injury is increased.



### **Awkward or Deviated Posture (Reaching)**

Extreme ranges of motion and deviations from the neutral posture (body properly aligned, placing minimal stress on joints, muscles, tendons, and nerves) put additional stress on the body.



### **Static Load**

The discomfort, tension, and fatigue created by the physical exertion of maintaining a constant posture or position may lead to stress or strain injuries.



### **Personal Risk Factors**

Contributing factors such as physical conditions (hypermobile joints, diabetes, etc.), fitness, outside activities, improper work methods, or physical/emotional stress make some individuals more prone to injury.



### **Environmental Risk Factors**

Extreme temperatures, loud noises, poor lighting, vibration, inadequate training or inappropriate equipment, machinery, or furniture make work more dangerous.

## Ergonomic Risk Factors of Technology

Technology is now a standard tool in almost every industry. The increased number of computer users and hours spent in front of a computer screen have led to a rapidly growing variety of computer-related health concerns.



Computer workstation risk is one of the major sources of cumulative stress and force in the workplace. While the process of using a computer keyboard seems ergonomic, issues associated with computer workstations are serious and often unrecognized. Because a significant number of workers use computer workstations, improperly designed areas can be a major source of loss costs. A poorly designed computer workstation can cause eyestrain, blurred vision, headaches, fatigue, and stress. The risk factors for a computer workstation are much the same as those for other types of workstations: repetitive activity, awkward posture, static loading, pressure on tissues, and personal factors such as individual physiology/stress.

### Typical Issues Related to Prolonged Computer Usage

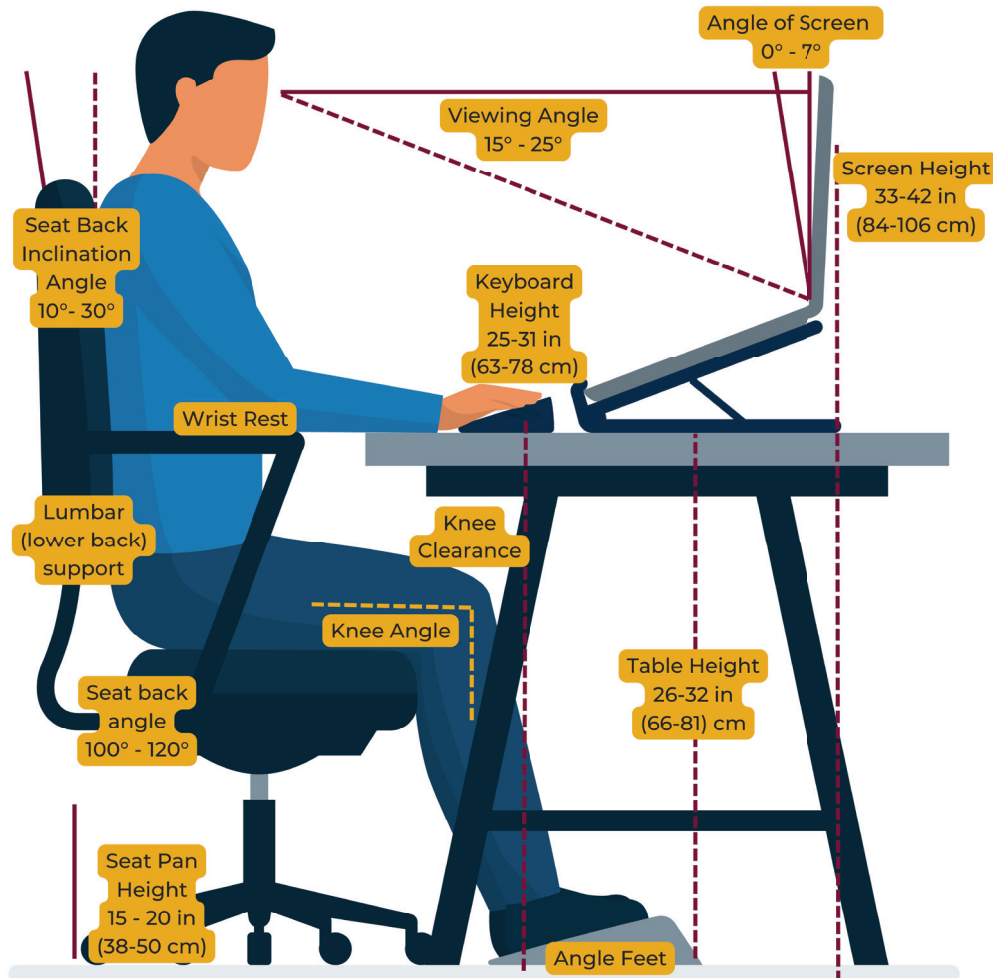
Like other repetitive activities, prolonged computer use can cause injury to workers. Some common issues include:

- Repetitive stress injuries – carpal tunnel syndrome and “texting thumb” that lead to pain, numbness, stiffness, etc.
- Vision problems – eye strain, dry eye, blurred vision, and computer vision syndrome
- Headaches – caused by posture, vision strain, stress, etc.
- A sedentary lifestyle – can lead to medical problems like obesity and deep vein thrombosis (blood clots due to immobility)
- Musculoskeletal – stress on hands, shoulders, neck, back, legs
- Fatigue and stress disorders – can impact behavior and emotions; resulting from work pressure, job environment
- Sleep disorders – too much artificial light from computers and cell phones affecting the body’s melatonin production and natural sleep/wake cycles



## Risk Control for Prolonged Computer Usage

Hazard controls for computer workstations include adjustable table and monitor heights, footrests, ergonomic chairs, and wrist pads. View the diagram for an example of how a computer workstation can be modified to avoid ergonomic injury.



Hazard controls also include workspace organization, job enlargement (expanding the job to include activities that provide a break from repetitive activity, awkward posture, static loading, etc.), frequent breaks, stretching and exercise, adequate lighting and glare control, and noise control.

## Section 2: Risk Control and Mitigation - Human Resources

Administrative controls include frequent work breaks, job design factors, educating employees on proper work methods, monitoring the work environment, early intervention, exercise, and stress reduction measures. Consider an example:

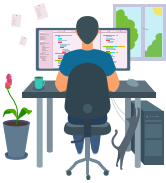


Allie works in a new customer service center handling complaints and documenting all activity in the company computer system. She handles as many as 25 complaints per hour.

Allie and her coworkers have quotas outlining the number of complaints and types of resolution required on a per-shift basis. After being open for a few months, several of her coworkers complain about wrist pain and the intensity of the requirements. The employer is concerned and hires a consultant who makes several recommendations. Among them is cross-training the phone operators and the filing clerks and having the members of both teams work half-days in each department. In this case, the risk is controlled through job enlargement.



### Knowledge Check



Louisa owns a small travel agency. During the COVID health emergency, all her employees were allowed to work from home. After a couple of months, several employees were complaining of arm and shoulder discomfort. Describe some steps that Louisa could take to determine causes and some control measures she could put into place for her telecommuting staff.



---

---

---

---



# Manual Material Handling

## Learning Objective:

2.6 Identify the risk factors and risk control measures associated with manual material handling and lifting.

Manual material handling creates a multi-faceted ergonomic hazard, as some injuries arise from continued exposure to ergonomic forces, often called cumulative trauma disorders (CTDs), while other hazards result in a sudden occurrence. However, many of the “sudden occurrences” are the result of continued exposure. Still, the worker may not realize the buildup of “mini injuries” waiting for that one extra push, pull, stretch, or strain to cross the line from unnoticeable to suddenly painful.



With respect to manual material handling exposures, these injuries typically are torso injuries located in the lower back or shoulders, commonly diagnosed as lower back strains/sprains and shoulder strains. Sprains/strains to knees, elbows, and wrists can also occur. The difference between a strain and a sprain is a matter of degree; both involve the same type of causation and injury. A strain is a tearing or stretching of muscles or tendons (particularly at the point where the muscle becomes a tendon), some of which are instant, while others are chronic and the result of long-term overuse or stress. A sprain is a ligament or joint capsule injury involving tearing or stretching. Ligaments and capsules provide joint stability, so weakening or tearing can create long-term instability. Sprains occur when a joint is forced beyond its usual range of motion. This exposure and these injuries ultimately lead to increased costs in the form of workers compensation, medical coverage, lost wages, etc.

## Risk Factors

### Frequency of Lifts

Manual lifting is a common workplace exposure, and the more frequent the lifts, the greater the exposure. There are two components of lift frequency that are risk factors: the number of lifts in a given time period and the duration of a single lift. If there is insufficient time for recovery between lifts, stress and overuse can accumulate in the muscles and tendons. If the duration of the lift is excessive, stress accumulates rapidly in the muscles and tendons involved in the lift.



A simple experiment can show how this works. Extend your arms and lift a dining room chair from waist-high to shoulder-high repeatedly over 30-seconds. Observe how your muscles feel. Then hold the chair at arm’s length, as if you were lifting it, and then hold it steady, simulating a long duration of one lift. You will notice your arm muscles beginning to tremble in a few seconds.

## Excessive Force Due to Load Weight

Manual material handling means more than lifting; it also includes moving materials by pushing or pulling. Excessive weights require more force to push or pull and to lift.

## Awkward Body Posture

Awkward body position or posture arises from the load's shape and size. Lifting a box or crate 36 inches long and 18 inches wide with no handles is problematic, as getting a comfortable grip on a surface without using two or more of the sharp edges that concentrate pressure on muscles and tendons is difficult. Asymmetrical objects are also challenging to lift.

## Improper Lifting Techniques

Improper lifting techniques (twisting, reaching, and bending) are risk factors due to the location of the material being moved and the location to which the material will be transferred.



For example, lifting an item from the floor located on the worker's right and moving it to an overhead shelf on the left means the worker must bend far over or squat, lift the item off the floor and twist or move the feet from right to left, then lift the item overhead and stretch to place it in the intended position.



## Personal Risk Factors

Personal risk factors usually arise from non-occupational causes. Workers, as individuals, differ in age, gender, and physical condition. Younger workers are more resilient physically, as their bodies have not accumulated the normal stress and strain of the aging process, not to mention the increased stress and strain of work. However, they have less life experience and may be more likely to take chances or engage in unsafe practices. The tasks being performed are also significant factors when it comes to the types of injuries that are most common. Individuals who work on computers are at greater risk of experiencing carpal tunnel syndrome, while workers who lift boxes from the floor more often have lower back injuries and work-related repetitive motion injuries. Physical condition is also an important factor, as workers in poor physical condition tend to tire more quickly and have less strength and flexibility.

## The NIOSH Lifting Equation



To quantify the risks associated with a lifting task, NIOSH (The National Institute for Occupational Safety and Health) has created a lifting equation. This equation can be used to calculate the overall risk index for single and multiple manual lifting tasks.

## Section 2: Risk Control and Mitigation - Human Resources

The equation outputs a composite lifting index (CLI). Any lifting task with an index greater than 1.0 is potentially unsafe and should be modified until the index is less than 1.0

In 2021, NIOSH revised its lifting equation. Along with the revision, NIOSH developed a cloud-based application (NLE Calc) that provides risk estimates to help evaluate lifting tasks and reduce the incidence of lower-back injuries in workers. The key benefits of using the application are:

- It calculates the composite lifting index (CLI) for multiple lifting tasks.
- It uses equations approved by NIOSH ergonomists, who were the original creators of the NIOSH Lifting Equation (NLE).
- It promotes better musculoskeletal health.
- It raises workers' awareness about their job tasks.
- It helps workers make informed decisions about the potential hazards to their musculoskeletal health.
- It provides job design guidelines for manual lifting tasks.
- It can be used as a research tool to collect manual lifting data.

For more information and an instruction manual, visit: NIOSH Lifting Equation App: NLE Calc | NIOSH | CDC. [cdc.gov/niosh/topics/ergonomics/nlecalc.html](https://cdc.gov/niosh/topics/ergonomics/nlecalc.html)

The NIOSH Lifting Equation can also be used to determine the recommended weight limit for any lifting task. The equation is:

$$\text{RWL} = \text{LC} \times \text{HM} \times \text{VM} \times \text{DM} \times \text{AM} \times \text{FM} \times \text{CM}$$

**LC** – Load Constant

**HM** – Horizontal Multiplier (horizontal distance)

**VM** – Vertical Multiplier (vertical distance)

**DM** – Distance Multiplier (travel distance)

**AM** – Asymmetric Multiplier (asymmetry or twisting of body)

**FM** – Frequency Multiplier (frequency of lift)

**CM** – Coupling Multiplier (coupling strength or grip)



Understanding the factors included in the lifting equation can give a risk manager insight into effective lifting hazard control methods without necessarily needing to arrive at an exact calculation.

## Section 2: Risk Control and Mitigation - Human Resources

Review the following table. The left column describes a factor in the lifting equation. The middle and right columns describe two different scenarios. For each factor, circle the scenario that would be **more likely** to cause an accident.

Circle the scenario that poses a higher risk of an accident.		
Lifting Factor	Scenario One	Scenario Two
<b>Load Weight</b> - Limiting the load weight reduces the hazard.	Lifting a single 50-pound weight	Lifting two 25-pound weights separately
<b>Frequency</b> - Reducing the number and duration of lifts of a given weight permits recovery between lifts and reduces the stress during a lift.	Lifting a 25-pound weight every ten seconds and holding it for ten seconds	Lifting a 25-pound weight every twenty seconds and holding it for five seconds
<b>Horizontal distance</b> - Holding the load closer to the torso reduces stress in the arms and shoulders.	Holding a 25-pound weight extended at arm's length (perhaps because of the shape of the object)	Holding the same 25-pound weight close to the torso
<b>Vertical distance</b> - Reducing the vertical distance of the lift reduces stress.	Lifting a 25-pound weight from the floor to a shoulder-high shelf	Lifting the same weight from a waist-high table to a shoulder-high shelf
<b>Distance the load travels</b> - Reducing the distance the load travels reduces the stress.	Moving a 25-pound weight 24 inches	Moving a 25-pound weight 12 inches
<b>Asymmetry</b> - Reducing twisting or rotation of the legs, knees, hips, torso, shoulders, etc., reduces the stress on muscles, tendons, and joints.	Lifting a 25-pound weight and turning 180 degrees to place it on a shelf	Lifting a 25-pound weight and turning 10 degrees to place it on a shelf
<b>Coupling strength</b> - Increasing the coupling strength or quality of the grasp reduces stress on the hands and lessens the likelihood of the load slipping or shifting.	Lifting a 25-pound weight with slick slides	Lifting a 25-pound weight with handles



For every factor in the preceding exercise, the scenario posing a higher risk of an accident is Scenario One. While NIOSH reduced these factors to a mathematical formula, common sense tells the risk manager that taking steps to reduce weight, frequency, distance, and asymmetry or increasing coupling strength will reduce the likelihood of accidents arising from manual material handling. This understanding should be applied when creating risk control measures for manual material handling and lifting.

## Risk Control Measures for Manual Material Handling and Lifting

### Planning the Lift

The most important hazard control technique is planning before the lift. Planning before the lift is not just a matter of looking at the load and thinking about how to move it from one point to another. Planning before the lift, like all planning, involves administrative control. The factors discussed previously should be used when planning how many lifts will be made in a specified time period, how much weight will be lifted, and what mechanical aids might be used to implement or supplement the lift.

### Mechanical Aids

The last component of material handling involves the use of mechanical aids. Conveyors that move materials from a loading area to an assembly area eliminate much of the manual lifting hazard (weight, frequency, distance, and asymmetry are zero). Hand trucks and pallet trucks eliminate much of the distance traveled while carrying the weight. Using hand tools that are suspended above the work area requires less effort to pull these items into place than repeatedly picking up the same tool, and having the tool within ready reach of the work surface reduces asymmetry.

One mechanical aid deserves special attention—the back belt. There is considerable controversy over the efficacy of back belts.





According to NIOSH publication 94-127<sup>3</sup>, these devices provide no physiological protection. Back belt programs are most effective when accompanied by a material handling education program—not just passing the belts out with an instruction to wear them. When properly worn, the belt’s design leads an individual think before the lift, thus planning the lift.

## ▶▶ Knowledge Check



Robert’s Fine Seafoods is a luxury restaurant. They receive multiple shipments daily of fresh seafood at the loading dock located about 50 feet from their walk-in fridge. The average weight of the shipments is 25–50 pounds. Employees must bend down to floor level to pick up the boxes and place them on shelves in the walk-in fridge.

List three risk control measures the restaurant could take to reduce the likelihood of an employee injury.

---

---

---

---

---

<sup>3</sup> Bureau of Epidemiology, Division of Surveillance, Hazard Evaluations, and Field Studies, National Institute for Occupational Safety and Health (NIOSH). “Occupational Noise Exposure: Bibliography.” Centers for Disease Control and Prevention (CDC). Last modified 1994. Accessed July 12, 2023. <https://www.cdc.gov/niosh/docs/94-127/default.html>

# Substance Abuse in the Workplace

## Learning Objective:

2.7 Describe the benefits and possible legal problems associated with a workplace substance abuse program.

Substance abuse involves both illegal and legal drugs and can occur on and/or off-duty. Managers should be trained in how to identify any residual effects, both short-term and long-term, of any drug that can impair a worker and ultimately affect the workplace.

Legal drugs (prescription drugs and over-the-counter medication) can be abused for the same intent as illegal drugs or simply misused by overdosing. Both abuse and misuse can result in impairments. Further, regular or required use of legal drugs can result in drowsiness, sleepiness, agitation, and even hallucinations. A reading of the side effects listed on prescription documents and containers often includes a warning to refrain from operating motor vehicles or power equipment until the user knows the individual effects.



The problem of legal drug use is compounded by privacy measures implemented by the Health Insurance Portability and Accountability Act (HIPAA). Employers may ask about an employee's use of medication. However, while a medication may be legal, it can still create the risk of harm to others when side effects cause impairment to the employee—particularly when they are operating equipment or a motor vehicle.

This may lead risk managers to believe that they are powerless to address the problems created by legal and over-the-counter (OTC) drug use in the workplace. However, no federal law states that an employer cannot educate and alert employees to the hazards of legal or OTC drug-induced impairments and encourage them to use common sense when performing their work while using legal and OTC medications.



Another legal substance commonly abused is alcohol, both while on duty and for recreational purposes. This is particularly problematic for certain occupational tasks, such as involvement in transportation (planes, trains, automobiles, and ships), emergency services, medical care, and many other sensitive activities. Risk managers should also encourage employers to take steps to prevent the inappropriate use of alcohol.



## Benefits of a Substance Abuse Program for the Organization

When an organization adopts an effective workplace substance abuse program, it can expect to receive several benefits. Organizations with a workplace program should expect to see increased productivity because workers are not impaired, absenteeism is reduced, and employee turnover is lessened. They should also anticipate fewer accidents (reduced impairment) and employee-related crime. The cost of financing the workers compensation exposure (which may include insurance premium credits) and providing health care should also be reduced. Last, the organization would be in compliance with the Drug-Free Workplace Act and other applicable legislation, particularly when transportation is involved.



Organizations that have federal contracts with a value of \$100,000 or those receiving a federal grant of any size must comply with the Drug-Free Workplace Act of 1988, amended in 1994 (41 U.S.C. 81). The key provisions of the Drug-Free Workplace Act include the following:

- Employers must have a published policy prohibiting the possession, use, distribution, and manufacture of controlled drugs on the premises.
- Employees must be made aware of the program content.
- A rehabilitation and counseling program must be provided.
- Penalties for workplace violations are stated clearly.
- Employees must be given a copy of the workplace substance abuse policy.

If an organization does not comply with these requirements, the organization cannot enter a federal contract of \$100,000 or more or receive a federal grant of any size. Compliance with the Act has the benefit of accessing federal funds.

## General Risk Control Measures

As in all risk control programs, clearly stated policies and procedures are essential. This includes clearly stated drug and alcohol testing protocols with details on testing procedures, use of qualified laboratories, and evaluation of test results. Examples of common policy and procedure statements are those such as:

- Individuals who abuse illicit or legal drugs without a prescription will not be hired.
- The use or presence of illegal drugs or alcohol is prohibited on the premises.
- Employees must report to work “fit for duty.”
- Management will notify appropriate authorities about any illegal drug use.



## Section 2: Risk Control and Mitigation - Human Resources

- Employees will not be terminated or subjected to discipline for seeking assistance under an Employee Assistance Program.
- There are procedures regarding voluntary notification to management when prescription drugs are being taken that may affect safety or interfere with job performance.

An organization should also have clear drug and alcohol testing protocols. Some statements (and example policy wording) are discussed on the following pages. The language shown here is for educational purposes only and should not be used in an actual workplace.

### 1. Employee consent for testing is a condition of employment.

#### SAMPLE LANGUAGE

All employees, as a condition of employment, are required to provide consent for drug and alcohol testing. Failure to consent may result in disciplinary action up to and including termination. By providing consent, employees agree to be tested for drugs and alcohol as outlined in this policy.

### 2. Testing will be conducted consistently without discrimination.

#### SAMPLE LANGUAGE

Drug and alcohol testing will be conducted consistently for all employees without discrimination. No employee will be singled out or targeted for testing based on personal characteristics such as race, gender, age, or any other protected category. Testing may be conducted on a random basis, following incidents or accidents, reasonable suspicion, as part of a pre-employment screening, or as required by law or company policy.

### 3. Statement of the drugs and substances covered by testing

#### SAMPLE LANGUAGE

The following drugs and substances are covered by testing:  
Illegal drugs, including but not limited to marijuana, cocaine, amphetamines, opioids, hallucinogens, and designer drugs.

### 4. Procedures for strict specimen control (chain of custody protocol)

#### SAMPLE LANGUAGE

Records will be maintained to document each person who has had custody or control of a specimen from its collection to the analytical laboratory, and the date and time of possession of each person involved in the process.

## 5. Use of reliable testing organizations

### SAMPLE LANGUAGE

Drug testing will be conducted by reputable and certified testing organizations that follow recognized testing methodologies. These organizations will comply with industry standards and guidelines for accuracy, reliability, and confidentiality.

## 6. Use of a medical review officer for evaluation of positive detections

### SAMPLE LANGUAGE

A qualified medical review officer (MRO) will be involved in the evaluation and interpretation of all positive detections. The MRO will review the test results and determine if there is a legitimate medical explanation for the positive result, such as the use of prescription medication. The MRO will maintain confidentiality and handle all medical information in compliance with applicable laws and regulations.

## 7. Test administration procedures and timing

This portion of the procedures should clarify when testing will be conducted.

### SAMPLE LANGUAGE

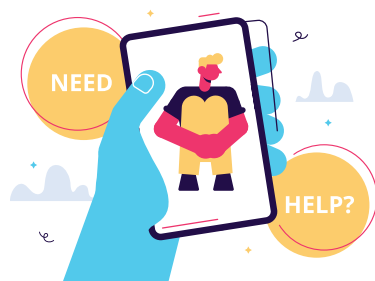
#### Test Administration Procedures and Timing

- a. **Pre-Employment and Pre-Hire Testing:** All job applicants will undergo drug testing as a condition of employment. This testing will occur after a job offer has been extended but before the individual begins working.
- b. **Random Testing for Sensitive Positions:** Employees in positions where safety is of utmost importance may be subject to random drug testing. The selection of employees for random testing will be conducted using a fair and unbiased process.
- c. **Required Routine Physicals:** As part of routine physical examinations, employees may be required to undergo drug testing. This may be conducted on a periodic basis to monitor the overall health and safety of employees.
- d. **Reasonable Suspicion:** If there is reasonable suspicion that an employee is under the influence of drugs or alcohol while on duty, they may be required to undergo testing. Reasonable suspicion may be based on specific observations, behavior, or other credible information.
- e. **Post-Accident or Post-Incident:** After an accident or incident that results in injury or property damage, involved employees may be required to undergo drug testing. This is to determine if substance use contributed to the event.
- f. **Just Cause:** In situations where there is evidence or reasonable belief of drug or alcohol use that violates company policies, employees may be required to undergo testing.
- g. **Treatment Follow-Up:** Employees who have tested positive for drugs or alcohol and have entered a treatment program may be subject to follow-up testing to ensure compliance with the program and ongoing recovery.

Administratively, there must be a substance abuse program training for managers, supervisors, and employees. The training program should include the following components:

Training for Managers and Supervisors	Training for Employees
<b>Program components and administration:</b> <ul style="list-style-type: none"> <li>• Recognition of signs and symptoms of substance abuse and impairment</li> <li>• Protection of employee rights and privacy</li> <li>• Incident handling and recordkeeping</li> <li>• Employee education programs and procedures</li> </ul>	<b>Explanation of roles, responsibilities, and limitations:</b> <ul style="list-style-type: none"> <li>• Adverse health effects of substance abuse</li> <li>• Details of the policies and procedures of the organization</li> <li>• Details of the drug-testing procedures and protocols</li> <li>• Enforcement provisions</li> <li>• Details of the Employee Assistance Program and its procedures</li> <li>• Signed acknowledgment of participation in education and acceptance of the substance abuse program</li> </ul>

### Employer Policy and the Employee Assistance Program



Adding to the usual problems of substance abuse are federal laws, particularly the Americans with Disabilities Act (ADA). The ADA considers drug addiction as a disability, and it is a two-edged sword. On the one hand, it *does not* provide protection for current users of drugs, permitting an employer to implement the drug-testing measures discussed previously. Ultimately, it is legal for an employer to fire or refuse to hire an employee for substance use.

On the other hand, the ADA *does* protect a former drug/alcohol abuser and a substance-abusing employee who voluntarily seeks assistance from the employer through an employee assistance program (EAP) from discrimination and discipline. To comply with legal requirements, the Employee Assistance Program should make the following statements:



- The focus of the EAP is correcting problems that affect employee performance.
- Participation in the EAP is voluntary and confidential.
- The administrator of the EAP is either an outside party (preferable) or in-house staff properly trained and able to function with confidentiality.
- Participation does not effect job security.
- EAP participation is offered as an alternative to discipline.
- Consistency in program application and administration will be maintained.

Tying back to the essential risk control techniques, we can view the substance abuse policy as follows:

Techniques	Example
<b>Avoidance</b>	Using drug testing and work sample tests as part of pre-hire employee screenings
<b>Prevention</b>	Having a written and implemented policy for operating as a drug-free workplace
<b>Reduction</b>	Providing wellness programs, EAPs, and other education on substance abuse
<b>Segregation/Separation/ Duplication</b>	Storing hazardous chemicals or medications in a secured location with limited access allowed
<b>Transfer</b>	Hosting an employee function, where alcohol is going to be served, off-site at a restaurant

## Legal Challenges with Substance Abuse Programs

Two significant challenges with implementing a substance abuse program are 1) inconsistent policies and procedures and 2) failing to act.

Policy and procedure problems often involve an inadequate chain of custody of specimens for testing and testing results.

Employees who are disciplined under the policies and procedures can counter with threats of litigation or complaints of slander or defamation, breach of confidentiality and privacy, inadequate recordkeeping, and illegal procedures. Above all, the employer and the risk manager must ensure that employee confidentiality is maintained and that only those in a “need to know” position receive the information.



## A Note on Cannabis



While marijuana use is still prohibited at the federal level, it is legal in seventeen states and the District of Columbia. An additional nineteen states allow its use for medical reasons. Marijuana legalization at the state level raises challenges for employers seeking to enforce their substance abuse policy. This becomes even stickier when the policies are required by Federal laws such as the Drug-Free Workplace Act. There are two main concerns when it comes to cannabis testing:

1. **Drug Testing** – Marijuana is detectable for several days after use. Traditional drug testing can be ineffective and even discriminatory in states where use is legal (or medically permitted). Employers who make employment decisions based on a positive finding may run the risk of litigation by the impacted employee.

2. **Medical use** – depending on the state law, employees who use marijuana to treat a disability may be able to request a reasonable accommodation.

### ▶▶ Knowledge Check



You are a supervisor in a warehouse. Your employees fulfill customer orders and prepare them for shipping. One of your employees recently suffered a back strain due to the nature of his job responsibilities. His physician has returned him to work with no restrictions and a prescription for a powerful pain medication. You are concerned about his fitness for work while taking the prescribed medicine. What are some steps you can take?

---

---

---

---

---

## Workplace Violence

### Learning Objective:

- 2.8 Name the risk factors and risk control measures used to prevent or reduce workplace violence.

Workplace violence is not a new phenomenon; it is as old as recorded history. What is new is the attention violence in the workplace has received in recent decades, particularly after a series of incidents involving employees of the U.S. Postal Service as early as 1983. The phrase “going postal” has entered the American lexicon as slang for extreme and uncontrollable anger, generally in the workplace. Some examples of workplace violence include active shooter situations, aggravated assault, homicides, intimidation, robberies/criminal intent, and terrorism/hate crimes.



There is no federal law establishing a duty to prevent workplace violence against employees. However, under the federal Occupational Safety and Health Act (OSHA), which regulates

workplace health and safety, an employer has a duty to provide a safe working environment. There is also an understood common law acceptance of a duty owed to keep others safe when on-premises.

The two sources of workplace violence are internal and external to the organization. Internal sources arise from an employee committing a violent act against a fellow employee or from an employee committing a violent act against a non-employee, such as a customer, vendor, contractor, or guest. External violence is imported into the workplace, such as a non-employee against an employee or a non-employee against another non-employee.

## Exposure Assessment

The risk manager must assess the exposures, perils, and hazards facing employees and non-employees in the workplace. One important indicator of the potential for workplace violence involves valuables, such as an operation that requires the exchange of money. Banks, currency exchanges, pawn shops, and charities that collect funds have ready access to cash in sufficient amounts to attract violent persons. Similarly, organizations that store, ship, or deliver high-value, portable goods are common targets.



Human-based perils and hazards arise from contact with the public, working with unstable or violent persons, working in high-crime areas, alone, late at night, and in areas with poor visibility or poor lighting. Working together, the risk manager and human resources manager can identify general employee risk factors that might indicate an employee may resort to violent acts committed against fellow employees or the public. Some of these factors will appear in resumes or job applications, such as gaps in employment, a false or incomplete application, or unfavorable or false references. Other factors may become apparent in job interviews, postings on social media, or after-work behavior.

## Possible Legal Problems for an Employer Arising from Workplace Violence



If an employee is the victim of workplace violence due to an outsider's actions, they may sue their employer in civil court for lack of safety and security in the workplace. The employer may be held legally liable for actual damages, pain and suffering, and punitive damages because of insufficient security and safety policies, procedures, and controls resulting in the employee's injuries.

Employers may also be faced with negligent hiring claims due to a lack of thorough pre-employment screenings (Fair Credit Reporting Act, ADA, criminal

background checks, etc.) when an employee commits an act of violence that injures a coworker or customer. Consider an example:



Peter comes home from school, and his mother sees that his arms are bruised. When she asks him what happened, he is silent. She speaks with her neighbor, who shares that her daughter, Alison, has similar bruises. Alison told her mother that the playground monitor often grabbed and even struck the children. A week later, the school calls and says there has been an accident, and Peter is being taken to the hospital. The X-ray reveals that his arm is broken in a “green-twig” fracture. Peter’s family sues the school for negligent supervision of the children on the playground. Peter admits that the monitor twisted and pulled on his arm. The monitor is now personally named in the lawsuit. During the investigation, it is discovered that the monitor has a history of child abuse. In the deposition, the district representative reveals that no background check was done before the monitor was hired. The lawsuit is now amended to include the school district and includes an allegation of negligent hiring and wanton disregard for the safety of a minor.

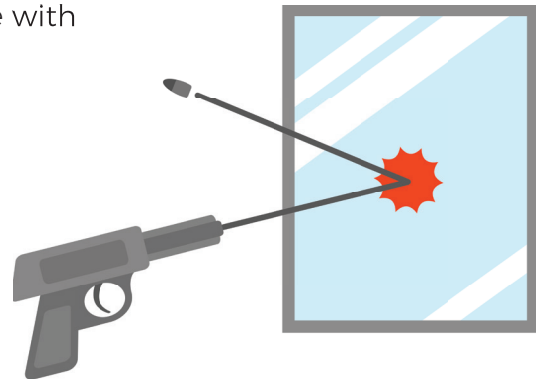
## General Risk Control Measures for Workplace Violence

General risk control measures can be grouped into five broad categories: physical, procedural, administrative, training, and evaluation.

### Physical Control Measures

This includes alarms, metal detectors, video surveillance with continuous recording, shatterproof or bullet-proof glass, enclosures and safe rooms, door locks, electronic key card systems, adequate lighting, and mirrors in blind walkways.

Depending upon the physical layout, escorts to parking lots or remote areas or a buddy system for employees working in remote areas may be appropriate. Signage such as “Driver has no cash,” “Cash is limited to \$50,” or “This area is under video surveillance” may also deter violent acts.



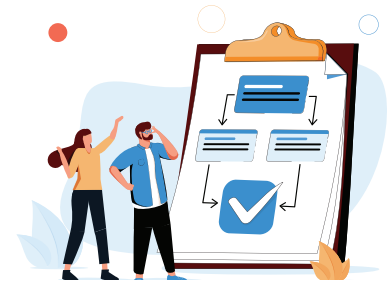
### Procedural Measures

These usually focus on the hiring process. Job interviews should be thorough, with reference and background checks for identity verification and criminal history. Credentials, education, and past employment history should be carefully checked for accuracy and completeness. The last procedural measure is pre-hire drug testing.



### Administrative Measures

Administrative measures begin with a written program. Written programs need a statement of management's commitment and are created with employee involvement. The organization's tolerance for violence should be stated clearly. For example, "zero-tolerance" is a popular phrase that came into common usage in 1994 following a federal law that required a school to expel any student who brought a gun to school at the risk of losing federal funding.



Another critical program element is the reporting process. All reporting should be prompt, with a comprehensive investigation immediately following all reported incidents and concluding with proper documentation. The anti-violence program must include a statement that there will be no reprisals in the event of reporting a violent act, and the organization must make a clear statement of its commitment to adequate security.

A second part of the administrative measures involves the creation of liaisons with police and other appropriate authorities and, if relevant, with an emergency response team within the organization. Access to the site must be controlled, and identification badges are an important element of creating and maintaining control of the site.

### Employee Training

Employees should be aware of the opportunity and procedure for anonymous reporting of suspicious acts or employee risk factors they have observed. Employees should be trained to identify risk factors and early warnings signs of the potential for violence. Training should also include emergency response procedures, ways to diffuse violent behavior, the location and operation of safety devices and safe rooms, and reporting/recordkeeping procedures.

### Program Evaluation

This is the final step in the workplace violence program. All records, including OSHA, medical, and incident reports should be reviewed to identify program deficiencies. Worksite assessments, employee reports of excessive behavior, and employee surveys and questionnaires must be evaluated. Last, the records of all training activities must be reviewed. Again, confidentiality is essential.





## ▶▶ Knowledge Check



A gas station in a neighborhood with increasing crime rates is worried about violence toward its employees. They have already implemented physical controls (video surveillance cameras, a bullet-proof panel between the cashier and customers at the check stand, and an under-the-counter button that will trigger a silent alarm) to control the risk of workplace violence. Explain three other risk control measures that could be used to improve the safety of employees at the gas station.

---

---

---

---

## Summary

An effective risk control program should engage all individuals within the organization. Without individuals to identify unsafe workplace behavior or hazardous conditions, accidents will happen. Likewise, any attempts by an organization to institute meaningful and effective risk controls are unlikely to succeed without the participation of people within the organization. Only when people are involved and engaged in the safety procedures will risk be controlled.

Most accidents and injuries arise from the following circumstances:

- Unsafe acts or behaviors
- Unsafe conditions
- Lack of awareness or training
- Uncontrollable events.

Accident prevention basics are used to control and reduce these exposures. There are six basics, with eliminating the hazard being the most effective (although it may not always be possible). In addition to accident prevention programs, workplaces should establish effective health and safety programs. To maximize their effectiveness, these programs should be designed with employee participation and training in mind.

Ergonomic risk factors are also an important contributor to accident frequency and severity. A risk manager should be able to identify ergonomic risk factors contributing to accidents and make recommendations to mitigate or control these risks.

More continuing and evolving risks in the workplace include workplace violence and substance abuse. These are affected by state and federal regulations, and there is no unique answer or control method for every possible situation, especially as these risks continue to change and evolve. General physical and administrative controls are provided in this Learning Guide.

## Section 2 Self-Quiz

**Directions:** Select the best answer for each of the following questions.

1. Why is it important to involve all members of an organization in the risk control process?
  - ☐ Lack of employee involvement in a safety program can upset shareholders.
  - ☐ Employee involvement in safety decisions is a legal requirement.
  - ☐ Individual employees are needed to help identify unsafe behaviors and hazards.
  - ☐ Employees should be involved only because their involvement boosts workplace morale.
2. Cruz is under high pressure to meet a production quota. He is well-trained in using machine guards but decides to remove his machine guard so he can work more quickly. His hand slips and is crushed in the machine. What is the root cause of this accident?  
**(Select all that apply).**
  - ☐ Unsafe acts or behaviors
  - ☐ Lack of training
  - ☐ Unsafe conditions
  - ☐ Uncontrollable events
3. A public swimming pool keeps highly corrosive and dangerous chemicals in a shed. What would be the **best** way to prevent an accident stemming from unauthorized access to the chemicals?
  - ☐ Use engineering controls such as posting a “keep out” sign warning the public not to enter the shed.
  - ☐ Eliminate the hazard by locking the shed and only allowing management access to the key.
  - ☐ Provide personal protective equipment in the shed next to the hazardous chemicals.
  - ☐ Train employees, advising them to make sure no one enters the shed.
4. A factory has purchased a new machine that will boost production by 20%. Management and supervisors are concerned with the risk of injury arising from the new protocols required to use the machine. What would be the best way of preventing an accident with the new machine?
  - ☐ Eliminate the hazard entirely by not using the new machine.
  - ☐ Provide mandatory safety training to all employees on how to use the machine.
  - ☐ Reduce the use of PPE so employees can work quickly with the new machine.
  - ☐ Post a sign advising employees that they are about to use a new machine.

## Section 2: Risk Control and Mitigation - Human Resources

5. XYZ Asphaltting has created a safety committee comprised of employees. This is an example of the \_\_\_\_\_ element of an effective safety and health program.
- ☐ Management Leadership
  - ☐ Accountability, Responsibility, and Authority
  - ☐ Employee Participation and Involvement
  - ☐ Hazard Assessment and Control
6. Which of the following is an example of appropriate interview techniques following an accident?
- ☐ A manager sits down with the employee and tells them their job depends on accurately answering interview questions.
  - ☐ The safety committee waits a week before conducting interviews so they can write clear interview protocols.
  - ☐ The manager asks all employees involved in an incident to send a two-sentence summary of the accident.
  - ☐ A manager lets the employee know that the purpose of the interview is to improve safety, not to assign blame.
7. Which of the following are examples of ergonomic risks? **(Select all that apply.)**
- ☐ Repetitive tasks
  - ☐ Excessive force
  - ☐ Neutral temperatures
  - ☐ Working with valuable products
8. Polly Factory Parts has one worker who uses a stamping machine on finished products. To stamp the product, the employee pulls down a lever. The employee does this all day. How could the factory reduce the risk of shoulder injury?
- ☐ Reduce the employee's waiting times in between pulls.
  - ☐ Automate the press and reassign the worker to another job.
  - ☐ Increase the force required to pull the lever to slow the worker down.
  - ☐ Require the worker to stand for the entirety of the shift.
9. Load weight, frequency, horizontal distance, and vertical distance are all factors in the NIOSH lifting equation. Which of the following statements regarding these factors is correct?
- ☐ Frequency is the only factor that impacts lift safety.
  - ☐ Increasing distance will make lifting safer.
  - ☐ Reducing any of the factors makes lifting safer.
  - ☐ Increasing frequency will make lifting safer.

## Section 2: Risk Control and Mitigation - Human Resources

10. \_\_\_\_\_ is/are a mechanical aid that can be used to control risks associated with manual lifting.
- ☐ Reducing frequency
  - ☐ Lift planning
  - ☐ Weight adjustment
  - ☐ Hand trucks
11. Which of the following substance abuse risk control methods would help avoid the risk of substance abuse in the workplace?
- ☐ Substance abuse education programs
  - ☐ Post-accident drug screening
  - ☐ Pre-employment drug screening
  - ☐ Hosting the employee happy hour off-site
12. What is a potential problem stemming from an employee substance abuse policy?
- ☐ Addiction is a mental condition, so employers can be sued for using a drug test to filter potential hires.
  - ☐ Employees may sue and argue that random drug screenings were not random and were discriminatory.
  - ☐ Employers may lose access to federal funding if they enact substance abuse programs that involve random drug screening.
  - ☐ Enacting substance abuse programs generally increases workers compensation premiums.
13. Which of the following would be an example of an administrative control to prevent employee violence?
- ☐ A pawn store installs bars on the outsides of their windows.
  - ☐ An employer conducts background checks on all employees.
  - ☐ An employer writes a zero-tolerance policy for workplace violence.
  - ☐ A retailer provides training on how to respond to violent customers.

## Set Yourself Up for Success!

### Visit the “Resources” Webpage at [RiskEducation.org/RCresources](https://RiskEducation.org/RCresources)

For valuable reinforcement, be sure to visit the “Resources” webpage. This webpage contains a variety of materials that will help you absorb the course material *and* set you up for success on the Final Exam. You’ll find:

#### Study Guide

Download a copy of the Study Guide. It contains all the Check-In questions, Knowledge Checks, and Self-Quizzes contained in this Learning Guide in a format that makes it easy for you to practice and check your answers.

#### Flash Cards

Play an interactive vocabulary game with a study set of digital flashcards to enhance your learning of the insurance and risk management terms used in this course.

#### Review Game

Use a fun, trivia-style review game to test your knowledge and prepare for the Final Exam.

#### Video Clips

View a video clip about an important concept related to one of the learning objectives in this section.



Employee Training

## In Addition...

#### Appendix

The Appendix of this Learning Guide contains a Glossary of terms as well as tips for study techniques and sample test questions that will help you prepare for the Final Exam.

## Section 3: Risk Control and Mitigation – Property and Liability

---

### Section Goal

In this section, you will learn about the various property and liability exposures organizations face and explore risk control methods to mitigate and address these concerns.

### Learning Objectives:

- 3.1 *List the common sources of employment practices liability exposures and the risk control measures used to address those exposures.*
- 3.2 *Apply risk control measures to the common types of fleet exposures and hazards.*
- 3.3 *Define key property exposure terms and describe the corresponding property hazard control programs.*
- 3.4 *Explain the common cyber exposures faced by businesses and the risk control methods that could mitigate those risks.*
- 3.5 *Describe the four types of contractual risk transfers and the three types of hold harmless agreements.*

All organizations must control risks related to many exposures. All organizations have property, and that property can be protected through proper risk control techniques. Furthermore, organizations should also be concerned with liability issues. One of the most significant liability threats is the employment practices exposure. Nearly everything the employer does or that happens in the workplace, whether the employer knows about it or not, can result in an allegation, a complaint, or litigation. The increasing use of technology also poses several risks that can result in either first-party or third-party claims against an organization.

# Employment Practices Liability Exposures

## Learning Objective:

- 3.1 List the common sources of employment practices liability exposures and the risk control measures used to address those exposures.

Employment practices liability arises from employee allegations of either unfair or inappropriate acts committed against them by someone who represents their employer and includes the legal costs incurred. Both current and former employees, as well as third parties, can pursue claims against the organization if they believe their rights have been violated. Ultimately, the rights of employees are set by a variety of different governmental agencies, and these agencies determine the proper employment practices. Major sources of employment practices guidelines include:

- the Equal Employment Opportunity Commission (EEOC)
- the Department of Labor (DOL)
- the vast number of Fair Employment Practice Agencies (FEPAs). These state and local agencies work with the EEOC to administer federal requirements.
- state and federal court decisions that form the basis of common law and become the official interpretation of statutes and regulations.



The function of risk management regarding employment practices exposures is to ensure that an organization has policies and procedures that prevent improper employment practices from occurring. The challenge to the risk manager is that many employment practices that emerge from this liability exposure emanate from two other functional areas within the organization: the human resources department and the legal department. If these three disciplines do not or cannot cooperate, the employment practices exposures will escalate, causing tremendous loss to the organization.



Another critical role of risk management is ensuring that the management of allegations of inappropriate employment practices occurs at the lowest managerial level possible. This could prevent the continuation of behaviors that could ultimately need to be escalated to higher managerial levels for resolution. Procedures should be created that allow employees to report their concerns to an organization, and these concerns should be promptly addressed. This is important because an organization's response to allegations at an administrative level may make or break a case when it goes to court.



## The Scope of Employment Practices Issues

The scope of employment practices issues encompasses several general areas:



**Violation of Statutes**



**Discrimination**



**Harassment**



**Retaliation**



**Invasion of Privacy**



**Wrongful Termination**

### Violation of Statutes (Statutory Liability)



Statutes are widely-ranging federal, state, and local laws that protect the rights of individuals. Agencies at every level of government are tasked with investigating, evaluating, and adjudicating complaints regarding employment practices and the protection of rights.

While the sources of statutory liability are complex, two key pieces of civil rights legislation should be a general concern for

all risk managers: the Civil Rights Act of 1964 and the Civil Rights Act of 1991.

The Civil Rights Act of 1964, Title VII, assured that all individuals could pursue and enjoy employment free from discrimination on the basis of race, color, religion, sex, or national origin. Discrimination based



## Section 3: Risk Control and Mitigation - Property and Liability

upon these factors is prohibited in hiring, promoting, firing, wage setting, testing, training, apprenticeship, and all other terms and conditions of employment.

Several decades later, the Civil Rights Act of 1991 strengthened employment discrimination protections and codified the theory of “disparate impact” (see definition below) in employment. Furthermore, the Civil Rights Act of 1991 granted employees greater rights when suing employers for discrimination, including jury trials for discrimination claims, compensatory and punitive damages, and statutory caps on those damages.



Another source of liability for employment practices is associated with employee disability and illness, led by the Americans with Disabilities Act of 1990 (ADA) and its amendments in the ADA Amendment Act of 2008. The Americans with Disabilities Act of 1990 requires employers to fully understand the definitions of “disabled individual,” “reasonable accommodation,” and “disparate impact.” Review the definitions of these terms.

### 1. “Disabled Individual”

A “disabled Individual” is any individual who has a physical or mental impairment that substantially limits one or more major life activities (e.g., “routine” activities such as walking, seeing, hearing, bathing, feeding oneself, or using the restroom), has a record of impairment, or is regarded as having such impairment.

### 2. “Reasonable Accommodation”

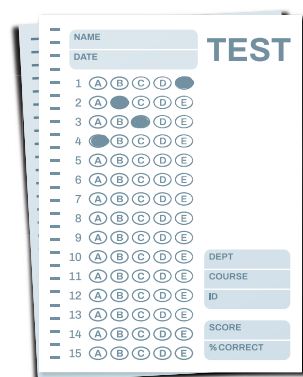
A “reasonable accommodation” is any modification or adjustment to employment, an employment practice, or the work environment such that a qualified individual with a disability has an equal opportunity to obtain and hold that employment.

### 3. “Disparate Impact”

This refers to a practice that appears to be a neutral employment practice but has an otherwise unjustified adverse impact on individuals within a protected class. Common examples of a disparate impact practice include written tests, height and weight requirements, educational requirements, and subjective practices, such as interviews.



In *Griggs v. Duke Power Co. (1971)*, black employees challenged a power company’s requirement that employees pass an intelligence test and obtain a high-school diploma to transfer out of its lowest-paying department. The court found that the two conditions imposed by the company created a disparate impact and were unrelated to job performance, noting that many white employees who were not high-school graduates had been performing well in the higher-paying departments.





**Note:** The ADA Amendments Act of 2008 broadened the definition of “disability,” the number and types of persons protected under the ADA, and other Federal disability nondiscrimination laws. It was designed to strike a balance between employer and employee interests.

Related to the ADA are the Family and Medical Leave Act of 1993 (FMLA), the Pregnancy Discrimination Act of 1978 (PDA), and the Occupational Safety and Health Act of 1970 (OSHA). OSHA (and its state versions) requires the risk manager to understand occupational safety and health issues. The third general group of statutes affecting employment practices deals with general business practices concerning employees:

- Age Discrimination in Employment Act of 1967 (ADEA)
- Worker Adjustment and Retraining Notification Act of 1988 (WARN)
- Employee Polygraph Protection Act of 1988 (EPPA)
- Equal Pay Act of 1963 (EPA)
- Older Worker Benefit Protection Act of 1990 (OWBPA)
- National Labor Relations Act of 1935 (NLRA)
- Uniform Services Employment and Reemployment Rights Act of 1994 (USERRA)
- Fair Labor Standards Act of 1938 (FLSA)
- Immigration Reform and Control Act of 1986 (IRCA)
- Attorney’s Fees Award Act of 1976
- Information Nondiscrimination Act of 2009

Compounding this long but not totally inclusive list is an array of state and local “mirror” laws that reflect the intent of federal legislation in state laws and local ordinances. Risk managers should be aware of these various statutes and how they may impact the employment practices of the organization they work for.

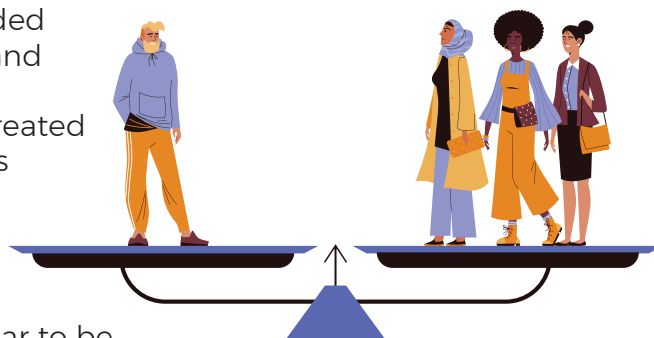


### Discrimination

The most common source of employment practices complaints is discrimination. Federal laws prohibit discrimination based on race, color, religion, sex, and national origin, as covered by the Civil Rights Act of 1964. Other legislation extends protection against discrimination based on pregnancy, ethnicity, ancestry, citizenship, disability, military service, genetic information, sexual orientation, marital status, and age. State and local laws may also include discrimination based on familial status, marital status, domestic partnership status, sexual orientation, blood traits, liability for military service, and AIDS and HIV status, among others.

## Section 3: Risk Control and Mitigation - Property and Liability

The types of prohibited discrimination are divided into two categories: discriminatory treatment and disparate impact. **Discriminatory treatment** addresses situations in which an individual is treated differently from other similarly situated persons because of that individual's protected status. Disparate impact, the focus of the Civil Rights Act of 1991, addresses the situation in which a protected group is impacted by an organization's policy or practice that may appear to be neutral but has the effect of adversely impacting the group.



Discriminatory practices can have substantial financial consequences for an organization, and policies should be established to prevent discrimination from occurring. Consider the real-world example of one such company:

### From *Business Insurance*, May 2023

A distribution company will pay \$709,971 to settle a U.S. Equal Employment Opportunity Commission sex discrimination lawsuit in which it was charged with refusing to hire female job applicants for order selector positions, the agency said Thursday.

The EEOC said company officials at Kenneth O. Lester Co. Inc., which does business as PFG Customized Distribution – Indiana, expressly stated sex-based criteria for the order-selector position in its Kendallville, Indiana, warehouse, including making statements to female applicants that the company prefers to hire men for that position.

The EEOC also said that the company discriminatorily assigned females to the small wares section of the warehouse, where they had less earning potential.

The company was charged with violating Title VII of the Civil Rights Act of 1964 in the lawsuit *EEOC v. Kenneth O. Lester Co., Inc. d/b/a/ PFG Customized Distribution – Indiana*, which was filed in U.S. District Court in Fort Wayne, Indiana.

The three-year consent decree settling the lawsuit provides \$650,000 in monetary relief to the class of female applicants who were not hired, \$39,971 to the female applicant who filed the underlying EEOC charge, and \$20,000 to a class of females who were subjected to work assignments based on their sex, the EEOC said.

The consent decree also enjoins PFG from failing to hire women in order selector positions because of their sex, among other provisions.

This case underscores the importance of risk management targeting employment practices liability exposures. Without measures to prevent and control discrimination in the workplace, companies can quickly find themselves paying out large settlements.

## Wrongful Termination

Another common source of employment practices issues arises from allegations of wrongful termination. **Wrongful termination**, discharge, or dismissal may be defined as;



When an employee's contract of employment is terminated by the employer, and the termination breaches one or more terms of the employment contract or an employment law.



Any termination process, even voluntary termination by the employee, can give rise to a wrongful discharge allegation. The risk manager faces an unusual challenge in managing this risk, as two other functional areas within the organization are likely to stake their claims to this exposure: human resources and legal.

Both functional areas have their own motivations. For example, the legal department may wish to focus on ensuring that termination follows the letter and spirit of the law, while human resources may be primarily focused on keeping employees happy. The risk manager, of course, focuses attention on minimizing the adverse financial and reputational impact of allegations of wrongful discharge and must recruit both areas as part of the risk management team.



When discussing wrongful termination, it is important to be aware of the relationship between wrongful termination and at-will employment. The term “at-will employment” became popular in the late 19th century and into the 20th century following a famous U.S. Supreme Court Case (*Lochner, 1905*) in which the court took the view that nothing should interfere with private contract rights or economic freedom, permitting an employer to fire an employee at any time.

Over the 20th century, many states created statutes that addressed at-will employment that protected employees. In particular, employees who are part of a trade union or employed for a public entity are not considered at-will employees and can only be terminated with just cause. However, at-will employment has become the general rule in private sector positions not governed by a labor union contract. In most employments, this means that the employee enters a contract with the employer that addresses how and when termination may occur.

One misconception about wrongful termination is that jurisdictions with “employment-at-will” legislation protect employers by permitting termination “at-will.” However, this is not true if the terminated employee can establish a motive for discharge that is unfairly discriminatory. Consider a scenario:

### Section 3: Risk Control and Mitigation - Property and Liability



An employer attempting to reduce its cost structure decides to terminate all employees who earn more than \$75,000 per year. If the only employees earning this salary level are over 60, the discharge appears to be based more on age than salary, but if employees of all ages are earning over \$75,000, the discharge would appear to be based more on salary than age.



When controlling risks associated with wrongful termination, having a written policy in place is critical. However, employment practices add a new facet: what the employer *does* outweighs what the employer *says*—or precedent trumps policy. Because of this interpretation by the courts, consistency in termination policies is a serious matter.

Added to this mix of common and contract law, the ADA creates a statutory protection granting rights to persons falling under its auspices. The ADA prohibits discrimination based on disability in hiring and all terms, conditions, and privileges of employment. The ADA defines disability as a physical or mental impairment that substantially limits one or more of the major life activities of an individual, a record of such impairment, or being regarded as having such an impairment. Physical or mental impairment is defined to include any physiological disorder or condition, cosmetic disfigurement, or anatomical loss affecting one or more of several body systems, as well as any mental, physical, or psychological disorder.

Under the ADA, an employer has a duty to make “reasonable accommodations” to the disabilities of the applicant or employee unless the employer demonstrates that doing so would create an “undue hardship” for the organization. The ADA Amendment Act of 2008 expanded the definition of disability and changed the threshold for claims of discrimination by persons regarded as having a disability by their employer.



Another important component of the ADA for employers to be aware of is provisions related to substance abuse. Under the ADA, substance abuse is considered an illness or disability, but an employee who is a current user is not protected and can be terminated or disciplined. An employee who voluntarily seeks assistance available in an Employee Assistance Program or a former substance abuser who is not a current user is protected.



Ultimately, wrongful termination can have a financial impact on organizations. Courts have awarded a variety of remedies when wrongful termination has been proven. These range from the reinstatement of the employee with the payment of back wages and any bonuses, commissions, and/or profit-sharing the employee would have earned to penalties for the employer—depending on the nature of the offense. Keep in mind that these statutes vary by jurisdiction, and there is no single determinative answer as to what constitutes wrongful termination and what are the appropriate remedies.

### Sexual Harassment

Sexual harassment is one of the most common sources of complaints in the workplace. Sexual harassment, as defined by the U.S. Equal Employment Opportunity Commission, is “unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature.” These behaviors are not new. However, society’s willingness to take the issue of sexual harassment in the workplace seriously has increased over time.

It is important to clarify misconceptions regarding sexual harassment. For example, some individuals may erroneously assume that such harassment can only occur between a male and female employee. However, The U.S. Equal Employment Opportunity Commission provides several circumstances in which sexual harassment can occur, including but not limited to:

- The victim, as well as the harasser, may be a woman or a man. The victim does not have to be of the opposite sex.
- The harasser can be the victim’s supervisor, an agent or client of the employer, a supervisor in another area, a coworker, or a non-employee.
- The victim does not have to be the person harassed but could be anyone affected by the offensive conduct.
- Unlawful sexual harassment may occur without economic injury to or discharge of the victim.

Regardless of the nature of the sexual harassment, there are several common characteristics. Overt harassment consists of visible behaviors that frequently involve unwanted physical contact. This may include “quid pro quo” (a Latin term meaning “this for that”), the promise or hint of something, such as a promotion or appointment, in exchange for sexual favors.



Sexual harassment can also be more subtle and consist of a pattern of inappropriate conduct that creates a hostile or uncomfortable working environment. This behavior generally does not result in physical contact but rather consists of an atmosphere, such as being subjected to inappropriate stories or language, gestures, whistles, or other suggestive signals.



A **hostile or offensive work environment** exists when unwelcome sexual conduct, overt or subtle, has the effect of unreasonably interfering with an individual’s work or performance or creates an intimidating, hostile, or offensive working environment. The behavior that constitutes “unwelcome sexual conduct” is problematic.



## Section 3: Risk Control and Mitigation - Property and Liability

Ultimately, there are two tests courts and administrative bodies use to determine if a behavior is considered unwelcome sexual conduct:

1. Was the person affected by the conduct actually offended? This test is subjective.
2. Would a reasonable person under the same circumstances have been offended? This test is considered to be objective.

The difficulty the risk manager and human resources manager have in managing the sexual harassment issue is that the behavior that constitutes sexual harassment is viewed from the victim's perspective without regard to the intent of the alleged harasser. What is offensive to one person may not be offensive to another.

This is indeed a very personal response and highly dependent upon circumstances that are always in a state of flux. Value judgments, such as "offensive," can also change over time.

Furthermore, some inappropriate remarks and behaviors are simply a matter of poor taste rather than misconduct. The distinction often cannot be defined but is known when observed. Management must understand the concepts of acceptable and unacceptable behaviors and determine what is considered normal conduct for the work environment. One should be aware that a single event (e.g., joke, remark, cartoon, photo, etc.) may be sexually offensive to one person in a group but not to others. This situation is not considered to create hostile workplace sexual harassment, even though one person is genuinely offended. In effect, the courts tend to side with the group's view and not one individual's.



Additionally, an organization may be held vicariously liable for conduct within the organization of which it is entirely unaware. This includes one of the most difficult challenges facing the risk manager: the actions of a third person. For example, a delivery or salesperson for a vendor might engage in unwelcome sexual conduct toward an employee. If the employer fails to monitor such conduct or, worse, fails to act when notice of such behavior is received, the vicarious liability may shift to straight liability.

### Retaliation



Another source of employment practices allegations is retaliation. The offending behavior is exactly what it sounds like: the organization's management or other employees retaliate against an employee who files a complaint, grievance, or lawsuit alleging injury from an employment practice. The *National Law Review* reports that retaliation continues to be



### Section 3: Risk Control and Mitigation - Property and Liability

the most frequently filed claim included in charges with the EEOC and that 56 percent of all charges filed in FY 2021 included a retaliation claim<sup>4</sup>.

Retaliation is considered an intentional act. Examples include transferring the employee to a less desirable position, verbal or physical abuse of the employee, subjecting the employee and their work to increased scrutiny, or giving the employee a less favorable (unearned) performance evaluation. The EEOC provides the following guidance:

EEO laws prohibit punishing job applicants or employees for asserting their rights to be free from employment discrimination, including harassment. Asserting these EEO rights is called “protected activity,” and it can take many forms. For example, it is unlawful to retaliate against applicants or employees for:

- filing or being a witness in an EEO charge, complaint, investigation, or lawsuit.
- communicating with a supervisor or manager about employment discrimination, including harassment.
- answering questions during an employer’s investigation of alleged harassment
- refusing to follow orders that would result in discrimination.
- resisting sexual advances or intervening to protect others.
- requesting accommodation for a disability or religious practice.
- asking managers or coworkers about salary information to uncover potentially discriminatory wages.

Participating in a complaint process is protected from retaliation under all circumstances. Other acts to oppose discrimination are protected as long as the employee was acting on a reasonable belief that something in the workplace may violate EEO laws, even if they did not use legal terminology to describe it.

Engaging in EEO activity, however, does not shield an employee from all discipline or discharge. Employers are free to discipline or terminate workers if motivated by non-retaliatory and non-discriminatory reasons that would otherwise result in such consequences. However, an employer is not allowed to do anything in response to EEO activity that would discourage someone from resisting or complaining about future discrimination.

---

<sup>4</sup> National Law Review. (2022, January 21). EEOC Roundup: Top 5 Takeaways for Employers – 2021 Enforcement and Litigation Statistics. *The National Law Review*. Retrieved from <https://www.natlawreview.com/article/eeoc-roundup-top-5-takeaways-employers-2021-enforcement-and-litigation-statistics>

### Invasion of Privacy

Invasion of privacy is the intrusion upon the privacy and personal information of another by a person or entity without permission or just cause. In certain circumstances, data collection, workplace monitoring, and other methods of obtaining private information have been found to be invasions of privacy. The U.S. Supreme Court has established some limited protections regarding prohibited employer inquiries. These primarily include marriage, education, raising children, and family relationships, in general.



Under most states' privacy laws, the test for invasion of privacy is whether the person who was violated had a reasonable expectation of privacy. There must be a serious and unreasonable compromise of the other's interests to find a privacy violation.

In the workplace, there are few, if any, privacy rights. Courts may be guided by the employer's written policies and procedures regarding searches of desks or lockers or privacy of phone calls made on company phones. Tracking of keystrokes and internet usage is common. Most employers have employees sign an acknowledgment that they understand there is no expectation of privacy in the workplace. Some other examples of actions that would constitute a privacy violation include:

- Placing cameras in restrooms and locker rooms
- Sharing confidential health information with parties who do not need to know
- Disclosing garnishments of wages

### Risk Control Measures to Address Employment Practices

Employment practices claims are expensive to defend and pay. Conversely, prevention techniques are generally inexpensive compared to the cost of litigation and, when diligently applied, can be highly effective in preventing and mitigating claims.

The general risk control measures for employment practices are:

#### 1. **Adopt sound policies and procedures.**

With input from human resources and legal, the risk manager must ensure that management has established sound policies and procedures.

#### 2. **Ensure policies and procedures are communicated and applied.**

Equally important, the risk manager must ensure that the policies and procedures are communicated to all personnel throughout the organization, are clearly understood, and are universally applied at all levels within the organization. Having a policy and not adhering to it is far worse than not having a policy at all.

### 3. Frequently review policies and procedures.

The policies and procedures must be regularly reviewed for content, legal conformity, and intent. As the organization changes, policies and procedures must adapt to the “new” organization and its personnel.



### 4. Ensure managerial support for policies and procedures.



Management must continuously express its support of established policies and procedures through written statements, in meetings, and by its own conduct. Organizations place themselves in peril when upper management adheres to their own set of rules while expecting all other personnel to follow the organization’s established policies and procedures. Senior management must approve and support policies and procedures that identify individual situations and patterns of behavior that

are acceptable and unacceptable and should be role models themselves. To borrow a military term, senior management defines the “conduct unbecoming” of all employees.

### 5. Take steps to verify that policies and procedures are being followed.

The risk manager must assist the organization in taking reasonable care to ensure that the established policies and procedures are being followed. Common methods of verifying adherence include:

- Employee questionnaires, including “blind” surveys that do not identify specific individuals
- Supporting an open-door policy by executives to discuss employment practices concerns
- Managing by walking around—management must “walk the talk”
- Retaining objective and confidential written records on all personnel, with a periodic review of those records

### 6. Create resources to respond quickly to allegations and grievances.

The risk manager must ensure that the organization has assigned resources to conduct a prompt, complete, and documented response to all allegations or grievances. The risk manager is not the judge, jury, or defense counsel on these matters. Instead, the risk manager is more like the court reporter, ensuring the facts are documented in an unbiased manner and retained.



### 7. Verify that disciplinary action is conducted fairly.

The risk manager must ensure that the appropriate functional area that conducts any disciplinary action does so in a manner appropriate to the individual situation and a manner consistent with actions taken on any previous situation involving substantially the same set of facts.

### 8. Document consistently.

Finally, the risk manager must be sure the organization is consistent in its employment practices and maintains documentation appropriately.

#### A Note on Hiring Practices



The organization must establish a written hiring and recruiting process that is clearly defined and consistent in practice. Care must be taken in designing and using employment documents—job postings, position descriptions, applications, the interview process, background checks, job offers, and the employee handbook. Consulting with counsel or a human resources consultant is advised.

During the hiring process, hiring managers or supervisors should avoid discussing discriminatory subjects in interviews and discussions with employees or candidates, such as age, marital status, ethnicity, religion, nationality, disabilities, etc. Proper training of managers and supervisors in this area is essential to avoiding claims of discriminatory hiring practices and to the success of the hiring process.

#### A Note on Employment Practices Liability Policies

An EPLI policy is available from the Insurance Services Office (ISO), but most EPLI policies are written on non-standard, non-ISO forms. Policy language and conditions vary by policy; however, they typically are written on a claims-made basis and include coverage for judgments/settlements, pre- and post-judgment interest, and other items. Coverage for punitive damages may be included as determined by state statute.

While key elements of the Insuring Agreement of EPLI policies may differ, most are written to provide coverage for claims filed by employees (or job applicants) against the organization because of an employment-related incident. Separate coverage may be available for claims filed by third parties, such as individuals with whom the business or business' employees have contact, such as vendors, independent contractors, volunteers, or other non-employees.





# Knowledge Check



Complete the chart below. In the left column, list the six types of employment practices exposures. In the right column, explain potential risk control methods that could be used to address those exposures.

1.		
2.		
3.		
4.		
5.		
6.		

# Fleet Hazards and Controls

## Learning Objective:

*3.2 Apply risk control measures to the common types of fleet exposures and hazards.*

Vehicle fleet safety is an exposure that requires specific hazard control techniques. Fleet exposures can be present in all four logical classifications of risk—property (physical damage to vehicles), liability (injury to third parties), human resources (employee injuries), and net income (loss of revenue). The risk manager should identify these exposures and apply risk control methods to protect against any potential losses to the organization's bottom line.



## Exposures

The first step to identifying fleet exposures is to determine the type of fleet being used. Each type of vehicle has unique exposures. Long-distance cargo transportation uses large vehicles, and while the trips are longer, they tend to be primarily on highways with flows of traffic that are parallel, not perpendicular, to the vehicle's route. Service and delivery fleets, on the other hand, are smaller vehicles used for intermediate and scheduled routes. They tend to operate in more urban areas with concentrations of other vehicles traveling parallel and perpendicular. These areas can be more densely populated and have pedestrians, bicyclists, parked vehicles, and other obstructions. Private passenger vehicles are not used to transport goods or services but may be used by sales forces or to transport passengers (e.g., taxi cabs). They tend to be used in more urban areas and are operated generally by non-professional drivers—those who do not have any special training in driving beyond simply having a driver's license. Buses may operate in a small or large radius and have the high-exposure cargo of many of passengers. Finally, non-owned vehicles of any type used at any time on a rental basis must be addressed in a fleet safety program.

## Common Types of Fleets



Long-distance cargo transportation (owned goods of others) – large vehicles with longer trips; trucks, tractor-trailers, trailers



Service and delivery – smaller vehicles used for intermediate and scheduled routes; pickup trucks, vans



Private passenger – not used to transport goods or services (used by sales personnel, taxis)

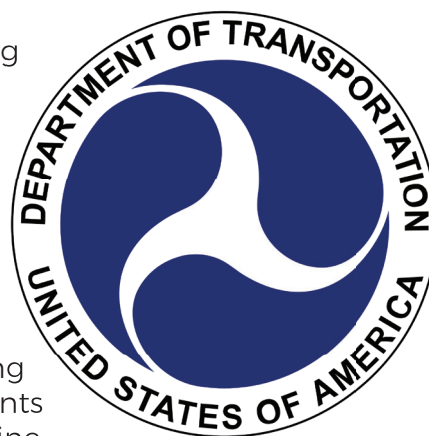


Buses, vans, shuttles – transport high numbers of passengers; livery vehicles



Non-owned vehicles of any type – rented or owned by others

It is also beneficial for risk managers to be aware of relevant transportation regulations and guidelines. In addition to having authority over other types of transportation, including air, rail, and pipeline, the Department of Transportation (DOT) also issues Federal Motor Carrier Safety Regulations and provides education and assistance for large commercial vehicles and buses, including special regulations for those that transport hazardous goods or are used for port security. DOT also has rules and regulations covering drivers pertaining to license requirements, hours of service, and drug and alcohol use. The vehicle requirements include roadside inspections and keeping maintenance records. Failure to comply with these requirements can come at a considerable cost, as DOT has the authority to fine companies that do not follow the rules and regulations and remove from service any vehicle that is not in compliance.



## Fleet Hazards

As mentioned previously, fleet exposures include property damage to the fleet vehicles and the cargo as well as liability for injury, harm, or property damage to third parties. Large vehicles can cause severe accidents, damaging the cargo and the vehicle itself and the driver and/or passengers, and cause third-party injury and/or property damage, as well.

Smaller vehicles have more frequent accidents. While private passenger vehicles can have expensive accidents, the accidents tend to be smaller when compared to large commercial vehicles. Liability can arise from negligent operation of an owned vehicle, resulting in third-party injury or property damage from negligent entrustment of a vehicle or from hired or borrowed vehicles.

Any or all types of accidents can occur with any of these vehicles. Rear-end collisions, accidents at intersections, accidents while backing up, and hitting stationary objects are collisions in which someone is at fault, creating liability for owner and driver alike. In addition, natural perils may also cause property damage even when the vehicle is parked and the driver is not present. Furthermore, driving during hazardous conditions such as weather-related flooding, snow, or ice, or when roads are under construction increases the likelihood of accidents. Review the following table for additional examples of fleet hazards.





### Section 3: Risk Control and Mitigation - Property and Liability

Risk Category	Risk Exposure	Hazard	Result
Property	Unsafe Road Conditions	A garbage truck overturns when it hydroplanes due to wet and slick roads.  (Business Auto Physical Damage)	Physical Damage to the Owned Vehicle
	Cargo	Meat cargo spoils due to malfunction of the refrigeration cooling system of the truck carrying property for a meat company.  (Business Auto Cargo)	Physical Damage or Destruction of Cargo Belonging to a Client
Liability	Impaired Driving	Due to long hours behind the wheel, the driver falls asleep, veers off the road, and causes a collision with another vehicle that results in passenger injuries.  (Business Auto Liability)	Injury or Harm to Third Parties
	Poor Vehicle Maintenance	Brake failure results in a rear-end collision with another vehicle, resulting in damage to that vehicle.  (Business Auto Property Damage)	Property Damage to the Property of Others

Risk Category	Risk Exposure	Hazard	Result
Human Resources	Routes and Traffic	During rush hour, the employee driver swerves off the road to avoid a rear-end collision but collides with a concrete embankment, resulting in head injuries to the employee driver.  (Workers Compensation)	Injury to an Employee Driver
	Drivers	An untrained employee driver causes an accident that injures a passenger in his vehicle who is a fellow employee.  (Workers Compensation)	Injury to a Fellow Employee
Net Income	Loss Use	A rental car company shuts down operations due to hurricane damage to its entire fleet.	Physical Damage and Loss of Rental Income
	Vehicle Value	A manufacturer recalls high-value vehicles with specialized equipment installed.	Increased Cost to Secure Replacement Vehicles

Check-In



**Directions:** Answer the following question.

John, the risk manager for a trucking company, is concerned with fleet risks and exposures. For each of the logical classifications of risk, provide an example of an exposure John should be concerned about.

### Administrative Controls

There are several hazard and administrative controls that can be used to prevent or reduce fleet accidents. Because the physical condition of the fleet (e.g., tires, engine performance, brakes, etc.) can be as much a factor in accident prevention as the safe operation of the vehicles, hazard control mingles with administrative control in controlling the risks.

### Fleet Safety Policy

The first line of defense is the fleet safety policy. This policy should include a management policy statement and details pertaining to driver responsibility and accountability (which include the authority to drive and rules and regulations), drug and alcohol use, cell phone use, and vehicle responsibility. Along with the driver responsibility, the vehicle inspection and maintenance program are a part of vehicle responsibility. Pre-trip and post-trip inspections should be made, along with scheduled preventive maintenance. All corrective action should be documented in case of vehicle malfunction or failure.



### Driver Qualifications



The second line of defense is making sure the driver is qualified and has been properly trained. Each driver should have a valid driver's license for the class of vehicles driven. Before a driver can be accepted as qualified, there must be some criteria to measure who is qualified to drive. The criteria for an acceptable driving record should be in written form and a part of the policies and procedures. The employment application should have information regarding the driver's qualifications and experience and should be in accordance with the written criteria for an acceptable driving record. Drivers who are transferred from another division should also have a record showing their qualifications and experience, even if it is not in employment application format. Driver disciplinary procedures also should be incorporated into the policy and procedures.

The U.S. Department of Transportation's Federal Motor Carrier Safety Administration sets forth general qualifications for drivers in their regulations. In Subpart B §391.11 General Qualifications of Drivers, it states, in part, that a driver must:

- Be at least 21 years old
- Be able to read and speak English sufficiently to converse with the general public and understand highway traffic signs
- Be capable of safely operating the type of commercial motor vehicles they drive and be physically qualified to drive a commercial motor vehicle
- Have a currently valid commercial motor vehicle operator's license issued by only one state or jurisdiction
- Have prepared and furnished the motor carrier that employs them a list of their violations (motor vehicle record or MVR)

## Section 3: Risk Control and Mitigation – Property and Liability

- Have no disqualification to drive a commercial motor vehicle according to the rules outlined in §391.15
- Have successfully completed a driver's road test or hold an operator's license or a certificate of road test that the motor carrier that employs them has accepted as equivalent to a road test

Beyond careful selection, training of drivers should include written procedures concerning orientation to the vehicle, instruction in defensive driving, and specific areas of awareness or exposure (e.g., backing up). It should also include instructions on responding to accidents, such as rules for reporting, as well as investigation forms and procedures.

An Accident Review Committee should play a more active role than simply determining if a driver is “at fault,” thoroughly investigating accidents and determining what can be done to prevent similar accidents in the future.



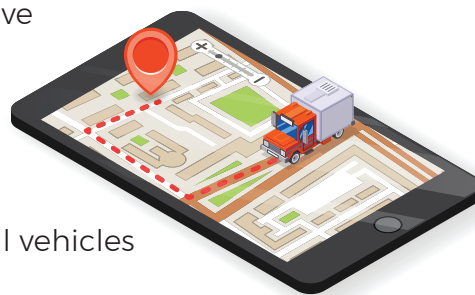
### Monitoring and Surveillance

A variety of monitoring and surveillance methods support driver safety and reduce accidents. These include:

#### 1. Telematics

These systems use a mobile device to send and receive data from vehicles to a server. The data is usually provided by the vehicle's onboard diagnostics, including dash cameras and sensors. Benefits include:

- **Tracking ability** – GPS technology allows the risk manager/fleet manager to know the location of all vehicles at any given time.
- **Improved safety** – Fleet managers can evaluate drivers' performance based on data regarding driving speed, hard braking, use of directional signals, seatbelts, etc. By reinforcing desired performance and focusing on safety standards, driver performance can be improved.
- **Maintenance improvements** – The use of telematics improves vehicle maintenance programs. Hours and miles driven are tracked, and preventive maintenance is scheduled accordingly.



### 2. Public Reporting



“How’s my driving?” signs and bumper stickers allow the public to report vehicles being operated in an unsafe manner. Common complaints include improper lane changing, speeding, and running red lights. Studies have found that vehicles displaying the decal are involved in 22% fewer accidents, resulting in a 52% reduction in accident-related costs<sup>5</sup>. This may be due to increased driver awareness of the sign and a desire to avoid complaints.

The last element of a fleet accident hazard control program involves the vehicles themselves. There should be a procedure that includes pre-trip and post-trip inspections to identify potentially hazardous conditions of the vehicle. One need only watch a commercial aircraft pilot do a “walk around” of the aircraft before it departs the gate to understand how important pre-trip inspections are. In addition, vehicles should be scheduled for preventive maintenance. All corrective action must be documented.

---

<sup>5</sup> Hickman, Jeffrey S., et al. *Impact of Behavior-Based Safety Techniques on Commercial Motor Vehicle Drivers*. Washington, D.C.: Transportation Research Board, 2007. Accessed July 20, 2023.

▶▶ Knowledge Check



**Directions:** Read the scenario and provide some fleet controls for each category of risk control.

Siblings Produce transports fresh produce to restaurants daily. They have a delivery fleet of medium-sized trucks that make multiple scheduled stops in a city. Create some sample risk control methods that the company could use.

Sample Fleet Risk Controls	
Avoidance	
Prevention	
Reduction	
Segregation Separation Duplication	
Transfer	

# Property Exposures and Hazard Control Programs

## Learning Objective:

3.3 Define key property exposure terms and describe the corresponding property hazard control programs.

An important category of the property assets of most businesses includes the buildings occupied as offices, manufacturing, storage, sales, residential, etc. The continued availability of building space for conducting operations is critical to the survival of most businesses and, for this reason, the risk manager must develop the knowledge and skills to protect these assets.

Property exposures fall under four general classifications: Construction, Occupancy, Protection and Exposure, commonly referred to as **COPE**.



### Construction

Various types of materials can be used to construct buildings, such as frame (wood construction), joisted masonry (masonry with wood joists), non-combustible masonry (masonry with steel or concrete floors and roofs), non-combustible metal (entirely metal structure), and fire resistive or modified fire resistive construction (metal beams and concrete with protective coatings such as gunite, a mix of sand and concrete).



### Occupancy

Occupancy describes who and what type of operation is occurring in the building. For example, the occupancy of a McDonald's restaurant is "restaurant" while the occupancy of McDonald's corporate headquarters is "office."



### Protection

This refers to the local, on-site protective safeguards, such as automatic sprinkler systems, fire and smoke alarms, fire doors, fire walls/curtains, special hazard protections like gaseous suppression in computer rooms and automatic shutoffs for flammable liquids and ventilation systems. It also includes putting into place fire brigades and housekeeping measures to minimize the impact of perils and hazards, as well as external protection such as a fire department.



### Exposure

This looks at sources of potential damage external to the building. For example, a building located next to another building used to store flammable liquids or a building located in a flood-prone area both have external exposures.

## Exposures to Loss

### Perils



Perils are the direct cause of a loss, and can be human, economic, or natural in origin. Human perils are like electrical fire caused by negligence or poor maintenance, theft, and vandalism. Economic perils could include property damage to a supplier or customer that causes an economic loss to an organization. Lastly, natural perils include events such as wind, hail, lightning, flooding and so on.

### Property Hazards

Hazards that contribute to the loss of property exposures are human, economic, and natural in origin. While a hazard is a factor that increases the chance of a loss, a peril is the cause of the loss. These terms often blur together, but it is important to distinguish between the two. Consider an example:



Paul owns a small warehouse he uses to store propane and various other flammable gases. One day, a fire breaks out from a lightning strike. The warehouse is completely destroyed in the ensuing fire.



In the example, the peril is the fire. The fire was worsened by the hazard, which in this case was the storage of flammable gases within the warehouse itself. Other common hazards affecting exposure to loss include:

- Geographic location, e.g., having a building where a windstorm or earthquake might be more prevalent
- Maintenance, particularly of plumbing, electrical, heating/ventilation/air conditioning (HVAC) and the roof
- Storage practices (especially when flammable materials are involved)
- Any special hazards, such as cutting, welding, or cooking activities

## Measures of Loss Potential

Outside of potential perils and hazards, risk managers should also be able to identify the potential impact of a property loss. To do so, the risk manager must be concerned about two measurements of loss potential when considering COPE: maximum possible loss and probable maximum loss.

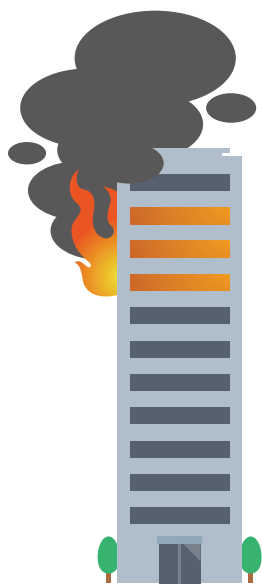
### Maximum Possible Loss (MPL)

First and most important, the risk manager must be concerned about the maximum possible loss or amount subject to loss. This is the measure of the greatest loss potential arising from the property, regardless of protective measures. The risk manager must assume the absolute worst combination of events, (e.g., a fire is accompanied by high winds, a





sprinkler system fails, automatic doors fail to close, and a host of other possible systems fail). What this entails is looking at the entire amount subject to destruction from the same chain of concurrent events.



The only factor that would limit the MPL in this scenario is adequate separation between structures or locations. For example, if an organization has all its operations conducted at one location across multiple buildings, the entire location (and all the buildings) would be subject to one loss. On the other hand, if the organization divides its operations into three separate locations (one in Texas, one in California, and one in North Dakota, for example), the original MPL would be broken into three lesser MPLs—one for each location.

Further, a single location may have several MPL values depending on the nature of the peril. Consider an organization with three buildings in the same location. All three buildings would be subject to the peril of a tornado, hurricane, or earthquake. However, if the separation between the buildings is great enough and there is no source of fuel (such as tall grass between the buildings), the MPL from a fire may be less than that of an earthquake. Similarly, if one building were constructed primarily underground, the MPL stemming from a tornado would be diminished.

### Probable Maximum Loss (PML)

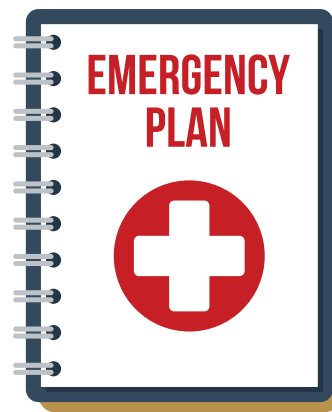
The probable maximum loss (PML) is the amount of loss expected, given some level of impairment or delay in fire protection (the definition varies by insurance carrier and by risk manager). Fire protective devices that serve to reduce the PML include automatically closing fire doors, parapets, protected openings such as windows, sprinkler systems, the protection class of the building, the water supply, the capabilities of the local fire department, and so on.

## Risk Control for Property Exposures

### Administrative Controls

To control property exposures and hazards, management programs can be implemented. Management programs consist of inspection programs. These programs include taking steps such as:

- Walking through the facility to identify hazards and exposures
- Implementing good housekeeping practices to ensure there is no debris on walking surfaces or items left in a location that could present a tripping hazard
- Ensuring that all equipment or machinery is in good condition
- Proper facility maintenance and repair
- Establishing policies and procedures for especially hazardous activities, such as welding or cooking



### Hazard Controls for Property Exposures

One hazard control would include fire protection services. The amount of protection would depend on whether the source is an internal fire brigade or an external municipal fire department. The amount of loss would be further affected by the protection class of the building.



The protection class is a classification that insurance underwriters use to measure the proximity of fire department availability, the distance of the water supply, and the capabilities of the external fire department, such as its status as a volunteer or full-time department, its training, and its equipment. Even the best fire protection services are of little use if there is no fire alarm system, usually in the form of smoke detection or heat detection, but sometimes a 24-hour watchman system will be used.

Another hazard control measure comes in the form of fire mitigation systems, such as sprinklers. The purpose of a sprinkler system is to contain the fire in a small area to reduce the severity of the loss, not to prevent a fire from starting. The effectiveness of a sprinkler system is determined by design density (whether it is specific to occupancy), water supply (pressure and flow rate), maintenance procedures, and system impairment testing procedures to identify any condition that would impact the ability of fire protection equipment to detect, control, or suppress a fire.

Finally, building security protection can be employed to protect property from exposures such as vandalism and theft. Security protection consists of physical barriers (safes, locks, bars, etc.), lighting, and either local or central alarm systems.

Although this Learning Guide section has primarily focused on administrative controls and hazard controls, most of the reduction methods will come into play when responding to property exposures. Eliminating the hazard, substitution of a less hazardous substance or process, engineering controls, administrative controls, use of personal protective equipment, and training can all be employed to protect organizations from loss to property.

## ▶▶ Knowledge Check



ABC Widget Factory opens a new manufacturing plant in a previously wooded area in the Sacramento foothills of California. Part of their manufacturing process relies on vinyl chloride, an odorless, flammable gas.

1. Explain two factors affecting their property exposures to loss.

a. \_\_\_\_\_

\_\_\_\_\_

b. \_\_\_\_\_

\_\_\_\_\_

2. The “C” in COPE stands for \_\_\_\_\_.

Give two examples related to this letter of the acronym that would reduce ABC Widget Factory’s exposure to loss.

a. \_\_\_\_\_

b. \_\_\_\_\_

Give one example that would increase their exposure to loss.

a. \_\_\_\_\_

3. The “P” in COPE stands for \_\_\_\_\_.

Give three examples related to this letter of the acronym that ABC Widget Factory could employ.

a. \_\_\_\_\_

b. \_\_\_\_\_

c. \_\_\_\_\_

## E-Business and Cyber Activity

It is difficult to imagine a business in today's world that does not use technology in some form or fashion. From simple email conversations to complex e-commerce transactions, computers have made personal and business lives more efficient. Retail and wholesale operations make and fulfill orders so that products can be distributed and sold to the public. Banks and other financial institutions allow transactions to be made via websites and mobile applications. From filling prescriptions to transferring complex medical scans, technology is deeply embedded in our lives. Professionals such as attorneys, engineers, and insurance agents all use technology in various ways every day.



As individuals and businesses use technology, they produce data. Data is an intangible business asset that can be found on computer systems and/or software, including but not limited to hard drives, flash drives, disks, tapes, laptops, tablets, readers, smartphones, smart watches, the Internet of Things (IoT) and third-party locations such as the Cloud. This data can include confidential information, payment information, and so on. This information is attractive to cyber criminals because it can be bought and sold online or used for other crimes like identity theft.

While cyber criminals certainly don't shy away from trying to hack large businesses, the government, or even cloud providers, the most common accessible targets are small to mid-sized businesses. This is primarily because smaller businesses may have less security measures in place. Nonetheless, these smaller businesses are often connected to larger businesses and can grant cyber criminals an easy way to get in through a "backdoor" connection. Keep in mind that no matter what the profession, any business that uses technology has an exposure to loss from a cyber standpoint. Whether it's business-to-business, business-to-consumer, or business-to-government, using technology has become an important way of life that carries substantial risk for loss. Consider an example of a business that may not ordinarily be viewed as a likely victim of cyber criminals.



A large regional grocery chain was using a digital system to control its refrigeration equipment. When a thermostat encountered an issue, it would contact the on-site server to look for solutions. If the on-site server could not fix the problem, it would contact the refrigeration company's system via a dedicated internet connection. If the refrigeration company's server could not resolve the issue, their system would automatically log a service call for the next day.

### Section 3: Risk Control and Mitigation - Property and Liability

Overnight, a hacker was able to get into the refrigeration contractor's system. The hacker discovered the connection to the grocery store and was able to gain entry. Once in the grocery store system, the hacker was able to get to the store's point of sale (POS) devices. The POS system was then compromised, and data (including customer payment information) was stolen.



This example illustrates that any business can have a significant cyber exposure, and data breaches and ransomware attacks can entail significant costs for organizations. The IBM Ponemon Institute does an annual assessment of the costs of a cyber breach.

The average annual costs of ransomware attacks between 2019 and 2022 are depicted below, with the 2022 figure reaching \$4,540,000<sup>6</sup>.

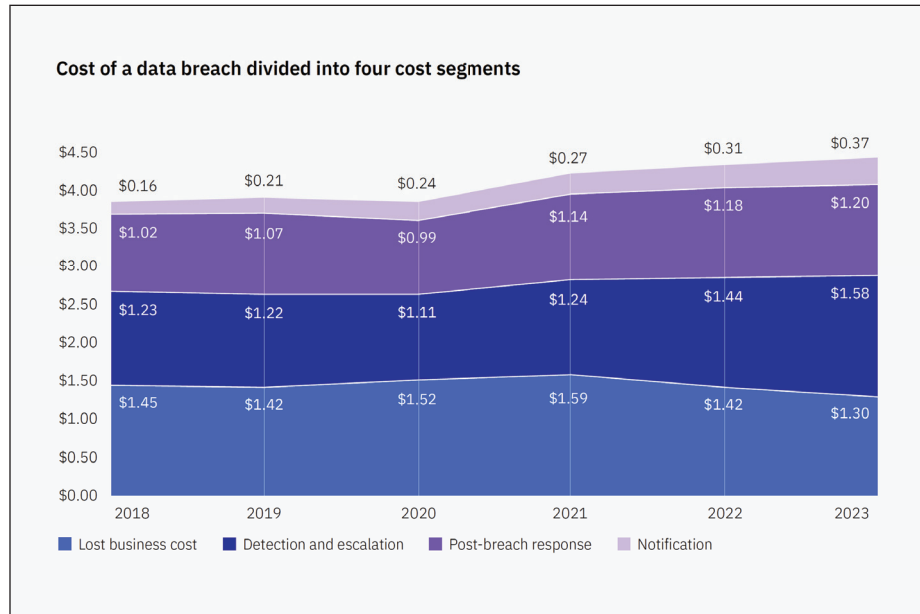
<b>2019</b>	\$3,920,000
<b>2020</b>	\$3,860,000
<b>2021</b>	\$4,240,000
<b>2022</b>	\$4,540,000

In addition, the study found that remote workforces have increased organizational vulnerabilities and thereby increased the cost of a cyber breach by one million dollars on average.

<sup>6</sup> IBM. "Data Breach Report." IBM Reports. 2022. <https://www.ibm.com/reports/data-breach> (Accessed July 20, 2023).

### Section 3: Risk Control and Mitigation - Property and Liability

Data breaches can also result in significant costs. The industries most heavily affected by data breaches include health care, financial, pharmaceuticals, technology, and energy industries.



The financial industry saw an increase in the cost of data breaches from \$5.72 million in 2021 to \$5.97 million in 2022, an increase of about .4%. The industrial industry, comprised of chemical, engineering, and manufacturing organizations, saw an increase from \$4.24 million to \$4.47 million in 2022, an increase of about 5.4%. The average total cost decreased slightly in four industries—pharmaceuticals, transportation, media, and hospitality. This data indicates that cyber risk exposures continue to be a concern, and risk managers should take steps to identify these exposures and implement risk control methods to prevent losses stemming from cybercrime.

# Cyber Risk Exposures

## Learning Objective:

3.4 Explain the common cyber exposures faced by businesses and the risk control methods that could mitigate those risks.

With the number of cyber incidents in recent years, businesses are better understanding the common cyber exposures that can cause problems. Cyber criminals target personal and business information available through social media sites and internet-connected devices like laptops, smartphones, tablets, and desktops. Even voice assistants, smart refrigerators, and other smart devices can be targeted by cyber criminals looking for ways to obtain information or perpetrate cyber extortion and ransomware attacks. Some common cyber exposures include the following:

### Collection of Private Information

Most businesses collect private information on their employees for HR reasons. Businesses such as insurance agencies and companies, accountants, physicians, and many others collect private information about their clients and customers.



### Data Storage

Data is stored in a number of places, including hard drives, backup drives, laptops, flash drives, tablets, and personal devices.

### Websites and Social Media

Most businesses have at least a basic website where customers can learn more about the business and what it does. Many businesses also have websites that are built for selling products. Another way of interacting with the public is through social media pages.

### Credit Card Transactions

Businesses with e-commerce generally accept credit card payments. Credit card data is also stored by brick-and-mortar businesses. Credit card data is collected and stored using point-of-sale devices, and this data can be lost during a cyber attack.

### The Internet of Things (IoT)



In today's "connected" world, the Internet of Things plays a very important role. Smart devices such as thermostats on refrigeration units, heavy garage doors, drones, GPS tracking devices, and other communication devices all contain embedded chips that can potentially be accessed by cyber criminals and used to grant access to other parts of an organization's network, such as in the grocery store example discussed previously.

### Regulation

The internet allows access to the insured from anywhere in the world, meaning the insured can be subject to state, federal, and even foreign regulations. Laws governing the protection of privacy and private information can vary greatly across the world, and failure to follow these laws can result in severe financial penalties. For example, in 2023, Meta (the parent company of Facebook) was fined over \$1.3 billion USD for breaching European Union rules regarding data privacy, even though it was not fined for similar behavior within the United States.



### First-Party Cyber Risks

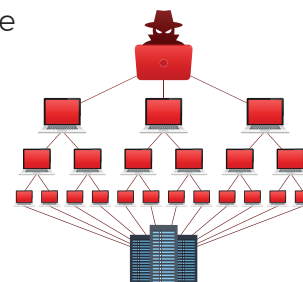
First-party losses are losses that have a direct effect on the insured's operations or property. This typically includes both direct and indirect loss or expense. First party loss exposures include:

- **Forensic Analysis** – When a cyber event has taken place, a computer forensic expert must examine the system and the data to determine when the event took place, what data was accessed, how data was manipulated, how to quarantine any malicious code, and many other factors. Sometimes, forensic analysis is what uncovers a cyber event in the first place. The average cost to have an outside firm perform computer forensic analysis to determine if a cyber breach has occurred and what data may have been compromised averages around \$700 per hour.
- **Business Income** – Many businesses rely on websites and e-commerce portals for income, such as point-of-sale devices at retail locations. Lost income results when sales cannot be made or systems cannot be accessed because data and/or systems have been compromised. Insureds can also have a loss resulting from a cyber event that affects a major supplier or other business on which the insured depends. Business income coverage from dependent properties may be an option available on some cyber policies.
- **Website Vandalism** – Even if the business does not rely on its website for e-commerce operations, a website is a valuable tool for promoting the goods and services provided. Websites can be vandalized by infecting them with viruses or malware. Images and words can be replaced with vulgar or profane images or language. The insured may have to pay for services to have the website scrubbed and content replaced.
- **Notification costs** – When confidential files are breached, cyber regulations require notification of affected parties. Notification can include notification by regular mail and email. Employee overtime or call centers may be needed to handle inquiries from affected parties. Some cyber regulations require the business to provide identity theft monitoring and protection for at least one year.





- **Ransomware and cyber extortion** – Malware can be installed on the insured's computer systems that will allow hackers to take control by encrypting data. The insured is then presented with a demand for ransom before the data is decrypted and given back to the insured. Other times, hackers will threaten to encrypt data or release sensitive information if the insured does not pay. This is known as cyber extortion.
- **Denial of service attacks** – Another way of attacking e-commerce portals is through denial of service (DoS) and distributed denial of service (DDoS) attacks. Hackers use infected computers they control to make repeated connections to an e-commerce portal or website. The repeated connections use up the available bandwidth so that others who wish to access the site or portal cannot.



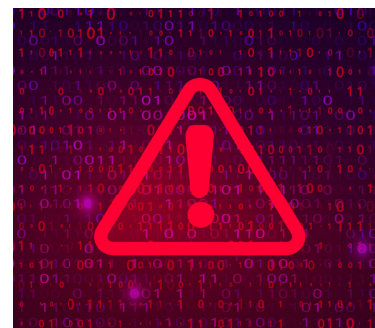
When the attack comes from one computer, it is a DoS attack. When the attack comes from multiple computers, it is a DDoS attack.

- **Repairing or restoring data** – When data has been damaged or destroyed, databases must be repaired or restored. The cost to re-enter or restore data can be very expensive.
- **Negative publicity** – When news of a data breach becomes public, there is never a positive spin. Many small businesses never recover from a cyber breach because the public may no longer feel comfortable having their information stored in the business's computer system. When a breach occurs, it can cost a significant amount of money to stabilize and restore the reputation of that business.
- **PCI DSS** – When a business accepts credit cards, it must have approval and certification from the Payment Card Industry (PCI). PCI's Data Security Standard (DSS) is the certification that is required. When credit card data is compromised, the business must go through the entire DSS certification process again; this is time-consuming and expensive.

## Third-Party Cyber Liability Risk

Most cyber losses are first-party losses. In the event of an information security breach, there won't necessarily be a liability claim against the insured. That could change, though, if the accessed data is used to steal someone's identity or in some other unauthorized manner. When that happens, the breach can result in first-party and third-party claims. Third-party liability claims can arise in several situations.

- **Infected emails** – Emails can include attachments that contain viruses and malware. If an insured's employee forwards an infected email to another company and causes that company's system to be infected, the insured can be held responsible.
- **Infected websites** – In addition to email attachments, websites can be infected with viruses or malware. If customers and others have virus or malware attacks that result from visiting the insured's website, liability issues can be created.



## Section 3: Risk Control and Mitigation - Property and Liability

- **Wrong recipient** – It's not uncommon to send the right email to the wrong person. Many email programs allow for auto-population of email addresses by just typing the first few letters and then hitting the tab key. If an employee is not paying attention, sensitive personal or corporate information can be sent to the wrong person, violating contracts or privacy regulations.
- **Infringement issues** – Copyrights and intellectual property rights can be easily violated. When websites are created, the content (words, pictures, videos, etc.) can cause issues if it contains information that has not been properly secured via royalties. Blogs, vlogs, testimonials, and website comments can cause libel and other disparagement issues.
- **Regulatory issues** – Lawsuits alleging violation of state, federal, and foreign regulations can be brought against the insured. Sometimes, there are fines and penalties that result from violating these regulations. Federal acts such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Gramm-Leach-Bliley Act are a few federal regulations that govern certain protected information. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws that govern privacy. The California Consumer Privacy Act (CCPA) is one of the strictest regulations in the country. Since business is conducted on the World Wide Web, insureds must be aware of foreign regulation such as the European Union's General Data Protection Regulation (GDPR) and how it affects business. Since fines and penalties are assessed directly to the insured, it's possible to see this addressed as a first-party coverage in some cyber policies.



As in all types of negligence, cyber liability requires a duty to protect a party from harm and a breach of that duty. The significant breach of duty for cyber liability is providing inadequate data security. This would include the unauthorized disclosure of customer personal data. Other examples include failure to provide secure transactions that comply with PCI protocols, failure to prevent or react to unauthorized intrusions to the data, including non-compliance with breach notification statutes, the failure to protect web-based storage and databases from unauthorized access and distribution, and the failure to exhibit due diligence in the development and implementation of new applications, systems, and procedures. Courts appear to be reluctant to limit liability for an organization if they fail to provide adequate security controls.



### CONTRACT VIOLATIONS



For example, in January 2023, T-Mobile experienced a data breach affecting 37 million accounts. This was the second major cyber attack they have had in less than two years and it came just months after settling a lawsuit related to a 2021 event, which compromised the information of 76 million people.

## Section 3: Risk Control and Mitigation - Property and Liability

Review the various types of cyber risks and examples of those risks in the following table.

Types of Cyber Risk	Examples
<b>First-Party</b>	An insufficient security system allows hackers access to proprietary information such as the recipe for a new food product.
	A former employee hacks into the former employer's computer system to post defamatory items from the company's social media account.
	An employee laptop containing their organization's confidential R&D information is stolen.
	A major cyber attack on air traffic control could result in loss of life and property.
<b>Business Interruption/ Net Income</b>	After a breach of guests' personal information, the reputation of an international resort is damaged, and reservation numbers are down.
	A business is required to take down its website due to copyright infringement for using unauthorized images.
	A cyber-criminal hacks a smart security system, causing it to malfunction, therefore resulting in loss of income to the business from damage to reputation and brand.
	A denial-of-service attack blocks agents from accessing an insurance company's website and prevents them from submitting applications.
<b>Third-Party</b>	A medical office employee emails a medical record to the wrong patient, breaching the medical record owner's right to privacy.
	An organization uses a "cloud" service to store customer data, which could result in a substantial loss if the cloud is breached.
	A national retailer has their credit card payment system hacked.
	An employee accidentally forwards an email containing a virus to their company's client list.

# Check-In



**Directions:** Match the activity in the left column to the type of cyber risk in the right column. Note, the terms on the left are used more than once.

<b>A. First-Party</b> <b>B. Third-Party</b>	_____ After suspicious activity on their network, a company assumes they may have suffered a data breach. The company hires a forensics investigator.
	_____ A company hires a web designer to rebuild their website. The web designer fails to secure permission to use several images they included on the website.
	_____ An E-commerce website suffers a data breach. As per state regulations, they must notify consumers and offer identity theft monitoring services.
	_____ A company based in the U.S. conducts most of its online business in the EU. They have access to confidential client information.
	_____ A nurse mistakenly sends a patient’s medical record to the wrong individual.

## Cyber Risk Control Techniques

Sound risk control measures begin with risk identification and analysis of the various exposures discussed previously. The risk manager should characterize the organization's cyber exposures, hazards, and potential perils that threaten the organization. Some potential methods by which these exposures can be identified include:

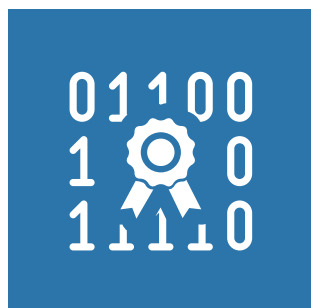
1. Perform a cybersecurity threat/vulnerability assessment and evaluate threat scenarios.
2. Evaluate new and existing applications, systems, and data management plans for proper security controls during planning, implementation, and operation. Are there any end-of-life systems/legacy systems with no technical support or patches? If it is not feasible to replace them, additional controls are advised, such as restricting user access and ensuring they are not internet accessible.



## Cyber Risk Control Measures

Risk control measures evolve and are developed as the frequency and severity of cyber losses increase. Depending on the nature of the organization, a combination of controls may be appropriate and effective.

### Zero Trust Architecture



Zero trust is a significant departure from traditional network security, which followed the “trust but verify” method. The traditional approach automatically trusted users and endpoints within the organization. This put the organization at risk from both internal employees and those who were able to obtain valid credentials. Once accounts are compromised, unauthorized and widespread access is available. As organizations responded to the changing workplace environments necessitated by the pandemic, the trust but verify method was no longer a viable option.

Zero trust architecture requires the continuous validation and monitoring of a user's privileges and those associated with their device. All access requests are reviewed before allowing access to company systems or assets. The zero trust model anticipates a breach and verifies each request as though it originated from an open network. Zero trust's focus is “never trust, always verify.” Every request is fully vetted and verified before granting access.

### Multifactor Authentication

Multifactor authentication (MFA) is a security layer that requires the user to provide two or more pieces of evidence to be authenticated. Traditionally, authentication requires only a username and a password. However, usernames are often easy to discover. For example, in many situations, a username is the same as an e-mail address. Furthermore, since passwords can be hard to remember, people tend to pick simple ones or



## Section 3: Risk Control and Mitigation - Property and Liability

use the same password at many different sites, increasing the likelihood that an unauthorized user will access an account.

When MFA is used, users must provide additional information beyond their password to access a system. This second factor is usually:

- Things you know—such as a password or other personally known data, like the answers to security questions
- Things you have—such as an ID badge with an embedded chip or a digital code sent to the user's cell phone or email
- Things you are—such as physical traits, like your fingerprints or voice. It is important to note that employer use of biometrics is undergoing legal scrutiny.

Many software programs innately require multifactor authentication—for example, Microsoft 360. The National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, offers guidance for creating MFA programs on this course's "Resources" webpage on Risk & Insurance Education Alliance website.

### Privileged Access Management

Privileged access management (PAM) is a security technology that allows differing levels of access within an organization. Some users have greater privileges than others. PAM offers a privileged level of access, which protects organizational assets. PAM follows the "least user" principle—users only receive that level of access required to perform their work responsibilities.

### Cybersecurity Awareness Training

Employees are critical to the success of a cybersecurity risk control program. Employees should be aware of the usual risks and threats and how to identify and respond to them. The goal is to create a culture of awareness. Conducting regular training and exercises keeps security top of mind. In addition, employees should understand the confidential nature of the data the organization collects and its proper handling. Training topics can include the variety and types of attacks, the importance of strong, unique passwords for each program used, restrictions on personal use of company devices, and when and how to access the internet on those devices. Consider a scenario:



Increasingly concerned with ransomware and phishing attacks in the manufacturing industry, XYZ Widgets decides to conduct cybersecurity awareness training. Employees are taught about email phishing and how to mark suspicious emails for further review. After the training, the company sends fake phishing emails to employees to ensure the training is successful. Employees who click on links in the simulated phishing emails are assigned further training.



## Incident Response Plan

In addition to taking steps to prevent cybersecurity incidents, organizations should establish an incident response plan. An **Incident Response Plan** is a set of protocols and instructions for responding to and mitigating a cyber attack. These plans integrate the organization's overall disaster recovery plan as well as an IT Recovery Plan and a Business Continuity Plan. These plans will be discussed in more detail in Section Four of this Learning Guide, but know that the Incident Response Plan should be widely disseminated, explained, and even practiced.

For the plan to succeed, it will need support and cooperation from all affected areas of the organization.

Some sample plan activities include:

- **Isolate the source** – Find the source of the breach and remove it from the affected systems.
- **Determine the scope** – Identify which systems were breached, to what degree, and the exact type and number of records that were accessed.
- **Maintain compromised hardware** – Hardware should be stored, as law enforcement may need it for a forensic evaluation.
- **Determine state and federal notification requirements** – Did the nature and scope of the breach trigger any statutory notification requirements?
- **Required notifications and any additional mitigation steps** – Determine when to initiate required notices and any other steps, such as offering credit monitoring services, etc.

## ▶▶ Knowledge Check



**Directions:** Read the scenario below and explain your response.



Ned owns a comic book store in the revitalized downtown section of his city. While meeting with Ned to discuss his insurance coverage, you discover he is also the largest comic book dealer on the internet, selling his comic books on an international sales platform. While Ned's local sales are lackluster, his e-commerce sales are lucrative.

What cyber exposures does Ned have? What cyber risk control measures could Ned potentially implement?

---

---

---

---

---

---

---

---



# Contractual Risk Transfer

## Learning Objective:

3.5 Describe the four types of contractual risk transfer and the three types of hold harmless agreements

Contractual risk transfer is the reduction of an organization's liability exposure through the proper structure of contracts and other agreements. It is a transfer of financial responsibility that uses external funds to pay for losses. Both non-insurance contractual transfer of control or responsibility and non-insurance contractual indemnification of financial responsibility are types of transfers. Contractual risk transfer shifts non-insurance financial responsibility for certain liabilities from one party to another.

For example, if a general contractor wants to be sure he shifts as much financial responsibility as possible for claims to another party, he may require subcontractors to sign an indemnification or hold harmless agreement before they can perform work for him.



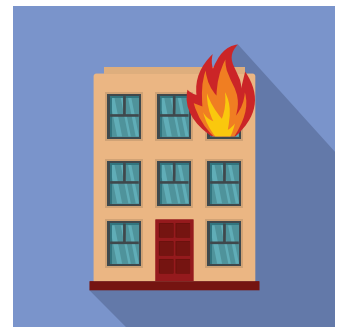
## Four Types of Contractual Risk Transfer

In total, there are four types of contractual risk transfer.

A **waiver of subrogation** is a pre-event agreement to waive the right to seek recovery from a responsible party's insurance carrier for loss payments made to the insured. For example:



A landlord buys a fire insurance policy from an insurer. The tenant's negligence causes a fire in the landlord's office building, resulting in one million dollars of damage. The insurer pays the landlord the million dollars. If the landlord's contract had a waiver of subrogation as to the tenant, that waiver would bar the insurer from suing the tenant after the insurer paid the landlord for the damages.



An **exculpatory agreement** is an arrangement whereby one party agrees to absolve a second party from any blame, even when damage or injury is caused by negligence of the second party. Consider an example:



Richard and Joan live next door to each other. Joan has a pool in her backyard. A fence surrounds the pool. Richard has a tall oak tree in his backyard, and the branches extend over Joan's pool. So, almost every day, Joan must skim leaves from Richard's oak tree out of her pool. Worse, she has to spend a lot of time backwashing the filter each spring due to the pollen—which is, again, caused by Richard's tree. One day, Richard tells Joan he plans to cut down the tree, but he worries about limbs falling and damaging her fence. Joan is so happy the tree

will be gone she quickly agrees that she will not ask Richard—or his insurance company—to pay for any fence repairs that might be caused when the tree is being cut down. Together, Richard and Joan write an agreement expressing the terms, and they both sign the document.

A **limitation of liability clause** in a contract with a client typically limits the liability of the company to some proportion of its fee or a defined dollar value. These are often found in equipment leases. These clauses are often called **liquidated damages clauses**. For example:



A developer sued the consulting engineers who had designed a man-made lake for a housing project. The lake liner failed, leading to a five million dollar claim against the engineer for damages to the surrounding houses. The engineer asserted that, as specified in a clause in its contract with the developer, liability was limited to the amount of its fee—\$25,000. A trial court agreed with the engineer.



**Hold harmless agreements** are contractual arrangements whereby one party (the indemnitor) assumes the financial consequences of the liability inherent in a situation, thereby relieving the other party (the indemnitee) of that financial responsibility. There are several different types of hold harmless agreements to be aware of.

### Types of Hold Harmless Agreements

Hold harmless agreements can vary in their language. For example, some agreements may include the indemnitee's cost of settlements or judgments paid to a third party and the costs of defense. Hold harmless agreements may also require indemnification at the conclusion of a claim or suit or require the indemnitor to assume the indemnitee's actual defense obligation during a claim or suit. This distinction is important because it identifies the responsible party for providing the indemnitee's defense and therefore, who selects and controls the defense for the indemnitee.

Beyond addressing the responsibilities of defense, the three main classifications of hold harmless agreements are limited, intermediate, and broad.

#### Limited Form Hold Harmless Agreements

In the **limited form** hold harmless agreement, the indemnitor assumes responsibility for the indemnitee's liability for the indemnitor's negligence only. This classification applies to agreements requiring indemnification for occurrences arising from the indemnitor's operations. Some examples include:



**Example A** — A contractor (the indemnitor) remodels an entire supermarket while the supermarket (indemnitee) continues operations. The contractor knocks over a display of eggs and walks away. A customer then slips on the broken eggs and is injured. The contractor must indemnify the supermarket for his own negligence.



**Example B** — Suppose the contractor knocks over a display of eggs and informs the supermarket manager, who does not clean up the mess promptly. A customer slips on the broken eggs and is injured. The failure of the supermarket to respond to a timely notification creates a shared liability situation; therefore, the contractor is only required to indemnify the supermarket for its proportionate share of the total liability. The store may not seek payment from the indemnitor for the supermarket's negligence in failing to clean up the hazard in a timely manner.



### Intermediate Form Hold Harmless Agreements

An **intermediate form** hold harmless agreement incorporates the responsibilities in the limited hold harmless agreement plus responsibility for the indemnitee's liability for the indemnitor's and indemnitee's joint negligence. This classification applies to agreements requiring indemnification for all occurrences arising from the indemnitor's operations, excluding only the liability arising from the indemnitee's sole negligence.

Under an intermediate form, using example B above, the contractor would be responsible for both his negligence and the supermarket's negligence for failing to clean up the broken eggs.

### Broad Form Hold Harmless Agreements

A **broad form** hold harmless agreement incorporates the responsibility of both the limited and intermediate, plus the indemnitor agrees to be responsible for the indemnitee's sole negligence.

This classification applies to agreements requiring complete indemnification of the indemnitee for all occurrences without reference to negligence; it can even include those situations arising from the sole negligence of another entity. Broad form hold harmless agreements are often found in construction contracts where the general contractor requires every subcontractor to indemnify regardless of fault. Consider some examples:



**Example 1** — If, in the example above, a store employee knocked over the eggs and the store failed to clean up, under a broad form hold harmless, the contractor would be required to hold the store harmless from any claim filed by the injured customer—even though he had no responsibility for the situation.

**Example 2** — Joe's Plumbing assumes responsibility for all liability without regard to the fault of himself and/or Big Construction Company. Here, Joe assumes not only the responsibility for his acts in addition to any acts arising from joint and/or concurrent negligence of Joe's Construction and Big Construction Company, but also those situations that result from the sole negligence of Big Construction Company.

### Section 3: Risk Control and Mitigation - Property and Liability



These broad form agreements would appear totally unreasonable since they would include losses that do not arise from the indemnitor's negligence and may involve situations in which the indemnitor has no control or involvement. These broad form agreements are sometimes referred to as being against public policy or unconscionable in that a negligent party may avoid responsibility for injury or damages by having made a contract with another party.

Nevertheless, the courts may enforce such agreements that do not violate a statute or public policy. Generally, the courts will require the intent of the parties to enter into such an agreement to be expressly reflected in the contract (absolutely clear and unequivocal) and may require specific consideration to be enforceable.

The risk manager should be aware of any anti-indemnity statutes (intended by the states to prevent parties from eliminating their incentive to exercise due care) that might affect the interpretation of a hold harmless agreement. Anti-indemnity statutes limit or prohibit the use of hold harmless agreements in contractual transfers in certain circumstances. In many states, for certain types of contracts, broad form hold harmless agreements are restricted or even entirely prohibited by state statutes as being against public policy. Since determining whether a statute applies is a legal opinion, the risk manager should always seek advice from legal counsel.



Comparison of Contractual Transfers			
Hold Harmless Agreement	Exculpatory Agreement	Waiver of Subrogation	Limit of Liability Clause
<b>Definition</b>			
Affirmative assumption of the financial responsibilities of another by contract	Pre-event exoneration of the fault of one party that results in any loss or specified losses to another	Pre-event relinquishment of the right of one or both parties' insurers to seek recovery from the culpable party for loss payments made to the insured	Pre-event limitation of the amount, type, or method of calculation of damages available to one or both parties to an agreement
<b>Tort</b>			
Does not absolve the indemnitee from its tort liability to a third party	Absolves the tort liability between one or both parties to a contract; does not apply to 3rd parties	Does not absolve the tort liability of the parties but prevents insurers from any recovery of loss payments based on such tort liabilities	Does not absolve the tort liability of one or both parties; however, it limits recovery of the amount of damages between the parties
<b>Funding</b>			
Requires indemnitor to be able to provide funding/financing of assumed liabilities	No affirmative obligation to provide funding except that required to absorb the loss	Same as exculpatory, except the insurer absorbs the loss under an insurance transfer	Requires funding or financing of amounts payable for the amount of damages as defined in the contract
<b>Anti-Indemnity Application</b>			
May be subject to anti-indemnity statutes	Not subject to most anti-indemnity statutes	Not subject to anti-indemnity statutes	Usually involves bills of lading, cargo, freight, or cartage and is not subject to anti-indemnity statutes

## Creating a Risk Control Program for Contract Review



When creating a risk control program for contractual review, the risk manager or senior management must decide what contracts or agreements will be reviewed and determine a mechanism for completing the review. Ensuring access to and reviewing all appropriate contracts (both those the organization uses and those of others the organization enters) will be challenging. The risk manager must work with the legal department or consultants to monitor, evaluate, and continuously update contract language.

There are also some practical problems with the contractual review process, such as who is in the driver's seat when negotiating the contract. It could be the risk manager, the operations manager, the legal department, or even another party. Sometimes, the risk manager is the last to know about a contract. This is why coordination with attorneys is necessary to verify the scope of assumed liabilities and the viability of contract language.

When negotiating a contract, it is wise to ask for only what an organization can give. State-to-state contract interpretation will vary because governing laws are dynamic, and there are limitations, such as safety in the workplace, sole negligence, and anti-indemnity statutes. Contractual transfer of risk also poses several common practical issues:

- The contract can shift the risk to another, but the risk still exists.
- Both parties are expected to perform or assume certain responsibilities; however, if either party fails to meet the responsibilities, those responsibilities may fall back on the other party.
- There is little or no control of either party's performance by the other party.
- A contract should not be substituted for normal business responsibility or more appropriate risk control techniques.

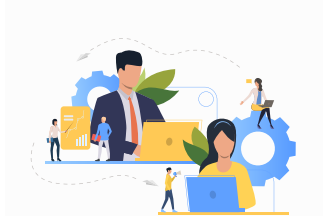


These agreements commonly appear in construction agreements, service contracts, purchase orders, waivers, leases, and other contracts and instruments. When looking for hold harmless wording, the risk manager should look for references to insurance clauses, liability clauses, hold harmless and indemnification clauses, or other camouflaged language, such as mutual release or waivers of subrogation.

## ▶▶ Knowledge Check



**Directions:** Identify and explain the results of the contractual risk transfer in the following scenario:



Wilson Designs hires an information technology company, ABC IT, to upgrade its data management system. The contract contains a mutual waiver of subrogation. One of ABC IT's employees is walking across Wilson's office when he trips over a rip in the carpet and breaks his leg. The ABC IT employee files a workers compensation claim. The following week, one of Wilson's own employees breaks his arm when he trips over tools that an ABC IT employee left on the floor. How will the waiver of subrogation impact ABC IT's and Wilson Designs' insurance carriers?

---

---

---

---

## Summary

Organizations face a multitude of property and liability exposures, which could subject them to losses and claims. An effective risk manager will consider the sources and put risk controls in place to reduce and mitigate those losses.

Employment practices liability encompasses several general areas: violation of statutes, discrimination in hiring, promotion, discharge, compensation, workplace harassment, retaliation, invasion of privacy, and wrongful termination. The risk manager uses specific risk control methods for each of those exposures.

Fleet exposures require specific hazard control techniques. Fleet exposures can be present in all four logical classifications of risk—property (physical damage to vehicles), liability (injury to third parties), human resources (employee injuries), and net income (loss of revenue). An effective fleet management program helps control and reduce accidents, injuries, and losses.



Property assets of most businesses include the buildings occupied as offices, manufacturing, storage, sales, residential, etc. The continued availability of building space for conducting operations is critical to the survival of most businesses. The risk manager must develop the knowledge and skills to protect these assets.

Cyber risk exposures include both first-party and third-party losses. First-party losses are those that have a direct effect on the insured's operations or property. Third-party liability claims can result from several acts, including infected emails, infected websites, and sending confidential information to the wrong recipient. Control measures evolve and are developed as the frequency and severity of cyber losses increase. Depending on the nature of the organization, a variety of controls may be appropriate and effective.

Contractual risk transfer is the reduction of an organization's liability exposure through the proper structure of contracts and other agreements. It is a transfer of financial responsibility and uses external funds to pay for losses. Creating a risk control program for contract review lets the risk manager analyze and respond to the obligations of the organization to others as well as the obligations of others to the organization.



## Section 3 Self-Quiz

**Directions:** Respond to the questions below.

1. Which one of the following is an example of a “disparate impact?”
  - ☐ An employer requires a pre-employment written test. An analysis of the data shows that mostly non-Caucasian candidates fail the test.
  - ☐ An employee talks about his husband in the workplace. A manager decides to fire that employee for his sexual orientation.
  - ☐ An interviewer asks a prospective employee where he is from. On discovering the employee is from Pakistan, the interviewer rejects the employee’s application.
  - ☐ A large consulting firm refuses to provide accommodation to an employee who has recently become wheelchair-bound.
  
2. Which one of the following would most likely be considered an example of sexual harassment?
  - ☐ A male employee invites a female employee to an informal happy hour.
  - ☐ Two coworkers at the same seniority level have a consensual relationship.
  - ☐ An employee made some off-color, sexually-oriented jokes at a holiday party.
  - ☐ A boss solicits her employee for a date in exchange for additional time off.
  
3. Which are appropriate risk control measures for employment practices liability exposures? **Select all that apply.**
  - ☐ Train interviewers to avoid sensitive topics like race and focus on a candidate’s qualifications during an interview.
  - ☐ Involuntarily reduce the hours of an individual complaining about sexual harassment so they can feel more comfortable.
  - ☐ Remove the names and addresses of prospective employees when sending resumes to a hiring committee.
  - ☐ Subject employees injured in a workplace accident to a performance improvement plan and increased scrutiny.

### Section 3: Risk Control and Mitigation - Property and Liability

4. Match the hazards described in the right column to their corresponding risk category shown on the left.

<b>A. Property</b> <b>B. Liability</b> <b>C. Human Resources</b> <b>D. Net Income</b>	_____ Severe tornado weather grounds most of a shipping company's air freight fleet but causes no actual damage.
	_____ Lightning strikes Peter's house and "fries" his computer.
	_____ An employee of a trucking company had a stroke and collapsed in the warehouse.
	_____ An employee of a delivery company is delivering his load to Tom's shoe store and strikes a customer with the hand truck.

5. Your client complains that their truckers have been in numerous accidents due to their own aggressive driving. Which risk control measure would most directly address this concern?
- ☐ Use "How am I driving?" signage on all vehicles.
  - ☐ Ensure all drivers have valid licensing.
  - ☐ Have GPS tracking of all vehicles.
  - ☐ Increase limits on the business auto policy.
6. In 2013, a fire began at a fertilizer distribution company. The fire reached the ammonium nitrate, resulting in a large explosion. The \_\_\_\_\_ was the peril; the \_\_\_\_\_ was the hazard.
- ☐ fertilizer distribution; explosion
  - ☐ ammonium nitrate; fire
  - ☐ fire; ammonium nitrate
  - ☐ explosion; fire
7. Which risk control measure could the fertilizer company have implemented to reduce or eliminate the hazard? **Select all that apply.**
- ☐ Stop the use of ammonium nitrate in the production of fertilizer.
  - ☐ Enhance the fire mitigation systems and store the ammonium nitrate in a separate building.
  - ☐ Work with local fire brigades to ensure rapid response to a fire incident.
  - ☐ Provide training to employees to correctly identify any safety hazards.

### Section 3: Risk Control and Mitigation - Property and Liability

8. A company could reduce its maximum possible loss from fire by \_\_\_\_\_.

- ☐ installing new fire mitigation systems
- ☐ relocating its operations to an area with a better-funded fire department
- ☐ separating its operations into buildings located in three different states
- ☐ purchasing a state-of-the-art fire alarm system

9. A graphics design and website hosting firm based in the United States offers a service where they design and host a client's website. They work with clients across the globe. One of their largest clients is an online music equipment rental service.

Read the statements below regarding the client's cyber risk exposures and determine if the statements are true or false.

- a) Data storage and collecting private client information are significant cyber risk exposures for the company.

True

False

- b) The company could be held liable if one of its client's websites is hacked and used to spread computer viruses.

True

False

- c) Since the company is chiefly based in the United States, they are only exposed to regulatory issues stemming from US statutes.

True

False

10. A company has instituted a new cybersecurity protocol that requires employees to enter a code sent to their work cell phone before logging into their work accounts. This is an example of \_\_\_\_\_.

- ☐ zero trust architecture
- ☐ multifactor authentication
- ☐ privileged access management
- ☐ an incident response plan

11. A natural gas distributor targeted in a ransomware attack is unable to distribute gas to homes. During the crisis, the company loses income. This is an example of a \_\_\_\_\_.

first-party cyber risk

third-party cyber liability risk

12. A healthcare company is hacked. The private health information of thousands of companies is presumably compromised, and a lawsuit occurs. This is an example of \_\_\_\_\_.

first-party cyber risk

third-party cyber liability risk

### Section 3: Risk Control and Mitigation - Property and Liability

13. Match the scenario on the right to the corresponding type of contractual risk transfer employed shown on the left.

<p><b>A.</b> Intermediate hold harmless agreement</p> <p><b>B.</b> Exculpatory agreement.</p> <p><b>C.</b> Limit of liability</p> <p><b>D.</b> Broad form hold harmless agreement</p> <p><b>E.</b> Waiver of subrogation</p> <p><b>F.</b> Limited form hold harmless agreement</p>	<p>_____ Bob needs some electrical work done. His buddy, John, is a good handyman who volunteers to do the work for free. John is concerned that he might damage something while doing the work. Both sign an agreement that Bob will not pursue John for any damages he causes while doing the work.</p>
	<p>_____ A construction company subcontracts with a roofer. A loss occurs for which the roofer and the construction company share joint liability. Under the contract, the roofer is only responsible for their share of the liability.</p>
	<p>_____ A logistics company has entered into a contract with a client to ship \$1 million worth of electronics. The logistics company specifies in the contract that the company's liability for any loss or damage of goods in transit is limited to \$500,000.</p>
	<p>_____ A contractor is hired to perform renovations in a commercial building. The property owner agrees not to have their insurer pursue legal action against the contractor's insurer in the event of a fire due to the contractor's negligence.</p>
	<p>_____ A subcontractor signs an agreement where he is responsible for all liability without regard to fault of himself and/or the company he is contracted by.</p>
	<p>_____ A construction company subcontracts with an HVAC company. A loss occurs that both companies are jointly liable for. Under the contract, the HVAC company is responsible for their own negligence and the negligence of the HVAC company.</p>

## Set Yourself Up for Success!

### Visit the “Resources” Webpage at [RiskEducation.org/RCresources](http://RiskEducation.org/RCresources)

For valuable reinforcement, be sure to visit the “Resources” webpage. This webpage contains a variety of materials that will help you absorb the course material *and* set you up for success on the Final Exam. You’ll find:

#### **Study Guide**

Download a copy of the Study Guide. It contains all the Check-In questions, Knowledge Checks, and Self-Quizzes contained in this Learning Guide in a format that makes it easy for you to practice and check your answers.

#### **Flash Cards**

Play an interactive vocabulary game with a study set of digital flashcards to enhance your learning of the insurance and risk management terms used in this course.

#### **Review Game**

Use a fun, trivia-style review game to test your knowledge and prepare for the Final Exam.

## In Addition...

#### **Appendix**

The Appendix of this Learning Guide contains a Glossary of terms as well as tips for study techniques and sample test questions that will help you prepare for the Final Exam.

## Section 4: Crisis and Disaster Planning

# Section 4: Crisis and Disaster Planning

---

## Section Goal

This section focuses on how a crisis or disaster can arise and its potential impact on the operations and livelihood of an organization. Crisis and disaster planning techniques and the four phases of crisis management will be explored. In addition, best practices in crisis communications are reviewed.

## Learning Objectives:

- 4.1 *Define a crisis, its characteristics, its phases, and the potential impacts it may have on an organization.*
- 4.2 *Describe the terms crisis management, business continuity, and disaster recovery, and explain the relationship between the three terms.*
- 4.3 *Describe the principles of an effective crisis management program, including general crisis management goals.*
- 4.4 *Explain the four essential steps of the crisis management process.*
- 4.5 *Describe the important considerations of reputation management during a crisis.*
- 4.6 *Use the principles of crisis management to respond to a hypothetical crisis scenario.*

Before discussing crisis management plans, it is essential to understand that no single type of event qualifies as a crisis. The characteristics of events that are called crises are wide, varied, and often contradictory.

In some cases, a crisis may have the potential to cause significant damage to the organization's reputation, while in others, the crisis is entirely self-contained and impacts only an organization's internal processes. A crisis may damage consumer, shareholder, and employee confidence in the organization or its brands, but in other cases, the crisis may strengthen confidence. It may directly involve multiple audiences and stakeholders or affect only one or a few.

A crisis may be newsworthy and attract the media's attention, remain unknown by the media entirely, or be simply noted and forgotten almost as soon as it becomes known. Crises may be unique to one organization or individual or affect many. Crises can be entirely unpredictable or largely anticipated. It is also important to note that an event can be considered a crisis when reputation is damaged, even if it does not have a significant, direct financial impact on an organization.



# Defining Crises and Other Key Terms

## Learning Objective:

- 4.1 Define a crisis, its characteristics, its phases, and the potential impacts it may have on an organization.

A crisis is any critical incident that threatens or causes injury to people, significant property damage, or a disruption of normal business operations. Crises may also include threats to an organization's financial welfare or reputation, such as potentially damaging media attention, public opinion, or regulatory action.

The impact of a crisis can take many different forms. A crisis can impact a business's operations in a variety of ways, ranging from a disruption in activity to a total shutdown. Financial consequences can also vary and may result in anything from increased expenses and reduced income to bankruptcy. In fact, a single event may have disparate impacts on various organizations experiencing the crisis.



Consider some examples:

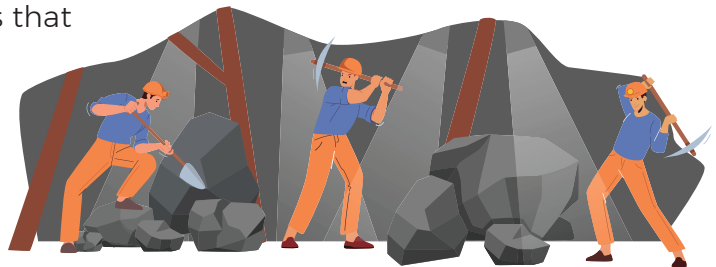


In 2005, Hurricane Katrina made landfall as a Category 3 storm. Undoubtedly, Hurricane Katrina created a multitude of crises. In particular, New Orleans was subject to large floods that resulted in the total cessation of business for many large and small companies in the city. However, companies in the French Quarter escaped major flooding and only suffered from a temporary disruption due to the storm and a lack of new customers afterward.



On January 2nd, 2006, an explosion in the Sago Mine in Sago, West Virginia, trapped 13 miners over 9,000 feet down, inside the coal mine. The malfunctioning emergency breathing apparatus of some rescue workers added to the woes of the trapped miners. Only one of the thirteen survived, and this disaster was the largest of its kind up to that date<sup>7</sup>.

To summarize, crises are incidents or events that cause injury to people, significant property damage, or damage to organizations. To properly prepare for a crisis, it is important to understand the various sources of crises.



<sup>7</sup> Davis, Matthew. "US Mining Safety Under Scrutiny." BBC News, January 5, 2006. Accessed August 11, 2023. <http://news.bbc.co.uk/2/hi/americas/4585482.stm>



## Sources of Crises/Disasters

### Human Hazards

A crisis may stem from many sources. Some of the most difficult to avoid and most expensive to mitigate are those caused by human hazards. These hazards may be accidental in nature, arising from simple negligence. For example, some restaurant employees could unintentionally cause a grease fire that spreads out of control, damaging an entire city block.

Other crises can be the result of organized and deliberate human actions. For example, in Boston in 2013, two individuals carried out a bombing at the Boston Marathon in a deliberate attempt to harm people and property.



### Environmental and Natural Hazards

Crises created by the occurrences of environmental and natural hazards are challenging and/or impossible to control because they can be widespread and far-reaching. A union of science and engineering methods have been applied to prevent or reduce the damage to structures from hurricanes and earthquakes, but not the prevention of the hurricane or earthquake itself. As a result of climate change, it is likely that the frequency of these hazards and the impacts they have on organizations and individuals will accelerate.

### Industrial or Technological Disasters

Industrial or technological disasters run the gamut from a loose wire connection that causes a serious fire to the failure of an entire system. For instance, in 2003, several tree branches touching high-voltage powerlines in Ohio cascaded into one of the most extensive blackouts in history because of a series of software issues and system failures.



One of the most notorious industrial disasters occurred in 1984 in Bhopal, India. During this incident, 40 tons of toxic gas leaked from a pesticide plant, killing at least 3,800 people directly. The incident ultimately stemmed from the facility operating with sub-par safety procedures, with some preventative equipment being disabled and others operating below safety standards<sup>8</sup>.

Overall, the disaster at Bhopal illustrates a critical point. Industrial hazards can be mitigated, reduced, or avoided by redundancy of systems and preventative maintenance, which are far less expensive than dealing with the event itself.

<sup>8</sup> Broughton, E. "The Bhopal Disaster and Its Aftermath: A Review." *Environmental Health: A Global Access Science Source* 4, no. 1 (2005): 6. <https://doi.org/10.1186/1476-069X-4-6>

## Biological Events or Pandemics



Disasters may also take the form of a biological event or a pandemic. These may be natural in origin, such as the Spanish influenza outbreak in 1918 that spread throughout the world and killed as many as 100 million people or the COVID-19 pandemic, which, according to the World Health Organization, has killed almost 7,000,000 individuals as of August 2023. Biological events may also be intentional, such as the case of terrorists using biological weapons.

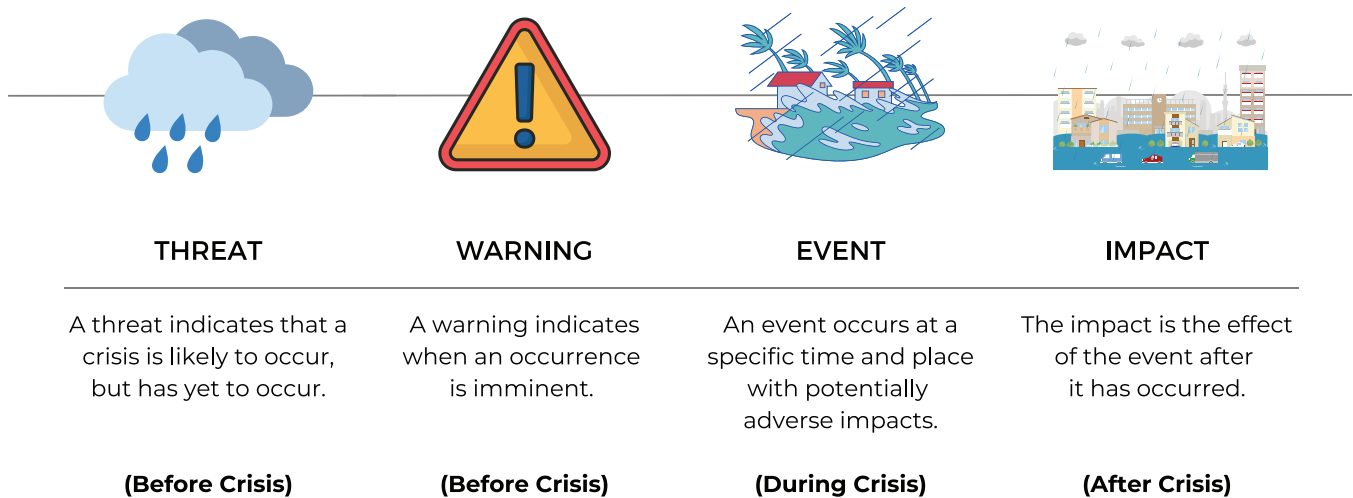
## Infrastructure and Transportation Disasters

Last, some disasters may arise from breakdowns of infrastructure and transportation. The mortgage crisis of 2008 was a breakdown of a financial infrastructure that led to severe economic consequences for many who overextended themselves with debt. A bridge collapse in Minneapolis in 2007 caused 13 deaths and 145 injuries. It also caused a significant downturn in the local economy and led to increased attention on other potentially dangerous bridges vital to local areas.



## Phases of A Crisis

Crises are composed of four major phases: threat, warning, event, and impact. The following graphic summarizes these phases.







The threat is simply a likely probability of occurrence; however, the event has not yet occurred. For example, a tropical storm brewing in the mid-Atlantic may not yet be considered a threat to the American coast due to its unlikely landfall. However, it becomes a threat if the storm increases to hurricane strength, curls toward the Caribbean, and then heads for the Florida coast. A warning is the second phase and is when the occurrence is imminent, i.e., the outer bands of the hurricane are just beginning to be felt. At this moment, the storm could still lose strength or turn out to sea. The third phase is an event—when the hurricane makes landfall. The event is happening. The final phase is the impact

## Section 4: Crisis and Disaster Planning

after the event has occurred. It is worth noting that not all crises have all phases. Some move directly to an event and impact with little to no threat or warning, such as an active shooter situation.

Recognition of these phases helps the risk manager schedule specific pre-loss, response, and post-loss activities. View the following example to see the different phases of a hurricane crisis and the risk management activities that would occur during the various phases.

### Example: Tropical Storm Margo Brewing in the Pacific Ocean

 <b>THREAT</b>	A tropical storm has strengthened into a hurricane and may hit a resort in Puerto Vallarta, Mexico. Monitoring of the projected path of the storm is required. A crisis management plan is in place and triggers activities such as purchasing materials for board-up, testing emergency radios and generators, collecting cots, gathering food supplies, etc. Resort employees are trained, and there is effective communication throughout the resort. Resources have been adequately allocated.
 <b>WARNING</b>	The storm has now built hurricane-strength winds and turns toward the east, headed for central Mexico. The occurrence is imminent, with the storm's outer bands being felt within a 200-mile radius of Mexico's Pacific Coast. Activities include boarding up buildings, removing outdoor property, and beginning evacuation of non-essential personnel.
 <b>EVENT</b>	The hurricane has struck land. The objectives are to protect human life, maintain communications, and continue to manage emergency priorities.
 <b>IMPACT</b>	Plans are executed for the continued protection of life and property, the most essential activities during this phase. Activities would also include cleaning up, restoring the premises, restoring operations, reporting insurance claims, securing funding for recovery, and maintaining a positive public image.

Section 4: Crisis and Disaster Planning

Overall, it is important to know the potential impacts of a crisis and where a crisis may originate from. Understanding this and how a crisis progresses allows risk managers to create and implement plans to mitigate a crisis’s impact on an organization.

▶▶ Knowledge Check



**Directions:** Respond to the following prompt.

Consider current events and provide an example of a crisis or disaster. Identify its source, and fill out the chart identifying the phases of the crisis.

Name of Event:	
Source of Crisis:	
Phases of Crisis	
Threat:	
Warning:	
Event:	
Impact:	

# Crisis Management, Business Continuity, and Disaster Recovery

## Learning Objective:

4.2 Describe the terms crisis management, business continuity, and disaster recovery, and explain the relationship between the three terms.

A crisis management plan is a response to crises that would negatively impact the business's ability to operate or damage its reputation. A business continuity plan (BCP) outlines how a company will continue should an unplanned occurrence take place. It acts as a prevention and recovery system for potential threats or disruptions. Disaster recovery implements elements of both the crisis management plan and the business continuity plan. The three form a road map for the organization's response to crises or disasters.

## Crisis Management

Crisis management is the act or process of managing a crisis to prevent a catastrophic loss, if possible, and reduce the impact of catastrophic losses on the organization, including its reputation and brand.

## Business Continuity

Business continuity refers to the ability of an organization to perform critical operational tasks during and following a disruptive event. A business continuity plan outlines a range of disaster scenarios and the steps the business will take to return to regular operations. These plans describe how a company will recover its operations or relocate them in the event of damage caused by natural disasters, a terrorist attack, or other unforeseen disasters. Any event that could negatively impact operations should be included in the plan, such as supply chain interruption, loss of or damage to critical buildings, equipment, or systems, etc. Plans and procedures are developed to ensure that mission-critical organizational operations continue during disruptive events.



To implement a business continuity plan, an organization may consider using a business continuity management system (BCMS). The purpose of a BCMS is to prepare for, provide, and maintain controls and capabilities for managing an organization's overall ability to continue to operate during disruptions. The business continuity management system combines interrelated methods, procedures, and resources to keep critical business processes running.

## Section 4: Crisis and Disaster Planning

If the BCMS complies with ISO 22301, then it will also have an internal and external audit component that supports the ongoing operation, review, and continuous development of business continuity. Overall, the primary purpose of a BCP is to provide the organization with strategies and information to maintain continuity of operations during and after a disaster.

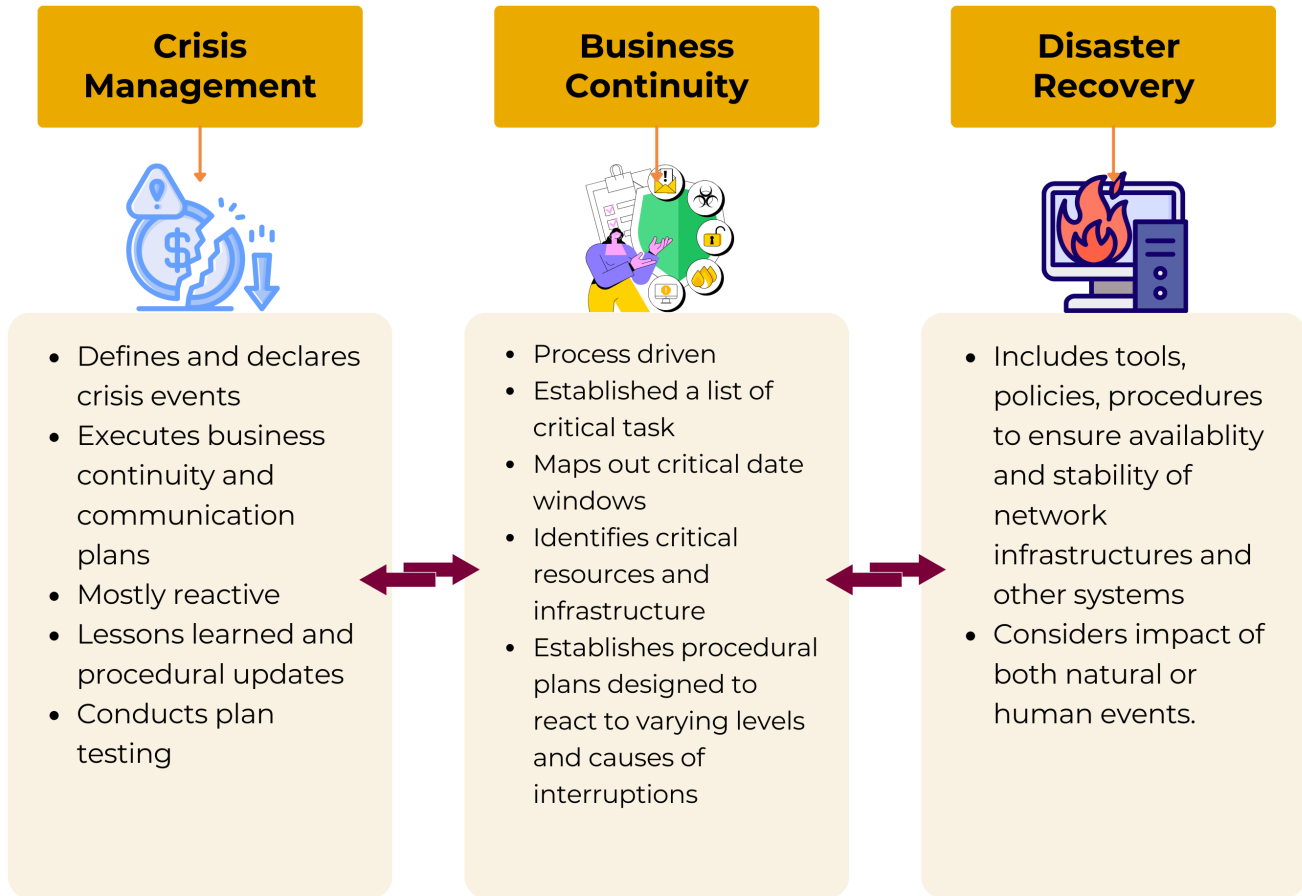


### Disaster Recovery

Disaster recovery involves maintaining the consistency and performance of vital resources, technology, and infrastructure during and after a disruptive event and returning to regular operations. Recovery is a combination of policies, procedures, and restoring functions critical to the organization's resumption of ordinary business activities after a disaster occurs (after "impact"). An organization can take several sub-steps in the recovery process from a disaster or crisis. These include, but are not limited to:

- Initiate any mutual aid agreements with vendors, customers or clients, and competitors.
- Secure the site, control access, and prevent subsequent damage or injury.
- Document damages.
- If operations are to resume at existing premises, ensure the safety of returning persons.
- Initiate salvage efforts.
- Review recovery needs and timelines for each affected department, facility, or location.
- Resume limited operations to meet customer and client needs.
- Implement special accounting procedures.
- Initiate employee support programs.
- Initiate communications with the public to preserve reputation, image, and brand.

## Section 4: Crisis and Disaster Planning



An organization's ability to effectively respond to a crisis requires a reciprocal relationship between crisis management, business continuity, and disaster recovery activities and teams. All three should be considered when developing an organization's crisis management plan.

From a global perspective, effective crisis management includes both business continuity planning and disaster recovery planning.

## Knowledge Check



**Directions:** Answer the questions below.

Consider the recent COVID-19 pandemic.

1. Did your organization have a plan in place that responded to the crisis?

---

---

2. What steps were taken to ensure business continuity and enhance recovery?

---

---

3. What changes were made to the plan in terms of responding to future events?

---

---



# Crisis Management Goals and Principles

## Learning Objectives:

- 4.3 Describe the principles of an effective crisis management program, including general crisis management goals.

## Principles of Effective Crisis Management

When establishing crisis management plan goals, it is essential first to consider certain principles to produce an effective crisis management program. Overall, there are five main principles:

### 1. Comprehensive

The crisis management plan should consider all hazards, all phases, all stakeholders, and all impacts relevant to a disaster.

### 2. Progressive

Crisis management plans should anticipate future disasters and formulate preventive and preparatory measures to build disaster-resistant plans and operations.

### 3. Risk-Driven

Sound risk management principles should be employed to assign priorities and resources. This includes hazard identification, risk analysis, and impact analysis.

### 4. Integrated

Crisis management should ensure a unity of effort among all levels of the enterprise and all involved customers, suppliers, government authorities, and the community.

### 5. Collaborative

The crisis management planning process should create and sustain broad and sincere relationships among individuals and organizations that encourage trust, advocate a team environment, build consensus, and facilitate communication.

By adhering to these principles and establishing clear crisis management goals, the crisis management program becomes more effective in ensuring organizational stability during a disaster scenario, ultimately safeguarding the organization's profitability and bottom line.



## Creating Crisis Management Goals

Just as risk management or risk control programs have goals and/or objectives, crisis management plans must have goals. Some goals are pre-loss objectives, and others are post-loss objectives. Both types are generally established by the organization's management or governmental bodies.

General pre-loss goals address the economy of operations (operating at the most favorable or effective costs), legality of operations, and humanitarian activities to maintain a positive public image. One important pre-loss goal for the risk manager is to obtain senior management's full support and commitment to the crisis management program, just as senior management has completely endorsed the risk management goals and/or objectives.



Post-loss goals include restoring and/or maintaining operations, sustaining profits and stable earnings, working towards growth, and maintaining a positive public image. Goals will have different weights or priorities with management and will compete for scarce organizational resources along with all other investment opportunities. The goal of crisis management is to effectively and economically minimize the operational and financial impact of the crisis. The following table provides some examples of goals throughout the various stages of a crisis.

Pre-Loss Goals	Goals During a Crisis	Post-Loss Goals
Establish a robust crisis management plan for the organization.	Prioritize the protection of human life as the utmost goal during the crisis.	Activate the business continuity plan to restore or maintain critical operations.
Create and implement training on the crisis plan and effective communication strategies throughout the organization.	Establish and uphold protocols to maintain communication and coordination during a crisis.	Proactively manage and maintain a positive public image after a crisis.
Optimize resource allocation to ensure sufficient support and implementation of the crisis management plan.	Maintain fiscal responsibility and minimize unnecessary expenditures during a crisis.	Execute a strategy to sustain profits and stabilize earnings after a crisis.
Conduct rigorous testing and validation procedures to ensure the effectiveness and reliability of the crisis management plan.		Conduct a review of the crisis management plan post-loss and implement necessary improvements.

## Section 4: Crisis and Disaster Planning



Establishing goals for a crisis management plan is crucial. Well-defined goals provide a sense of direction that ensures an organization has allocated its resources properly when preparing for a crisis. Furthermore, goals can serve as a benchmark that can be used to refine and improve the crisis management plan after a loss has occurred.

### ▶▶ Knowledge Check



**Directions:** Respond to the following prompts.

You are a leading consultant for a crisis management firm. One of your clients is a municipal government agency preparing a crisis management plan that responds to a chemical or bioweapon attack.

1. Provide an example of a pre-loss goal, a goal during the crisis, and a post-loss goal for the crisis management plan.

---

---

---

---

2. Describe one principle the crisis management plan should follow, and explain why that principle is important in this context.

---

---

---

---

# Crisis Management

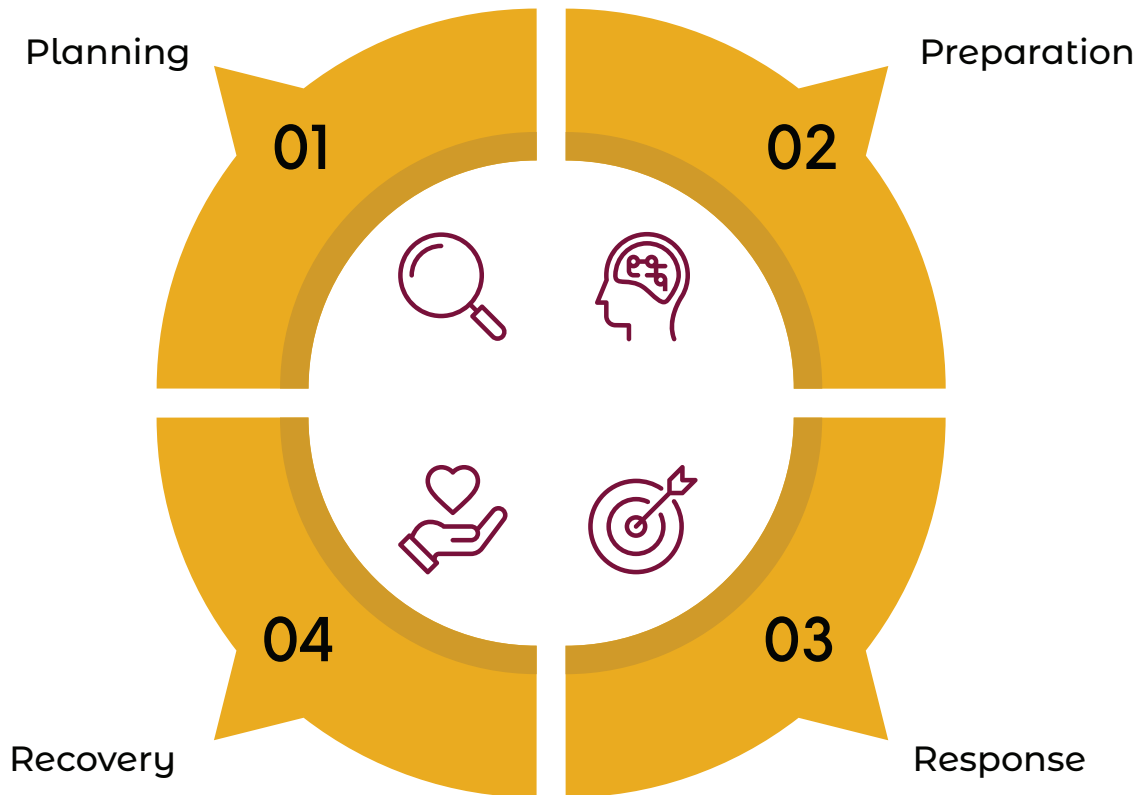
## Learning Objective:

4.4 Explain the four essential steps of the crisis management process.

Managing a crisis begins long before an actual event occurs. Having a plan in place and being prepared can help minimize property damage, prevent injury, and save lives. A crisis plan must be customized to the individual organization—each has its own needs, goals, resources, and definition of what constitutes a crisis.

The actual crisis management process consists of four essential steps:

### Crisis Management Process



## Planning—the First and Most Important Step

“Failure to plan on your part does not constitute a crisis on my part.”

—Anonymous

Crisis management planning involves a proactive and systematic approach aimed at preparing organizations to navigate and mitigate unexpected and high-impact events effectively. To produce an effective crisis management protocol, the planning phase should include the following steps:

1. Establish the crisis management team.
2. Identify potential disasters or crises.
3. Conduct a vulnerability and impact analysis.
4. Identify and prioritize mission-critical business needs.
5. Identify asset requirements.
6. Coordinate communication.
7. Develop the crisis management plan.
8. Write, distribute, and implement the plan.
9. Test, evaluate, and update the plan.



### 1. Establish the crisis management team.



Crisis management is too monumental a process to be successfully handled by any one individual. First, a one-person “team” likely lacks the cross-organization, multiple-level vision to truly comprehend what happens at all levels of the organization during a crisis. Second, the individual is not likely to secure cross-organization and multiple-level buy-in to coordinate activities in a climate of uncertainty, chaos, and disruption. Third, few individuals have detailed knowledge of all the important activities an organization undertakes on a

day-to-day basis. A crisis management team is essential to establishing an effective crisis management program.

The crisis management planning team must have an effective coordinator or team leader. While expertise is always desirable, leadership and communication skills, along with the appropriate level of authority, are more important to generate actions and create buy-in from the organization. The team will develop the plan as a committee composed of representatives from across the organization’s various operational and managerial levels. This multi-level structuring engenders upper management support and



## Section 4: Crisis and Disaster Planning

garners the details of operations from line managers, supervisors, and employees. Participation by line employees is essential, as these employees are the potential members of an immediate response team, the ones who know how to shut down equipment and secure property, and ultimately are the ones who must implement evacuation and the myriad other details needed to protect persons and property.

The members of the planning team need to have expertise in operations and how operations can be adequately protected or recovered. They need the individual authority to obtain missing information required to formulate a plan, as well as the requisite level of group authority to represent their organizational interests. Depending upon the situation, a crisis will require other special skills, such as effectively communicating with the media or public authorities and officials. Last, all team members must have leadership skills to inspire others to cooperate with the plan creation effort and execution.

The planning team must determine the structure of the crisis management team, which can be flexible, depending upon the organization's structure, except with respect to the crisis communication system. The crisis communication system is best served by a wheel structure.

In this communication structure, a single individual (or position) acts as a central hub for communication. They are responsible for outgoing external communications, as well as disseminating information to the various members of the organization. All members of the organization should be connected to the leader but may not necessarily be structurally related to one another. Ultimately, only one officially designated spokesperson should receive and provide information from the team to authorities, media, and stakeholders.

The planning team must also define authority within the group. One critical authority is that of the designated spokesperson—the only authority for official communications. Similarly, one person must have the authority to initiate the crisis management plan. A defined chain of command and commensurate authorities at appropriate levels are critical to having an effective crisis management plan. Imagine the chaos on a cruise ship if a dining room steward had the authority to issue an “Abandon ship!” order.

Lastly, the planning team should establish a schedule and a budget to track progress and justify the costs and benefits to senior management. The schedule and budget include the crisis management plan's training requirements and exercises (test runs).



## 2. Identify potential crises and disasters.



The planning team must identify potential disasters or crises by examining those previously experienced by the organization and evaluating past responses. The team needs to consider the proximity of the organization's facilities to risk factors and infrastructure resources such as highways, railways, rivers, power plants, military bases, earthquake zones, tornado zones, flood plains, and hazardous activities such as nuclear power generators and chemical plants.

The team also needs to review the vulnerability of the organization's key vendors and clients by asking, "What happens if a disaster strikes their operations?" and "How does their disaster affect our operations?"

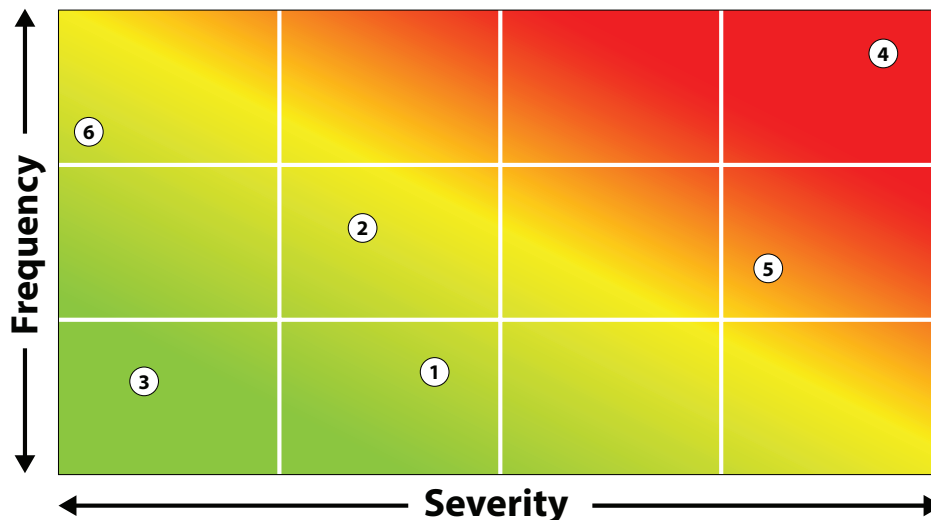
## 3. Conduct a vulnerability and/or impact analysis.

Once the team is established, their first order of business will be to conduct a vulnerability and impact assessment to determine the organization's vulnerability to all reasonably foreseeable disasters and/or crises. This is best accomplished by a brainstorming activity, an exercise in which there are no "wrong" responses. The team must be encouraged to consider all possible disasters or crises, regardless of the likelihood of occurrence. Once the team has identified many possible disasters, the disasters are ranked.



One way of ranking the disasters/crises is by using a heat map. Heat mapping is a visual representation of complex sets of data interpretations that use colors to indicate patterns or groupings of how risk will impact an organization. Values are assigned for each risk based on measurement scales for both severity and frequency. The more severe a risk is thought to be, or the more often it is expected to occur, will determine the number assigned. The higher the assigned number, the greater the impact or likelihood of an event. Each risk is plotted on the map based on the assigned value, which assists an organization with risk prioritization.

### Heat Map Risk Matrix



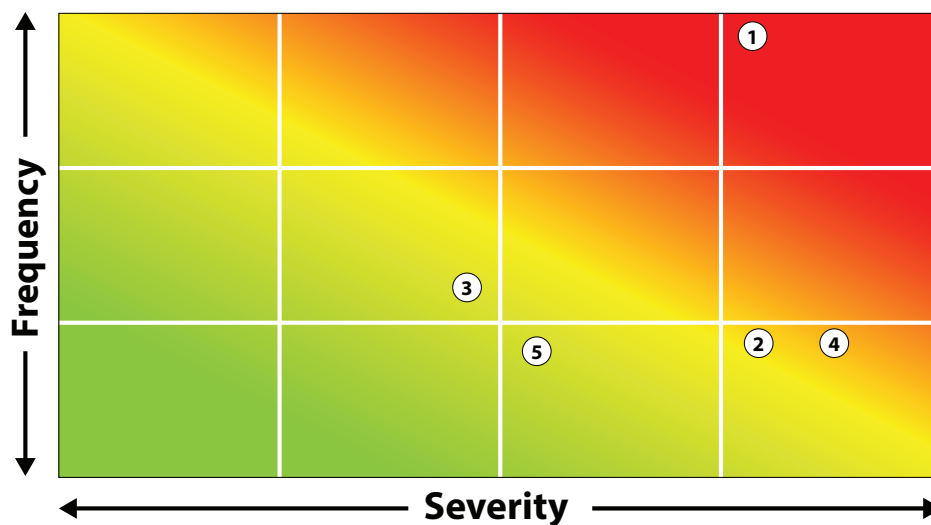
## Check-In



**Directions:** Respond to the following prompt.

You are part of a crisis management team conducting a vulnerability/impact analysis for an oil refinery located on the coast of the Gulf of Mexico. Brainstorm at least five disasters that could reasonably impact your organization. Classify each potential disaster based on likelihood and impact using the heat map below. You are allowed to make assumptions but be prepared to explain those assumptions.

### Heat Map Risk Matrix



1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_



#### 4. Identify and prioritize mission-critical business needs.



While considering the listed disasters or crises, the team should identify products, services, and operations critical to the organization. Aspects of these include equipment and personnel issues, utilities (including telecommunication capabilities), products and services provided internally and/or externally, and employee, vendor, and customer contact lists.

After the team accumulates this vast array of information, it must then prioritize the activities. The objective is to establish an optimum “return to operations” (RTO) for mission-critical operations. It means initiating those activities that are essential, moving to enact those that are important, and, if funds and personnel are available, arranging for those activities that are desirable. Where appropriate, mutual aid agreements, reciprocal agreements, and/or “standby contracts” for shared office space, technology, or other infrastructure resources may be considered to reduce the economic impact of the crisis.

#### 5. Assess and review internal and external resources.

As the disasters or crises are ranked, the team must assess the organization’s current situation and capabilities. This sub-step requires reviewing internal resources in the form of the risk management plan, insurance programs, contracts, employee handbooks, hazardous materials (“hazmat”) plans, safety manuals, security procedures, environmental policies, fire protection plans, and evacuation plans. The insurance review must include identification of coverage, conditions, exclusions, applicable limits, and deductibles/retentions.



Organizations should get involvement from each vendor identified as providing a critical business need and make them a part of the planning and response activities. The team should also identify contractors and vendors that may provide pre-loss and post-loss resources. The internal resource review includes identifying key personnel from each operational unit, backup personnel and services, and the availability of warning, response, and recovery equipment such as fire suppression, communication, and transportation.



The team must also identify external resources. Some services are provided by governmental agencies such as the Federal Emergency Management Agency (FEMA), state and local disaster planning and response organizations, law enforcement agencies, and fire departments.

Other services are provided by vendors such as utility companies, information technology service suppliers, and other types of vendors. Insurance brokers or carriers may also provide engineering resources for pre-loss actions and claims handling resources for post-loss activities. Customers, clients, and even competitors may also offer external resources (e.g., reciprocal arrangements for office or manufacturing space). Lastly, the team must assess the capabilities of hospitals and emergency clinics, first responders like paramedic and EMT services, and the American Red Cross and Salvation Army.

## Section 4: Crisis and Disaster Planning



Organizations may need to engage external resources well before a crisis event, depending on the nature of the operation or location of the facility. Establishing partnerships with these groups and how their response will mesh into the organization's crisis management plan is essential, and some of these groups can also provide pre-loss resources. For example:

FEMA provides planning and training for active shooter situations.

The U.S. Department of Transportation and various state motor vehicle departments provide HAZMAT training for drivers.

The U.S. Environmental Protection Agency provides guidance and training for hazardous spill containment.

Links to these resources are available on the "Resources" webpage for this course.

### 6. Identify asset requirements.

Part of the resource assessment process requires the team to identify the funds needed and potential sources to contact when the crisis management plan is triggered. Also, the team must identify necessary supplies, such as water, food, first-aid and first-response items, generators and fuel, and protective equipment—as mundane as ordinary gloves, boots, goggles, hard hats, and coats, or as exotic as hazmat suits.



Further, the team must determine if emergency materials such as sandbags, braces, plywood, pumps, and blocks are required and, if so, the amount needed. Related to the material resources is the issue of where the physical resources are stored (on-site or remotely) and how such resources will be retrieved when needed. The team should also consider the availability of alternative premises from which the crisis management team and/or the entire business can operate.

### 7. Coordinate communication.



Internal communication systems revolve around notification and training. The natural changes in seasons (or quarterly) can be appropriate times to remind employees of evacuation procedures and schedule dates for training drills. Employees need to know the method of notification, when they will be notified, and who will notify them. The notification plan must accommodate employees with physical disabilities, as well as those who work in environments where the standard notification devices will not be adequate (e.g., using a horn or siren in a noisy work setting where employees must wear protective gear like headphones). Further, if visitors are permitted on the premises, the notification plan must

address knowing when non-employees are present, where they are located, and how they will be notified and accounted for. The notification process also provides an opportunity to

show that the organization cares about the safety and well-being of the employees by addressing home disaster safety tips.

External communication systems can be divided into two types: communication with the public and communication with the media. Proactive crisis management involves informing the public what they can and cannot expect from the organization during a disaster. This includes providing information on alternative premises that would be occupied in the event of a disaster. Communication with the media begins well before any disaster by establishing positive media relations. A positive relationship with the media is an invaluable asset during times of crisis for organizations facing strikes, terrorist threats, or allegations of sexual harassment for age, race, and sex discrimination. Further, service organizations may use the media to disseminate general disaster safety advice as a public service.

### 8. Develop the crisis management plan.

After determining communication protocols, the planning team will have taken all the other necessary steps to develop the crisis management plan. For each identified impact, the team must determine the strategic plan for that impact, the emergency response procedures specific to that impact, the mitigation plan, the recovery plan, and all necessary support documentation.

During this process of creating the impact-related elements of the plan, the team needs to consider the likely obstacles, such as:

- Financial constraints
- Organizational resistance
- Informational gaps
- The “fog of war” factor, the natural haziness during a period of uncertainty
- Communication difficulties
- Unexpected events that cloud a crisis during its impact and shortly after its occurrence



The team must prioritize the impacts of the contemplated activities (e.g., the scarce or limited resources needed by ordinary operations may become even more scarce or limited during the crisis period) and allocate resources according to their priority in pursuing the pre-loss and post-loss goals.

After prioritizing the activities, the team must write and test the draft plan. It is then reviewed, and the results are analyzed.

The draft is revised, and a final plan is written to include an executive summary for those who are not expected to read the entire crisis management plan (such as primarily

## Section 4: Crisis and Disaster Planning

stakeholders who are outsiders). The plan is then distributed to a broader audience within the organization to seek feedback and organizational buy-in. It is important to note that a plan should be in place for each identified crisis. Based on the type of risk, risk level, and risk impact, organizations should prepare for all potential disasters with:

- A strategic plan
- Emergency response procedures
- A mitigation plan
- A recovery plan
- Any needed supporting documentation

### 9. Test the plan.



After the plan is distributed and feedback is received and reviewed, it is ready to be tested. Testing can occur at several levels, with the least disruptive to the organization being a tabletop exercise described as follows. A crisis simulation is introduced in a conference room setting, and the plan is implemented as a talk-through exercise. Obvious flaws and weaknesses are noted for future consideration and revision.

A more intense level of testing can be performed using simulations in which the mock disaster is staged in a more realistic setting than a conference room, and the crisis management plan is executed and tested. The testing can occur with respect to specific functions rather than on

an organization-wide basis and may include evacuation drills, either specific to a function, department, or facility, or on a wider scope.

The last step in testing should be a full-scale drill. Full-scale drills involve the entire organization in a more realistic simulation. These simulations may also include external resources who participate in the testing with respect to their necessary response, such as having a fire department, local, state, or federal disaster agencies, the American Red Cross or Salvation Army, or other outside organizations respond in a training exercise. In some cases, a mock media session may also be conducted. To establish the method and frequency of drills and tests, the crisis management team should determine the following:

- Who is responsible for conducting testing of the plan?
- How often will tests take place?
- What scenarios will be the focus of the test?
- Which business groups will participate and to what extent?



## Section 4: Crisis and Disaster Planning



Once the plan has been thoroughly tested and appropriately modified, the crisis management plan is integrated into company operations. Like any risk management plan, integration is facilitated using senior management endorsement and encouragement, proper communication, effective orientation and training, and emphasis on the benefits to the organization and its personnel, property, vendors, customers, and, ultimately, the bottom line.

Since organizations change over time, any crisis management plan must be continuously evaluated and updated, with at least a semi-annual review and a formal annual audit. Also, if a catastrophic event occurs, a post-event review is essential, as that event has provided an opportunity to observe the strengths and weaknesses of the initial plan.

The Sago Mine disaster mentioned earlier in this text, is a good example of the importance of a post-event review. The mine had a disaster plan with warning devices to detect explosive gases, blast curtains, emergency rations, oxygen supplies, and evacuation plans. The investigation after the accident indicated that rescue equipment was inadequate and faulty, and communication in the mine was impossible. Perhaps the most tragic aspect of this event was the initial press conference inadvertently leaked preliminary and overly optimistic information indicating that 12 of the 13 missing miners were safe and being rescued when, in actuality, all twelve reported as alive were already dead, and the one reportedly dead miner was alive. In a post-event review, these issues would be analyzed, and corrective actions implemented to strengthen the plan.



To summarize, crisis planning is crucial for organizations to handle unexpected challenges effectively while maintaining public trust. The planning phase involves identifying potential crisis scenarios, establishing clear communication protocols and response teams, conducting regular training, and developing strategies for external communication and cooperation with stakeholders and authorities. Go to this course's "Resources" webpage at [riskeducation.org/RCresources](http://riskeducation.org/RCresources) to view samples of a disaster plan and a disaster checklist.

### Step Two—Preparation

The crisis management team should have identified each peril or crisis during the planning stage. Preparation, the second step, requires the team to generate countermeasures for both loss prevention and loss reduction. The following steps can be used to guide this process:

#### 1. Establish emergency response and evacuation procedures.

Since protecting life is a prime goal and consideration, evacuation routes and procedures should be implemented if this has not already been done. These should also include procedures



for evacuating any guests or vendors on the premises and those with disabilities. Current procedures and routes should be reviewed to confirm continued viability, as official evacuation routes may have changed.

### 2. Implement prevention and control measures.

Prevention and control measures should be implemented for each specific expected peril (e.g., fire, earthquake). These would include both pre-loss and post-loss control measures. These include a maintenance or safety program to prevent or mitigate potential perils and hazards. Regular inspections of all facilities provide information on needed maintenance and identify safety issues.

### 3. Review and obtain continued power for critical operations.

Continued power for critical operations should be reviewed and obtained if not already in place. The organization may need a backup power source in case of emergency. The equipment, facilities, and operations it will cover/service should be decided. Once the backup is put in place, it should be tested. Sufficient fuel for utilizing alternative power sources (based on anticipated downtime) should be obtained and safely stored. The organization's power needs should be re-evaluated at least annually and whenever there is a significant change in operations.

### 4. Work with outside emergency response organizations to reduce response times.



In preparation for an event, the risk manager should work with outside emergency response organizations to reduce response time delays and ensure the safety of premises and people. For example, the location of shut-off valves and standpipes should be clearly indicated for fire and hazmat responders. The organization's crisis management and disaster recovery plans should be shared with these entities to ensure proper coordination of efforts, as well as the workability of the plan in various types of crises.

### 5. Create agreements for backup resources.

Depending on the nature of the organization, arrangements should be made for backup supplies, facilities, and possibly personnel. Contracting in advance with a disaster recovery provider may be the easiest way to accomplish this. Many organizations enter into mutual aid agreements to support limited continued operations.

### 6. Evaluate and establish emergency funding.

Proactively planning for funding and expenses following a disaster is another critical step. The team should make their best estimates of funding needs and ensure those funds are readily available in an emergency. Note that if a disaster strikes a wide area, banks may not be open, the internet may be down, and the usual way of acquiring funds may not be available. Pre-authorized requisitions and purchase orders for supplies can be valuable. Although not a widespread practice, having a good amount of cash available may be necessary.



### 7. Provide training on emergency procedures.

This is the time for employee training on the plan and emergency procedures, particularly evacuation, use of emergency equipment, the locations of outposts or temporary office locations, communication protocols, and securing the physical premises when a warning has been issued.

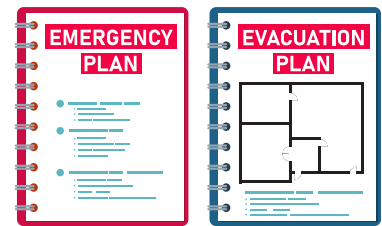
### 8. Store and protect critical information.

All critical information and important records should be safeguarded and backed up. Where are the backups stored? If in the cloud, who will have access? If the organization uses a physical server, it should also have a backup process—perhaps a replicating server in another location not prone to the same disasters.

In summary, the preparation step includes these essential components: communication, education, evacuation, identification, inspections, procedures, purchasing, safeguarding, and training.

## Building the Crisis Management Kit

Building the crisis management kit requires a planning exercise consisting of pre-loss planning for several activities that must take place at the warning and impact stages. A crisis management “kit” is not just an accumulation of equipment or gear. Rather, it is an assembly of diverse information, instructions, plans, and physical materials. Contents of the kit should include:



- Lists of team members, structured organizationally, and their backup members, as well as a list of non-employees (e.g., authorities, customers or clients, vendors) to be notified. The list should include phone numbers (both landline and cell phone numbers) and email addresses to accommodate communication via cellular devices.
- Lists of emergency contact information: landline and cell phone numbers and e-mail addresses of emergency services, such as police, fire, medical, and disaster agencies
- An aerial photograph of each site and the geocode for its location, using latitude and longitude in a geographic information system (GIS). Although one would think emergency responders could find a street address, the confusion and chaos of a disaster can change everything (e.g., a tornado or hurricane obliterates street signs and landmarks). The use of technology reduces the potential for error. Further, the emergency responders would be aware of impediments on routes to a disaster location and can use the GIS data to calculate response times or alternative routes.
- Maps and directions for travel to and between locations and evacuation routes and alternative routes, including locations of assembly areas for those at the facilities and the location of on-site and off-site shelters. Information regarding the



communications outpost must be provided in the event telecommunication systems are disabled.

- Detailed emergency procedures, including essential shutdown procedures for employees not familiar with the normal operations in the event the trained employees are unable to safely close and secure systems.
- Master keys and access codes to secured locations if the employees with access to these items are unavailable.
- Physical equipment, ranging from the extreme of hazmat gear to more mundane gear like radios, walkie-talkies, flashlights, cameras, and money.

### Step Three—Response



Life safety comes first in any response. Protecting the lives of employees and non-employees takes precedence over all other activities. Besides the moral issue inherent in safeguarding human life, public outrage and media condemnation following any response that protected property before life (even if no lives were lost) can seriously damage an organization's reputation and profitability.

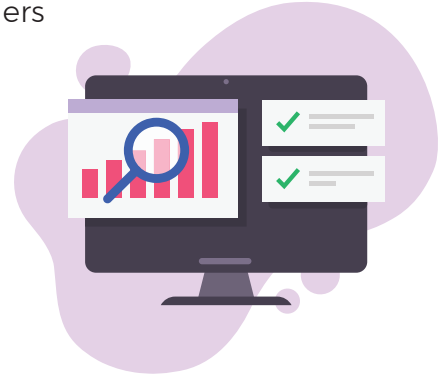
Once the crisis management plan is triggered, the type of response is determined. All response plans should include the following standard requirements. Note that these are not in order of priority.

- The appropriate number of alternative/temporary premises for communication must be established and staffed with personnel. Basic access controls must be considered, as well as potential backup sites.
- Outposts must be well stocked with all necessary supplies. Monitoring expiration dates on supplies and restocking procedures must be in place. An inventory of supplies should be maintained.
- The communication plans must be well-practiced and in place to be effective. Communication efforts must be initiated with both internal and external stakeholders.
- Damage assessment must be conducted before any recovery efforts can begin because the nature and extent of the damage will determine the priorities of the recovery phase. The review includes documentation of details, site access and status of utilities, the taking of photos and videos, and documentation of damages and losses.



## Section 4: Crisis and Disaster Planning

- Coordination efforts must be initiated with first responders and local, state, and federal agencies.
- Financial expenditures must be made as needed and documented, with the need for additional resources evaluated. A separate accounting code should be used for crisis-related expenditures, including all employee time utilized for clean-up, security, repair, etc.
- Employee and family considerations such as notification and assistance must be initiated. Support efforts are initiated.
- Media time must be scheduled. Initiate communications with the public to preserve reputation, image, and brand.
- Insurance partners (carriers, agents/brokers, and claims staff) should be notified and utilized.



After the active phase of the crisis is over, efforts should be centered on restoring operations and ordinary business activities while maintaining profits and public image.

### Step Four—Recovery



Recovery is a combination of policies, procedures, and restoring operations critical to the organization's resumption of ordinary business activities after a disaster occurs (after "impact"). An organization can take several sub-steps in the recovery process for a given disaster or crisis; however, the following five overall steps should be undertaken first, as these will apply in almost every situation:

1. Follow the hierarchy of priorities developed during the planning process.
2. Coordinate all activities as stated in the plan.
3. Identify and provide for essential personnel.
4. Ensure that personnel and the chain of command are in place.
5. Establish communications with insurance and/or recovery partners, customers/clients, vendors, and employees.

## Section 4: Crisis and Disaster Planning

Depending on the crisis or disaster, the crisis management team will take other specific sub-steps as appropriate. Possible sub-steps may include:

1. Initiate any mutual aid agreements with vendors, customers or clients, and competitors.
2. Secure the site, control access, and prevent subsequent damage, loss, or injury. Protect the site and property from further damage. Initiate salvage efforts, preserve any undamaged property, and determine if there is any functionality or alternative use for damaged property. Be sure to coordinate with insurers to establish the extent of the damage.
3. If operations are to resume at existing premises, ensure the safety of returning personnel and other workers.
4. Review recovery needs and timelines for each affected department, facility, or location.
5. Resume limited operations to meet customer and client needs.
6. Review and revise the plan for future events.

Remember, crisis management is a continuous process. An organization should evaluate and update its plan continuously. The plan may change based on experience, industry research, or changes in operations and personnel.

## ▶▶ Knowledge Check



**Directions:** Read the scenarios below and respond to the prompts.



XYZ Electronics is a leading data storage company known for its innovative products, exceptional customer service, and, most importantly, its proven track record of keeping personally identifying information (PII) and other sensitive information secure. You are part of a team developing a crisis management plan for XYZ Electronics. Identify the first two steps of the crisis management process. List at least one example of an action that XYZ Electronics should take during those steps.

Step One: _____	<b>Actions during step one:</b>
Step Two: _____	<b>Actions during step two:</b>



XYZ Electronics has encountered a severe security breach, and it is found that a third party has accessed the sensitive information of over five million individuals. In some cases, this information included Social Security numbers and payment information. Identify the next two steps of the crisis management process and explain at least one example of an action that XYZ Electronics should take during each step.

Step Three: _____	<b>Actions during step three:</b>
Step Four: _____	<b>Actions during step four:</b>

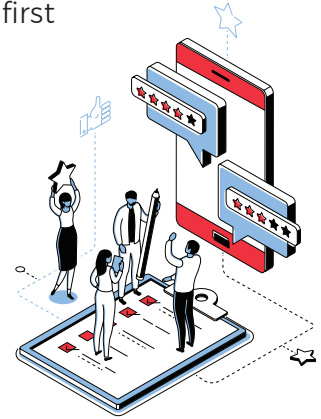
# Reputation Management During a Crisis

## Learning Objective:

4.5 Describe the important considerations of reputation management during a crisis.

In order to manage its reputation during a crisis, an organization must first know how it is perceived by the public. Market research activities help assess public perception of the organization and its brands and image. Even among organizations enjoying a strongly favorable public perception and a high level of public trust, astute management will take pre-crisis actions to bolster the “trust piggy bank” to prepare for that rainy day of adverse circumstances that might tarnish an otherwise spotless perception.

Once a loss occurs, post-loss crisis communication is a critical tool for managing public perception and protecting the organization's reputation. Four important goals of crisis communication are:



<b>Goal 1</b>	Quickly and accurately address any issue that has the potential to threaten the organization's reputation.
<b>Goal 2</b>	Establish a network of internal and external advocates who will work on the organization's behalf in managing perception and reputation.
<b>Goal 3</b>	Prevent an issue from escalating into a crisis.
<b>Goal 4</b>	Minimize the long-term adverse impact of a crisis.

Managing a company's reputation during a crisis is crucial as it directly impacts public perception, trust, and loyalty among customers, investors, and other stakeholders. To successfully protect an organization's reputation during a crisis, there are several considerations risk managers should be aware of:

## Reputation is a Key Corporate Asset

### IMPORTANT CONSIDERATIONS FOR MAINTAINING REPUTATION DURING A CRISIS

*"If you lose money for the firm by a bad decision, I will be understanding.  
If you lose reputation for the firm, I will be ruthless." – Warren Buffet*



Reputation is a crucial asset for any organization. A strong reputation influences consumer choices, investor decisions, and partnerships, ultimately driving business success. As a result, reputation management is strategic and must be proactive and ongoing. The organization is concerned with reputation, public image, goodwill, market share, and maintaining or growing those areas. This is often challenging because an organization does not wholly own or control its reputation.



In today's social and economic climate, perception is everything. The use of the internet for communications—both positive and adverse—allows the rapid spread of information, which is difficult to respond to and often impossible to control. Proactively monitoring communications, posts, media services, and the like is essential to “taking the temperature” of public perception and responding accordingly.

## Reputation Management Has Specific Goals.

A primary goal of reputation management should be to eliminate misinformation and negative publicity by quickly and accurately addressing any issue that can potentially threaten an organization's reputation. Some additional goals could include:

- Build a network of advocates.
- Establish sound relationships with the media.
- Prevent an issue from escalating into a crisis.
- Minimize the long-term impacts of a crisis.
- Show that an event is an anomaly—not a usual occurrence.



By building a network of internal and external advocates and establishing sound relationships with the media in advance, the risk manager has a more likely opportunity to prevent an issue from escalating to a crisis and may even minimize the long-term adverse impact of a crisis.

When appropriate, the organization should attempt to disassociate itself from the event and show it as an anomaly and not indicative of the organization.

## The Initial 24-Hour Period



The initial 24-hour period is a critical time in the reputation management process. The organization's management only has 24 critical hours to quickly gather the information, confirm its accuracy, and tell the story. Letting issues linger without being addressed, even when the facts are unknown or uncertain, appears to be an attempt to cloud the issue, conceal facts, or shift blame. Regular and continuous communication is

better than permitting one-sided speculation, even if no additional information is confirmed or available.

How the organization acts and responds in the first 24 hours of a crisis sets the tone for the narrative that follows. The management of an organization under the dark cloud of a crisis must show true leadership by allowing actions to speak louder than words. Bluster, evasion, denial, and empty reassurance ring hollow when the truth becomes known. The “truth”—real or otherwise—will become known, thanks to a chaotic media circus and the reliance many “truth seekers” have on blogs, social media, and other media-sharing mechanisms.



Communication in the first 24 hours of a crisis should focus on the organization's crisis story. This consists of having a single spokesperson for the organization telling the facts as they are and as they unfold. The truth should be told without exaggeration or speculation.

After that first 24 hours, the second day is the time for communicating the response. By the second day, more of the facts will be known, and the initial “fog of war” or confusion during

rapidly breaking news and shattered or disrupted systems will have cleared enough for management to understand and report the full extent of the crisis.

The second day will be the time to monitor the news media, including the informal news network that many use to disseminate the facts—real or otherwise—via blogs, social media, and internet-shared video and audio messages. It is the time to communicate widely and consistently, telling the official story.

### Crisis Communication Requires Discipline

The speaker must maintain credibility and control the dialogue. If the speaker cannot create an aura of trust and credibility, the listeners, particularly the media, will scrutinize every aspect of the message and sensationalize the real story. Press conferences can quickly disintegrate into media-feeding frenzies. A strong communicator must maintain control to tell a consistent and accurate account rather than creating the story the media wants to hear.



Employees and customers are important advocates in the communication process. However, those individuals must be guided (and possibly coached) to tell the truth and to follow the same rules all speakers must follow. Lastly, communication exists to tell the story, not to speculate, discuss blame, or shift responsibility. Communication should be centered on providing the factual information that an organization has available during a crisis.

### Telling The Story—Message Delivery



How the story is told is as important as the facts of the story itself. As a witness swears in court, it is important to tell “The Truth, the Whole Truth, and Nothing but the Truth.”

The speaker must tell the plain and unvarnished truth. In the chaos and uncertainty of a crisis, some facts may be forgotten, or a misspeaking may occur. The public, consisting of ordinary people, each of whom have forgotten important things in their

everyday lives, will be forgiving of forgetfulness or an accidental misstatement, especially when corrected immediately. However, a lie requires intent, and most people will be more reluctant to forgive a deliberate act such as a lie.

The media may investigate forgetfulness as a deliberate lie, but there is no real story behind a truthful and convincing “I forgot” after the initial flurry of accusations claiming cover-ups and obfuscation. However, trust is broken once a lie is revealed, and a search intensifies to uncover other untruths.

The speaker must also demonstrate empathy toward others affected by the organization’s crisis. These affected parties might be employees and their families, customers, clients, vendors, or the public. A “let them eat cake” attitude does not endear the speaker or the organization to the listeners. For example:



## Section 4: Crisis and Disaster Planning



In 2010, British Petroleum's Deepwater Horizon oil rig malfunctioned, resulting in the largest marine oil spill in history. The incident devastated both marine ecology and local economies in the Gulf of Mexico. The CEO made several insensitive comments, stating that the oil spill was "tiny in relation to the total water volume" and that he would "like my life back." Given the fact that 11 employees lost their lives in the explosion and the livelihoods of many others along the Gulf Coast were threatened, the damage was done. He would have been well-advised to empathize with all concerned from the outset.

The focus of the truth-telling should be first on the facts but with emphasis on the measures the organization is taking to protect lives and mitigate damage.

Consider an example:



Carrefour is a chain of grocery stores that operates in Brazil. In 2020, on the eve of Brazil's national holiday for awareness of the black community, a black man was beaten to death by security guards contracted by Carrefour, resulting in a wave of protests against the stores. The chain immediately terminated its contract with the security company and fired employees involved in the incident. It swiftly complied with criminal investigations into the conduct of the individual security guards, and ultimately, the CEO issued the following statement:

"Internal measures have immediately been implemented by Carrefour Brazil, notably towards the security company involved. These measures do not go far enough. My values and the values of Carrefour do not allow for racism and violence."

By reacting swiftly and clearly outlining its response, Carrefour was able to control the damage to its own reputation as well as mitigate the potential for future violent events to occur at its stores.

### Answering the Tough Question

Truth and facts are not nearly as interesting as lies and fiction. Answering the tough question is always easier when the speaker focuses on the truth and known facts. Consider an example.



In 2002, Donald Rumsfeld served as the U.S. Secretary of Defense. During a press briefing, he was asked about reports indicating a lack of evidence showing that Saddam Hussein was providing terrorist groups with weapons of mass destruction, Rumsfeld stated the following:

"Reports that say something hasn't happened are always interesting to me because, as we know, there are known knowns: there are things we know we know. We also know there are known unknowns: that is to say, we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."



## Section 4: Crisis and Disaster Planning

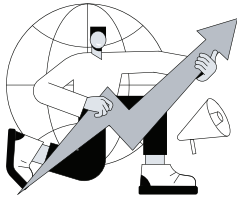
Since Rumsfeld was serving as a spokesperson for the United States, critics viewed this statement as an attempt to dismiss the lack of justification for military action against Saddam Hussein in the early 2000s. Although Rumsfeld later wrote a book titled, *Known and Unknown: A Memoir*, and an explanation of his use of this enigmatic language is found in an author's note, his reply to the question clearly illustrates what can happen when organizational spokespersons stray from the known facts when speaking with the media. When responding to tough questions, being avoidant or perceived as avoidant can quickly damage an organization's or an individual's reputation. When responding to these questions, there are four critical elements a spokesperson should include in their response:



1. **Acknowledge responsibility.** This is not the same as blaming oneself or the organization; rather, it might take the form of simply saying, "There was an explosion in our plant today, and employees were severely injured. This is all we know at this time."
2. **Control the agenda.** This is easier done in a press release than in a press conference. However, a press release tends to increase speculation because it does not allow the media to ask questions (even if they will not be answered in detail).
3. **Enforce message discipline.** The most crucial factor in message discipline is restricting communication to one and only one individual. The organization's crisis management and crisis communication systems must make it clear to all other individuals that they are not authorized to speak on behalf of the organization and that all questions must be directed to the designated official. Even "off the record" remarks will reappear in print. The designated individual must maintain personal message discipline and not allow repeated questioning or personal emotions to cause them to deviate from the official message.
4. **Respond proportionately to the crisis.** A complete media lockdown is not appropriate for a largely internal crisis, just as a one-line press statement regarding the complete destruction of a major facility is not appropriate. The authorized speaker must address media speculation appropriately, with "those are the facts as we know at this time," or "we do not have that information available right now," and not with abusive remarks, threats, or worse, "no comment."



## Restoring a Damaged Reputation



Because proactive reputation management is strategic and ongoing, there is really no distinction between building a reputation with customers and stakeholders before or after a crisis. Trust is an essential component of a successful business relationship, and continuing to act sincerely and substantively, even amid uncertainty, chaos, and confusion, is the primary path to maintaining a positive reputation, as well as recovering a reputation that has been adversely affected by events.

Within the context of a crisis communication plan, management must take several specific steps to recover a damaged or imperiled reputation, the most important one being that the organization must accept responsibility for its role in the crisis. Management must also help those immediately impacted because it is humanitarian—the right thing to do. Management must take long-term corrective action to assist in the recovery and to prevent future harm. The organization must also address any systemic problems and resolve those promptly to start rebuilding the relationship with all stakeholders.



These actions are most effective when the organization's management communicates its intentions and actions openly and transparently. When confidence is shaken, a public relations campaign may be warranted to help restore a level of confidence in the organization, its management, and its brand. Public relations initiatives solicit support from other organizations within the same industry or region. To maintain relations with the general community, individuals from the organization can participate in forums, such as speakers' bureaus, or provide public service announcements.

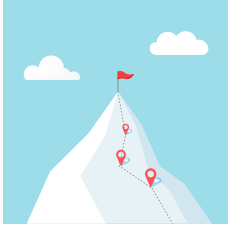
To prepare for the future while recovering from a tarnished reputation or a catastrophic event, the organization can establish a media outreach program to create a positive image with the existing media and new media contacts. Educating the customer aids in developing and maintaining a positive reputation, as does an advertising or marketing campaign focusing on organizational responsibility and capabilities. Last, the organization should implement a government affairs program to establish a positive relationship with applicable levels of government, particularly those who assist during a crisis.



## Knowledge Check



**Directions:** Respond to the following prompts.



You are the risk manager of Ricky Mountain Experiences, a survival-type outdoor climbing and trekking tour operator with an international clientele. During a recent tour, several high-profile clients died from exposure during a three-day blizzard when the guide's radio failed, and he could not call for help. Media coverage was widespread. You know that how an organization responds in the first 24 hours of a crisis sets the tone for the narrative.

A. Provide three considerations when responding to a crisis.

---

---

---

B. Message delivery is also critical following a crisis. Provide two guidelines for message delivery.

---

---

---

## Summary

Overall, the foundation of crisis management lies in the ability of the crisis management team to identify potential vulnerabilities. Once these are identified, a strategic planning matrix should be created to guide an organization's response through a crisis.

A critical component of an effective crisis management team is cross-functionality. The crisis team should be composed of individuals from different areas of the organization so that a complete understanding of an organization's potential crises can be established. Crisis management also relies on effective delegation, so roles, responsibilities, and authority should be established for managing a crisis or disaster.

With a team in place, a crisis management process should be developed. This will include drafting likely scenario plans, which should be tested, implemented, and revised as needed. A communication plan and system with an identified spokesperson is also essential, as it allows an organization to control its messaging and protect its reputation.

Crises continuously evolve, so organizations should monitor issues proactively and regularly. Annual training and disaster/crisis simulations should also be conducted to ensure that individuals in the organization understand the plan and know what actions they should take. After a crisis or disaster occurs, participants should be debriefed, and an organization should learn from its efforts and update the crisis management plan using the knowledge it learned during the actual crisis.

# Practical Exercise

## Learning Objective:

4.6 Use the principles of crisis management to respond to a hypothetical crisis scenario.

## Background and Instructions

A risk manager for a large resort hotel chain is working with her organization to develop a comprehensive crisis management plan. In preparation for its completion and implementation, she has decided to perform a tabletop exercise to test the plan and make necessary modifications before it is finalized. She has requested your participation and has provided the following information:

### Method

The tabletop exercise will simulate a crisis situation in an informal, stress-free environment.

The assessment is designed to elicit discussion between you and your fellow participants as you examine and resolve problems based on existing plans, procedures, and knowledge of the organization. This assessment is scenario-driven and should focus on the roles and responsibilities of every crisis management team member.



### Facilitator

Your faculty member will be the facilitator. The facilitator will provide scenario updates, moderate the discussions, provide additional information, and resolve questions as needed.

### Crisis Management Team Members

You will respond to the scenario presented based on knowledge of the crisis management process and your personal experience and acquired knowledge.

### Assumptions

The scenarios will require several broad assumptions. During this exercise, assume the following:

- The scenario could occur.
- Events occur as they are presented.
- There are no hidden agendas or trick questions.
- All participants receive identical information at the same time.

### Exercise Rules

There is no single or “correct” solution. Each scenario is different, and each team will uniquely respond to the facts. Everyone is encouraged to contribute and ask questions. Remember, there are no “stupid questions” in a “what-if” exercise. Varying viewpoints and even disagreements are expected and encouraged. Silence indicates agreement.

Respond to the scenarios based on your knowledge of crisis management plans and capabilities.

### Suggestions

Treat the scenarios as actual events. Participate openly. Asking questions and sharing thoughts is strongly encouraged and will enhance the exercise experience. Issues arising from the scenarios will be thoroughly discussed.

As you review the stages, consider what actions are appropriate based on your knowledge and experience and the information provided by the facilitator. Keep the objectives in mind throughout this tabletop exercise.

### Stage 1 Narrative

A hotel chain’s corporate office has recently relocated to North Carolina’s Atlantic Coast. The building is a modern, four-story structure providing an open view of the ocean vistas and the company President’s yacht in the marina below. All the company’s corporate office operations are housed in the facility, including the executive offices, computer services, human resources, reservations, finance, and accounting. The company’s information technology (IT) services are provided by a set of servers located in a fire-protected and secure room on the top floor of the corporate headquarters. The servers store all the company’s accounting and finance transactions, internal corporate communications, and reservation records for the various resorts. All the company employee email service is processed through an email server, which is included in the server stack. Even though the IT department’s regular operating hours are from 8:00 AM to 5:00 PM, Monday through Friday, the reservations server can be accessed remotely at any time from any of the company’s resort facilities.



On Saturday afternoon, September 6 (two days before Labor Day), the National Weather Service issues a hurricane advisory for much of the Atlantic Coast due to a minor Level 1 storm churning in the ocean north of Puerto Rico. The various weather computer models are unclear as to the projected path of the storm, so the National Weather Service issues a watch to cover the entire “cone of impact” provided by the various models. They believe the storm could hit land anywhere from Melbourne, FL, to Norfolk, VA, in the next

72 hours. The company President is out of town, visiting the company's facilities in Cancun, Mexico.

## Stage 1 Questions

- A. You are the head of the company's Emergency Response Team (ERT). Given the above information, what are your first steps after seeing the weather service announcement on the television?

1st priority? \_\_\_\_\_

2nd priority? \_\_\_\_\_

3rd priority? \_\_\_\_\_

Who will you contact? \_\_\_\_\_

How will you communicate with them? \_\_\_\_\_

What will your instructions be? \_\_\_\_\_

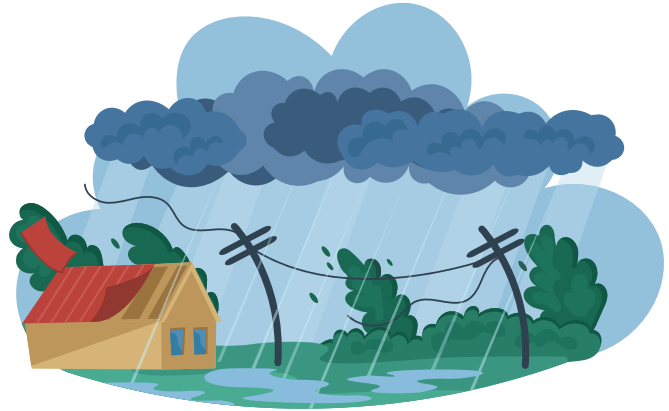
- B. You are the IT Manager and have just been contacted by the head of the Emergency Response Team (ERT).

What will be your first steps? \_\_\_\_\_

Who will you contact and why? \_\_\_\_\_

## Stage 2 Narrative

At 8:30 AM, Monday morning, the Labor Day holiday, the National Weather Service issues a hurricane warning for the North Carolina coastal area. Overnight, Hurricane Kelly has grown rapidly into a Level 3 storm and has established a path that will move onshore approximately 20 miles south of the company's corporate headquarters. It is expected to reach Level 4 before landfall at approximately 2:00 PM.



Based on the projected path and severity of the storm, Carolina Power has announced that they will shut down the power grid in the projected impact area at noon. The city fire department has issued a mandatory evacuation order effective at 10:00 AM for all buildings and residences within 15 miles of the coast.

## Stage 2 Questions

- A. You are the head of the company's Emergency Response Team (ERT). Given the information above, what will be your first steps?

1st priority? \_\_\_\_\_

2nd priority? \_\_\_\_\_

3rd priority? \_\_\_\_\_

Who will you contact? \_\_\_\_\_

How will you communicate with them? \_\_\_\_\_

What will your instructions be? \_\_\_\_\_

- B. You are the hotel chain's risk manager.

Who will you contact? \_\_\_\_\_

How will you communicate with them? \_\_\_\_\_

What will your instructions be? \_\_\_\_\_



## Stage 3 Narrative

On Tuesday morning, the storm has passed, leaving extensive damage in its wake. The corporate office sustained moderate wind damage to the glass exterior, primarily on the ocean side of the building. The roof sustained some damage but is doing a reasonably good job protecting the offices on the top floor. The basement area of the corporate office has approximately two feet of water, but critical equipment for the operation of the building is either located three feet above the floor or on the upper floors. The only property damaged in the basement appears to be accounting records from previous years.



Carolina Power has reported extensive power outages with a projected recovery of three weeks for the areas closest to the coast. Virtually all cell and landline phone services are down in an area up to 35 miles inland from the Atlantic Coast.

## Stage 3 Questions

You are the head of the Emergency Response Team. Your home has also sustained substantial damage, as have the homes of many of your coworkers at corporate headquarters.

What is your 1st priority? \_\_\_\_\_

What is your 2nd priority? \_\_\_\_\_

What is your 3rd priority? \_\_\_\_\_

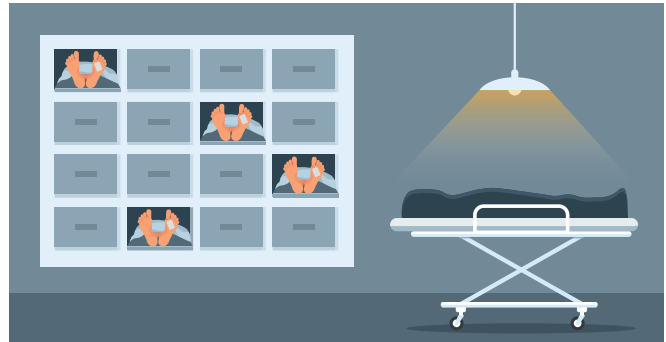
Who will you contact? \_\_\_\_\_

How will you communicate with them? \_\_\_\_\_

What will your instructions be? \_\_\_\_\_

## Stage 4 Narrative

During the clean-up of the corporate offices, a body is discovered in the building's basement. The body's identity is unknown, and it appears the victim drowned. Law enforcement authorities have arrived, and the county medical examiner has alerted the media, who has descended upon the corporate office in large numbers, complete with television feeds and news helicopters. Reporters are attempting to enter the premises and are clamoring for statements.



The company President has seen this news from his hotel room in Cancun and has called Mary, the risk manager, with instructions to “Get this circus under control NOW!”

## Stage 4 Questions

You are the risk manager. What actions would you take to preserve your organization's reputation? \_\_\_\_\_

---

---

---

---

---

## Section 4 Self-Quiz

**Directions:** Answer the questions below.

- Which of the following is the best example of a crisis?
  - ☐ A company's CEO plans to resign in a few months due to personal issues.
  - ☐ An organization launches a product line that returns less profit than anticipated.
  - ☐ A cyber-attack compromises sensitive customer data stored on a server.
  - ☐ A department within a company undergoes routine restructuring.
- A crisis management team has identified several potential crises that could impact their organization. Match the crises described in the right-hand column to their source in the left.

<b>A.</b> Industrial disaster	_____ Intentional industrial sabotage by a disgruntled employee
<b>B.</b> Infrastructure disaster	_____ A systems failure at the main plant leading to chemical spillage
<b>C.</b> Human hazard	_____ A breakdown of the primary railway the company uses to ship its chemical precursors
<b>D.</b> Natural hazards	_____ Severe blizzards that impact operations at the central manufacturing plant

**Directions:** Use the word bank to complete the sentences below.

<b>threat</b>	<b>warning</b>	<b>event</b>	<b>impact</b>
---------------	----------------	--------------	---------------

- A hurricane's predicted path is altered by meteorologists. The storm is expected to make landfall and impact a company's operations by 4:00 PM. This is an example of a(n) \_\_\_\_\_.
- Gunfire is suddenly heard in a hospital. The hospital is sent into a lockdown, and emergency services are contacted. This is an example of a(n) \_\_\_\_\_.
- A concert venue receives an anonymous email stating that an intentional bombing will occur on the premises in the coming weeks. This is an example of a(n) \_\_\_\_\_.
- After a severe security and malware breach, a company must spend weeks conducting tests to ensure the security of its systems. This is an example of a(n) \_\_\_\_\_.

## Section 4: Crisis and Disaster Planning

7. Which of the following statements defines a business continuity plan (BCP) correctly?
- ☐ The BCP outlines how a business will continue critical operations during a crisis.
  - ☐ The BCP establishes the team that defines and declares crisis events.
  - ☐ The BCP details the marketing and outreach tactics used to restore lost reputation.
  - ☐ The BCP creates a process by which key executives can be replaced after a crisis.
8. The crisis management team of a coastal real estate firm has started to plan for the increasing occurrences of severe weather and flooding. Which principle of crisis management does this decision demonstrate?
- ☐ Risk-driven
  - ☐ Integrated
  - ☐ Progressive
  - ☐ Collaborative
9. Which of the following goals is the highest priority during a crisis?
- ☐ Protecting business property
  - ☐ Protecting human life
  - ☐ Keeping media communication open
  - ☐ Preserving company reputation
10. How should communication be coordinated during a crisis?
- ☐ External communication should be bottom-up during a crisis, for example, from a factory floor worker to the top tier of management.
  - ☐ Communication should cease during a crisis. Due to the “fog of war,” transmission is unreliable and can cause issues.
  - ☐ Communication should remain flexible, and any individual in the organization should participate in that communication.
  - ☐ A central spokesperson should be identified. All internal or external information should go through this individual.
11. Why would a crisis management team use a heat map risk matrix?
- ☐ To track the geographical spread of a crisis and its impact on different regions
  - ☐ To visually identify the likelihood and severity of the impact of potential crises
  - ☐ To visualize the expected financial cost of preparing for a crisis
  - ☐ To assess the overall financial losses following a major crisis

## Section 4: Crisis and Disaster Planning

12. A hospital on the Gulf Coast has a large intensive critical care unit with many patients on life support. Which of the following would be an important consideration for the hospital during the preparation phase of crisis management?
- ☐ Has a crisis management plan been created?
  - ☐ Has the crisis management team conducted a vulnerability assessment?
  - ☐ Is a backup power source needed and available?
  - ☐ Have insurance claims been filed?
13. An organization initiates a mutual aid agreement with its competitor to use facilities. These types of agreements would be activated during the \_\_\_\_\_ phase.
- ☐ planning
  - ☐ preparation
  - ☐ response
  - ☐ recovery
14. A company owns a large apartment condominium. The apartment building collapses, leaving 11 individuals dead and hundreds of others displaced. Which of the following steps should the company take to manage its reputation during the crisis? **(Select all that apply).**
- ☐ Empathize with the individuals and families directly impacted by the crisis.
  - ☐ Provide potential speculative reasons as to why the collapse occurred.
  - ☐ Explain the steps it is taking for its recovery efforts during the crisis.
  - ☐ Avoid any public questioning and provide no comment to any journalistic inquiries.
15. A large chemical fire at a factory has taken the lives of at least two workers and injured dozens. Which of the following actions should the factory management avoid?
- ☐ Acknowledging the event occurred
  - ☐ Allowing middle management to provide their own statements on the event
  - ☐ Ensuring that all reported statements are truthful and accurate
  - ☐ Providing direct assistance to affected workers and their families

# Set Yourself Up for Success!

## Visit the “Resources” Webpage at [RiskEducation.org/RCresources](https://RiskEducation.org/RCresources)

For valuable reinforcement, be sure to visit the “Resources” webpage. This webpage contains a variety of materials that will help you absorb the course material *and* set you up for success on the Final Exam. You’ll find:

### Study Guide

Download a copy of the Study Guide. It contains all the Check-In questions, Knowledge Checks, and Self-Quizzes contained in this Learning Guide in a format that makes it easy for you to practice and check your answers.

### Flash Cards

Play an interactive vocabulary game with a study set of digital flashcards to enhance your learning of the insurance and risk management terms used in this course.

### Review Game

Use a fun, trivia-style review game to test your knowledge and prepare for the Final Exam.

### Video Clips

View a video clip about an important concept related to one of the learning objectives in this section.



Crisis Management

### Downloadable Document

Review ISO 22301—Business Continuity.

## In Addition...

### Appendix

The Appendix of this Learning Guide contains a Glossary of terms as well as tips for study techniques and sample test questions that will help you prepare for the Final Exam.

# Section 5: Claims Management

---

## Section Goal

In this section, you will learn about one of the risk manager's key responsibilities—the process of managing claims. In addition, alternative dispute resolution (ADR) will be discussed as an alternative to litigation. Finally, the considerations that should be made when selecting a third-party claims administrator and defense counsel will be reviewed.

## Learning Objectives:

- 5.1 *Describe claims management and how it supports the risk control program.*
- 5.2 *Describe the actions and considerations for the investigation phase of the claims management process.*
- 5.3 *Explain the evaluation step of the claims management process, including how damages and reserves can be calculated and set.*
- 5.4 *Discuss the resolution step of the claims management process, including the four types of alternative dispute resolution (ADR) methods.*
- 5.5 *Analyze the three types of claims management plans and the considerations that should be made when selecting a plan.*
- 5.6 *Describe the components, requirements, and possible findings of a claims audit.*
- 5.7 *Explain the role of a third-party administrator (TPA) and the major considerations of the selection process.*
- 5.8 *Explain the considerations when selecting defense counsel for an organization.*

In the broader risk management process, the first key step is to identify loss exposures or risks. Once a risk or exposure is identified, it is analyzed, controlled, financed, and administered. As an essential part of risk control, claims management follows this same format. During this process, the claims manager should:



1. Identify the facts of the claim.
2. Conduct an analysis of the potential liability.
3. Undertake actions to minimize or reduce the financial impact of the claim. (Since the loss was not avoided or prevented, the only remaining option is to reduce it.)
4. Identify financial obligations and resources.
5. Resolve the claim and report the results.

Before discussing the specific steps of the claims management process in detail, it is essential to understand what claims management can accomplish and how it supports an organization's risk control program.

# Defining Claims Management

## Learning Objective:

5.1 Describe claims management and how it supports the risk control program.



Claims management is the **prompt resolution** of an organization's **losses subject to insurance or an active retention program**, including **claims** by **other individuals or entities** to which it may be **legally bound** or **ethically responsible**.

Several key points in this definition need to be discussed in greater detail.

## "Prompt"

The goal of claims management is to resolve claims matters promptly and at the optimal cost. Unlike fine wines and violins, claims do not get better with age. Like fine wines and violins, however, they do increase in value with age. For example, medical costs associated with injuries increase dramatically each year, and the longer an individual is out of work, the less likely they will return. In each of these instances, the cost of the claim increases the longer it remains unresolved.





## “Resolution”

Resolution is the process of bringing claims to a conclusion using denial of responsibility, negotiation, alternative dispute resolution techniques, litigation, subrogation, or salvage disposition.



## “Losses”



Losses result in reduced asset values and, ultimately, shareholder value. Losses can occur on a first-party basis, affecting only the organization itself. Losses may also be third-party in nature and arise from an organization’s legal or moral liability to an employee or third party.

## “Subject to insurance or an active retention program”

Except in the case of non-insurance contractual transfers where the responsibility for an exposure is transferred to a third party outside the organization’s direct control, all an organization’s losses or claims will be financed externally (through insurance) or internally (preferably through an active retention program).

While an insurance company is responsible for managing insured claims, its goal will always be to protect the insurance company’s assets before those of the insured entity.

However, claims can impact an organization’s future premiums, deductibles and retentions, limits, and underwriting acceptability. Consequently, the risk manager must still monitor the management of insured claims to ensure they are resolved in a way that is favorable to the organization.

Actively retained losses must be handled by the organization or by outsiders. In either case, the risk manager must manage those losses, even if the processing is outsourced to an insurance carrier, law firm, or third-party claims administrator. Passively retained losses must still be brought to their conclusion using the same resolution techniques as other claims and will be managed in the same manner as actively retained losses.

## “Claims”



Just as a distinction is made between incidents, accidents, and losses, there is a difference between a loss and a claim. A claim is a demand or obligation for payment or performance to another party (an employee or a third party) who is alleging a breach of common law or statutory/contractual duty. A claim against the insured does not become a loss to the insured unless and until the insured’s assets are reduced by payment or legal expense.

## “Other persons or entities”

The “other person” may be an employee working in the course and scope of employment, or a “third party”—an outside or unrelated person or organization such as a corporation, limited liability company, partnership, or governmental/regulatory entity.

## “Legally or ethically bound”



The organization may be legally obligated to another party because of common law (usually regarding a negligent act), statutory liability, or contractual liability. An organization may also make a voluntary payment based on moral or ethical obligations, usually called an *ex gratia* payment, to compensate the injured party without legal fault or responsibility.

*Ex gratia* payments can be used to resolve issues in which there may be a question of liability, to maintain customer relations, or to protect the organization’s reputation.

## The Role of Claims Management in Supporting the Risk Management Process

The risk manager’s role in claims management is to take actions to minimize or reduce the financial impact of claims on an organization. Risk managers can accomplish this through claims management in several ways.

### Gathering Data

A large part of the claims management function is related to gathering data. The risk or claims manager will collect incident/accident reports, identify and analyze contractual obligations, verify loss or claim amounts, and conduct appropriate investigations to determine liability. Gathering claims data allows the risk manager to identify trends and frequent types of losses the organization has experienced in the past. This ultimately helps prioritize risk control efforts to assist in reducing losses.

### Enforcing Contractual Obligations

Related to the data gathering aspect of identifying and analyzing contractual obligations is the enforcement of those contractual obligations. A hold harmless or indemnification provision or additional insured status is meaningless if no one requires the responsible party to perform. Enforcing these obligations can protect an organization’s assets. Consider a scenario:



## Section 5: Claims Management



Blue Bird Construction is the general contractor on a custom new home build project. Blue Bird requires their subcontractors to indemnify them for any claims of damages arising out of their work. Al's Plumbing is running the plumbing lines for the house. One of Al's employees starts a fire when welding piping, causing significant damage to the house. The owner sues Blue Bird, but Blue Bird's risk manager knows that Al's has signed an indemnification agreement for their work and makes a formal demand that Al's take over the defense and payment of the claim. By enforcing the contract, the risk manager has controlled and possibly eliminated the claim.

### Mitigating Damage

During a claim and after a loss, the claims management process serves to reduce or mitigate damages. Some mitigation actions reduce the dollar amount of damages paid out, while others attempt to restore asset value by recovering amounts from responsible parties through subrogation or salvage. For example:



During a severe thunderstorm, a tree crashes through the roof of Wildon's Supermarket, causing water damage to the interior fixtures and products. To prevent further damage to the interior, Wildon's hires a contractor to remove the tree, shore up the roof trusses, and temporarily cover the hole. In this way, the property and premises are protected.

### Promoting an Equitable Resolution

The claims manager must work to find a satisfactory solution for the claimant and the insurance carrier. Frequently, a negotiated settlement will not result in the highest or lowest payment amount to the claimant but will provide both parties with a fair and equitable result.

### Reducing Fraud

Claims fraud can exist internally, externally, or systemically. Internal fraud is perpetrated by persons inside the organization (e.g., embezzlement). External fraud is conducted by individuals outside the organization (e.g., a hacker who gains access to the pricing matrix and reduces pricing on an item to obtain it for a lower price). Systemic fraud arises out of organizational failures or inadequate organizational governance. An example of systematic claims fraud could be an adjuster stealing from a carrier by making checks payable to an accomplice and coding them to a claim file. This would be an indication of inadequate controls on check issuance.



### Loss Forecasting

Claims management is involved with setting reserves based on the initial report of the incident and the flow of information that follows. Losses may be trended to account for the effect of inflation and developed to account for the natural increase in the dollar value (or the number of losses) that occurs over time using triangulation. This information may be used to predict or forecast losses into future periods.

### Advising and Consulting

Claims management may advise or consult with other departments within the organization. Loss control, legal, operations, administration, sales, product development, and human resources may benefit from the information provided by the claims management function. For example:



The claims manager may receive a claim for operations that are not covered by the insurance policy and not revealed in the insurance application. The claims manager will alert the underwriter of this exposure so that a decision can be made regarding adjustments needed to obtain coverage for those operations.

Overall, claims management is an important aspect of risk control. Proper management of claims will reduce overall loss costs. Any money not spent on the payment of claims will enhance the organization's bottom line, thereby reducing the organization's total cost of risk.

## Knowledge Check



**Directions:** Answer the questions below.

1. Explain how enforcing the contractual obligations of others supports claims management and risk control.

---

---

---

---

2. XYZTech is an IT company. During a project with a long-term client, XYZTech experiences some disruptions that may have resulted in a small financial loss to the client. How might an *ex gratia* payment to the client benefit XYZTech?

---

---

---

---

# The Claims Management Process

Having explored the reasons for claims management, the types of claims management, and who might perform the claims management, it is time to discuss the process of claims management. The three key steps of the claims management process are **investigation**, **evaluation**, and **resolution**.

## Investigation

### Learning Objective:

5.2 Describe the actions and considerations for the investigation phase of the claims management process.

The claims management process begins with a report of an event, whether an incident, accident, occurrence, claim, or loss.

### Reporting



As mentioned, investigations begin with a report. While every person in the organization is responsible for reporting the events that come to their knowledge, every report should be directed to one person in the organization who will be the point of contact for reporting. Considering the organization's defined claims management philosophy, this person will determine whether the event is "reportable." This person may be the risk manager or a designated person (DP) in the organization.

An organization that is highly proactive in loss prevention will be far more interested in incidents than accidents because preventing an incident that could lead to an accident helps control claims frequency.

Thus, employees should be trained to report every incident to the DP immediately. The DP then forwards the incident information to the risk manager, safety manager, or loss control manager for further action.

Information about accidents reported to the DP must be forwarded to the insurance adjuster, third-party administrator, or internal claims administrator immediately and, if required, to the appropriate regulatory body (e.g., workers compensation authority, OSHA) within the reporting timeframe.

If the DP's first notice of an accident is the service of a summons and/or complaint, the DP must deliver that notice to the risk manager, insurance adjuster, administrator, or defense counsel without delay. If the DP learns of a catastrophe or crisis, or a potential catastrophe or crisis (e.g., flood or storm warnings, fire), the crisis management team leader must be



notified immediately, in addition to the risk manager, insurance adjuster, or third-party administrator.

### Gathering Information



Prompt and thorough investigation is critical, as the information gathered will shape the response, the evaluation, and the resolution. This information should include such factors as weather, physical conditions, official reports, and even media reports. Witnesses must be identified, contacted, and statements taken quickly, as memories fade over time or are altered by subsequent exposure to the “facts” reported by others. Additionally, investigators must promptly and carefully collect and preserve any physical evidence.

Outside support may be used to aid in the investigation. Appraisers, engineers, accountants, and other experts provide a specialized focus and an independent eye for the investigation. A claims history or record of previous claims involving the same individual(s) or circumstances should be procured. The principal goal of any investigation is to uncover the facts that may impact the decision related to liability and damages.

However, an investigation that collects only outcome-oriented details undermines the goals of insurance and retention programs. The questions the investigators must ask are uniform regardless of the type of investigation. What happened? Who was involved? Where did it happen? When? How? Why? These questions are simple but lay the foundation for a complete and accurate investigation.

Another question that should be asked is, “What else?” or “What else could have happened?” The answers may give rise to possible defenses to litigation, such as the assumption of risk, contributory or comparative negligence, the existence of a hold harmless or indemnification agreement, or defective work or product of another potentially responsible party.



## Section 5: Claims Management



Imagine an individual being struck by a foul ball at a baseball game. The injured party may claim that someone should be held responsible for their damages. However, further investigation reveals that this is a classic example of the assumption of risk. The injured party was (or should have been) aware of the possibility of being hit when attending a ball game. Courts have typically held that there is no liability on the part of the batter, the team, or the ballpark for this type of injury.

### Documentation



Throughout the investigation and during evaluation, the claim is documented. The claims service provider should have a protocol in place for determining what gets reported, by whom, and when. There are cost-benefit issues in the reporting process. Ideally, every iota of information should be reported, as each detail might have predictive or defensive value later. However, the cost of capturing, reporting, recording, and maintaining minutia is high. The value of more specific data must be balanced against its cost of capture and maintenance.

Related to this issue is the question of who benefits from the reported information. Some information that is captured may be used against the organization or the insurance carrier. This issue is humorously illustrated with the following:

- The documents in the claim file should be considered to have the title “Dear Ladies and Gentlemen of the Jury” emblazoned with a rubber stamp on every page. Whatever is in a claim file is discoverable in a court of law, and documents placed before a jury are often enlarged to be the size of a poster, with the damaging comment, typed or a hand-written note, prominently highlighted.
- Another person observed that the “e” in e-mail and e-data actually stands for “evidence” or “eternal.”



## ▶▶ Knowledge Check



**Directions:** Answer the question below.

As risk manager for Uno's Fine Foods, you are advised that multiple cases of food poisoning have been sustained by a group of young students attending an awards banquet in one of your restaurants. What steps would you take during the investigation phase of the claims management process?

---

---

---

---

---

---

## Evaluation

### Learning Objective:

*5.3 Explain the evaluation step of the claims management process, including how damages and reserves can be calculated and set.*

Once the investigation is ongoing, and information is being gathered and documented, the claims service provider must evaluate the claim. First, the investigator must identify if any insurance policy, including any policies purchased by other potentially responsible parties, provides coverage for the defense or damages. Next, the investigator should attempt to determine if the organization is potentially liable for the claimant or injured party's damages. Related to that is the question of damages, or what amount of money will justly compensate the claimant for injury or loss.



### Coverage



Coverage must in be place for a value to be placed on a claim. As part of the evaluation, an organization should identify available insurance coverages and notify all potential insurers. Insurers will then send notification of any coverage issues. Early in the investigation, especially if there is any doubt whether an insurance policy provides coverage, the insurance carrier's adjuster or a claims representative will analyze the insurance policies to determine coverage. This evaluation or analysis is familiarly known as a "DICE" analysis, an acronym taken from the first letters of the four sections of the policy that will be analyzed in depth:

- The Declarations (the who, when, where, and how much) of the policy,
- The insuring agreement (the how or what),
- The conditions (the requirements for coverage to be made available),
- And the exclusions.

From this investigation, coverage issues may arise that must be resolved. The two initial activities the adjuster or claims representative will consider are a **reservation of rights letter** and a **non-waiver agreement**. Both are used when the investigation indicates that there may be a question of coverage.

To fully understand how these documents are used, it is important to understand two legal concepts: waivers and estoppels. These two words are often used together as if they are a necessary pair. However, they are two separate concepts. A waiver is a voluntary relinquishment of a known right. In the context of a claim, the insurance carrier may, through its actions and communications, give the insured the impression that the claim is covered, only to find out that coverage is lacking. The insured has relied on the carrier's actions to his detriment and will argue that the carrier has waived the right to deny coverage.



Estoppel is a legal concept that keeps someone from asserting or denying something in court that contradicts what has already been established as the truth for one of several reasons, or it is a legal doctrine that prevents the re-litigation of facts or issues previously resolved in court.

A reservation of rights letter is used as a tool to avoid the repercussions of estoppel or waiver arguments. The letter states that the insurance carrier believes there are issues regarding whether the insurance policy provides coverage for the type of claim made against the insured or submitted by the insured. The letter identifies explicitly and states all policy provisions that determine whether coverage for the claim exists. It also specifically states that the insurance carrier does not waive its right to deny the claim following its subsequent investigation. By stating this



## Section 5: Claims Management

up-front, the reservation of rights letter attempts to avoid arguments that may force the insurance carrier to be responsible for an otherwise uncovered claim.



For example, a policyholder submits a claim for an automobile accident. The adjuster reviews the Declarations and finds that the vehicle involved in the accident was not listed on the policy.

The adjuster will issue a reservation of rights letter that states the reason for the coverage issue, all applicable policy provisions, and “we reserve the right to deny coverage pending the results of our investigation.” If the letter is not sent, an insured might argue that the actions of the insurance carrier to accept and investigate the claim report are a voluntary relinquishment of their rights under the policy (waiver) or that their actions constitute a promise to pay the claim with the subsequent denial causing injury or harm to the insured (estoppel).



In most claims, the insurance company sends a reservation of rights letter automatically to permit investigation and preserve policy defenses. Because it is unilateral (one-sided, only protecting the carrier’s interests), created by the insurance carrier, and sent without any discussion with the insured party, a reservation of rights letter tends to irritate insureds or be seen only as an automatic response.

A non-waiver agreement is a better alternative to a reservation of rights letter. It is bilateral (two-sided, protecting the rights of both the insurance carrier and the insured) and is the result of both the insurance carrier and insured organization discussing the case and recognizing that there may be coverage issues. It permits the adjuster to continue processing the claim while preserving insurance carrier’s rights to deny the claim if the development of facts and establishment of the law warrants a declination. A good risk manager should be aware of possible actions taken because of coverage issues and be prepared to respond.

Important timing issues exist when resolving coverage issues. The insurance carrier must respond promptly after submitting the claim, using either the reservation of rights letter or the non-waiver agreement. Failing to respond promptly might be considered a waiver of rights (voluntary action not to respond) or estoppel (action inconsistent with a position taken). On the other hand, the insured organization must act promptly for the same reasons.

When all coverage issues are resolved, the insurance carrier must promptly notify the insured organization, particularly if the coverage is disclaimed, to avoid allegations of unfair claims settlement practices or bad faith claims practices and suits for extra-contractual damages.

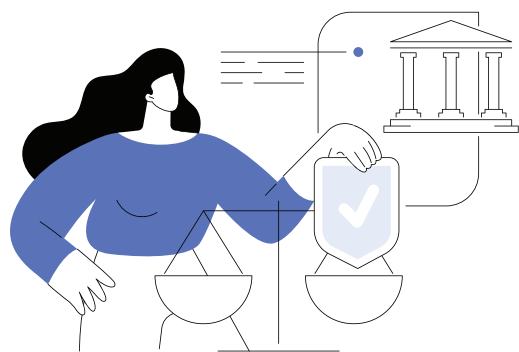
When the parties cannot resolve remaining coverage issues by negotiation, the parties have three methods for resolving the open issues.

## Section 5: Claims Management

1. **Declaratory judgment.** Either party may file a declaratory judgment action, which is a legal proceeding asking the court to resolve the issue based on the law rather than the facts.
2. **Arbitration or mediation.** This involves a meeting of the parties in a forum to encourage a resolution or force a resolution without entering into litigation.
3. **Assignment.** In an assignment, the insured organization that has a cause of action against another party can assign the cause of action to its insurance carrier. The insured organization receives whatever benefits are available under its insurance policy, and the insurance carrier assumes the responsibility for resolving the matter through whatever means are at its disposal.

Whenever coverage issues arise, two additional factors must be considered. A dispute may harm the continued relationship of the parties, particularly if the disagreement is divisive, extended, or expensive. Another concern is how the resolution will be funded. Litigation is the most costly method of resolving a coverage dispute, and while arbitration is often part of the insurance contract wording, the costs of resolving the coverage issue will not be covered by the insurance policy.

### Liability



In all losses and claims, it is important to think about theories of liability that may be used for or against the organization. The liability issues inherent in third-party claims are also important in first-party losses. In the investigation, the organization may find that a third party is responsible for causing the damages and thus must reimburse the organization or the insurer. This latter source of repayment is referred to as subrogation and is explained at greater length later in this section. Overall, the degree of liability must be determined, as it impacts the total value of the claim.

The following three general theories of liability explain how liability is determined and the potential remedies for liability.

**Contractual Liability** – This is the theory of liability that is established by the body of contract law. The potential remedies include the payment of actual damages (the most common remedy) as well as liquidated or limited damages, reformation of the contract, rescission or avoidance of the contract, and, rarely, specific performance.

**Regulatory or Statutory Liability** – This is established by legislation or regulation. Common examples are consumer protection statutes, financial responsibility laws, and environmental protection acts. Remedies include payment of actual damages, statutorily determined damages, fines, penalties, and injunctions.

**Torts** – These are civil wrongs or harm committed by one party against another. Some torts arise out of strict or absolute liability (e.g., situations in which one party is responsible without regard to fault). Common examples of strict liability are some types of products liability and absolute liability imposed for certain activities, such as those that are inherently dangerous (e.g., blasting, excavation, demolition, etc.) or by statute (e.g., products liability

## Section 5: Claims Management

or dram shop laws covering dispensing of alcoholic beverages). Some torts are intentional torts—acts intended to result in harm. Common examples are assault and battery, libel (written), and slander (spoken). The tortfeasor (the person who commits the wrong) intends harm through assault, battery, libel, or slander.

**Negligence** is the last type of tort and is the one that occurs most frequently. Negligence is based on the principle of failure to act according to the reasonable person. Four tests establish a cause of action based on negligence. First, one party must owe a duty to another party. Second, a breach of that duty must occur. Third, injury or damage must be sustained. Fourth, the breach of duty must be the proximate cause of the injury or damages.



### The elements of negligence—all must be proven to be actionable.

- A duty owed by the first party
- A breach of that duty
- Injuries or damages sustained by the third party
- A causal connection between the breach and the injuries/damages



For example, a company truck driver owes a duty to others to drive safely. Assume the driver is distracted by a cell phone call and runs a stop light. If there is no collision, there is a breach of duty, but the breach did not cause any damage. However, if the driver crashes into another vehicle and causes damage to that vehicle and its occupants, the breach of duty (careless driving) is the proximate cause of injury and damages. In this case, the action would meet the legal standard for negligence.

## Negligent Entrustment and Negligent Supervision

In many business personal activities, the concept of negligence may be extended from the primary tortfeasor (wrongdoer) to include other parties. This result of ever-growing and evolving theories of negligence has given rise to the concepts of negligent entrustment and negligent supervision.

Negligent entrustment is the entrustment of a dangerous object, usually a vehicle, boat, or piece of mobile equipment, to anyone that the owner of that object knew or should have known was not sufficiently capable of operating that object safely without causing injury to themselves, to a third party, or the property of another. For example, a business owner entrusts the company car to someone who is obviously intoxicated (or someone the owner knows might be intoxicated) by giving the keys to the intoxicated person. If the intoxicated person causes injury, the person will be negligent, either by strict liability if a dram shop law applies or in common law (a tort), and the business owner may be held liable for negligent entrustment.



Negligent supervision arises out of employment situations and is the failure to supervise or regulate the behavior of a person whom the supervisor knows or should have known was a

## Section 5: Claims Management

danger to themselves or a danger to a third party (e.g., hiring a known violent felon to work in the complaint department of a retail store). Another common situation that creates a scenario of negligent supervision is tolerating the behavior of an employee who continues to sexually harass fellow employees.

### Check-In



**Directions:** Respond to the questions below.

At a Lake Tahoe resort, a maintenance staff member forgot to clean the snow and ice from a parking lot. As a result, two guests slipped on the ice. Their incident reports are as follows:

**Guest number 1** suffered a broken leg when she fell after stepping on the ice. Her medical bills are \$4,000, and her lost wages are \$1,000. Is the Lake Tahoe resort negligent?

---

---

---

**Guest number 2** landed in a snowbank after slipping on the ice. He brushed off his ski clothes and continued to the chair lifts. Is the resort negligent?

---

---

---

### Damages



Evaluating the types of liability that exist with a claim can be used to establish an understanding of the potential damages related to a claim. The types of damages available in tort liability are compensatory (or actual) damages, statutory damages, and punitive or exemplary damages. Compensatory damages (or actual damages) include past and future economic damages, called special damages, or damages that can be clearly established through bills, invoices, or paystubs for lost wages. Compensatory damages also include past and future non-economic damages known

## Section 5: Claims Management

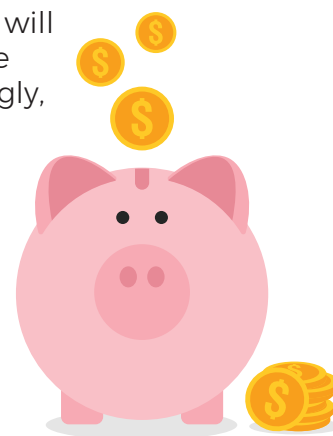
as general damages, or payments for pain and suffering, loss of companionship, consortium or affection, or inconvenience.

Statutory damages under tort are those defined by statute, such as payment of attorneys' fees or civil penalties paid under consumer protection statutes. Punitive or exemplary damages are imposed by the courts to punish a negligent party for their egregious, willful, or wanton conduct. Some statutes impose double or triple damages or a formulaic calculation of punitive damages based on specific damages. These damages are intended to discourage such behavior by the negligent party or others in the future.

### Reserving

The final portion of the evaluation is reserving. The setting of reserves will have an ongoing impact on many facets of the organization. After the degree of liability is assessed and the damages determined accordingly, the anticipated values of the damages and related expenses will be captured as reserves in the claims file. The reserves for liability claims reflect the future funds needed to resolve those claims. Accurate reserving ensures that the organization will have sufficient funds to pay its contractual obligations and liabilities imposed by statute or tort in the present and the future.

Reserves must include both anticipated loss payments and loss adjusting expenses. Accurate reserving is critical to the organization's "bottom line" or financial results and long-term financial solvency. With respect to an insurance carrier, accurate reserving is important when determining the insurer's financial rating in the insurance industry. Also, for insurers and self-insurers, accurate reserving is a factor in avoiding excessive scrutiny by regulators (e.g., the IRS and others). The two methods of establishing reserves are the individual case method and the formula method.



### Individual Case Method



An individual case reserve is the value assigned to a specific claim by a field adjuster or home office claims adjuster based on an investigation of the claim and the experience of the claims adjuster with similar cases. The individual case method is preferable because the reserve is more likely to represent the actual liability of the organization. It is most commonly used for property claims and certain third-party liability claims. This method is more effective when there are no coverage issues and the extent of the loss is readily calculable. However, it requires a high level of expertise and experience on the part of the claims adjuster.

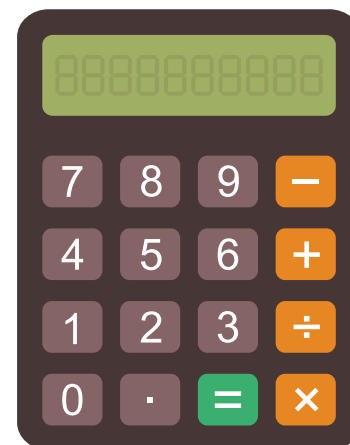


## Formula Methods

Formula methods are based on a mathematical approach. There are several formula methods an organization could potentially employ:

### 1. Average Value Method

This method relies on past experience for specific categories of claims to project reserves. For example, an organization may reserve its automobile physical damage claims (claims that are limited with respect to their ultimate value by the vehicle's value) by calculating the average value of physical damage and multiplying that value by the number of accidents. Please note that the average value method may be viewed as a sign of bad faith because the merits and weight of the individual claim are not considered.



### 2. Tabular Value Method

This method is useful for workers compensation and bodily injury claims in which a disability percentage, mortality, morbidity, and remarriage rates are established. The adjuster establishes the reserve by multiplying the tabular factors for each category times the average wage for that person. For example, if the person is determined to be 50% permanently disabled, has a life expectancy of 20 years, and has an average annual wage of \$50,000, the adjuster will calculate the reserve for the claim to be \$25,000 times 20 years.



Accurate reserving is important for several reasons. If reserves are set too low, the organization's assets will be overstated, the risk of future insolvency or bankruptcy is increased, problems with industry ratings may be created, and regulators may focus attention on the organization. If reserves are set too high, the organization's assets are understated, tax reporting problems and stockholder problems may be created, and the organization may mistakenly believe it does not have the financial resources to pursue profitable ventures or underwrite additional business.

A critical aspect of accurate reserving and reserve adequacy is the proper inclusion of reserves for **incurred but not reported (IBNR)** claims. The two types of IBNR claims are "pure" and "broad."

Pure IBNR claims are those that have occurred but have not yet been reported or recorded as reserves. Pure IBNR claims arise from the reporting and recording process through naturally occurring delays between the event and the discovery and/or report. For example:



## Section 5: Claims Management



A product manufactured by the insured fails and causes injury to a third party on January 2nd. Although the third party immediately pursues a workers compensation claim against their employer, it may take several months, or even a year, for the product defects claim to be reported to the manufacturer. Finally, on December 10th of the same year, the manufacturer learns of the alleged product failure and resulting injury to the third party. Although incurred, the claim against the insured manufacturer was not reported or recorded for an extended period after the injury-producing event.



**Broad IBNR claims** represent the natural change in the value of claims over time. The claims represented by broad IBNR values have been incurred, reported, and recorded, but the value has changed, and that difference in value has not yet been reported and recorded. In the early life of a claim, the broad IBNR portion of the claim tends to increase. Near the end of the life of the claim, the broad IBNR portion tends to decrease.



Arthur has sustained a crushing injury to his leg, which will require several surgeries to repair. His convalescence and recovery are expected to take several years. When his injury is first reported and reserved, the broad IBNR factor is quite large, accounting for an anticipated increase in medical costs and the development of the claim. As Arthur approaches recovery, the broad IBNR amount is reduced as most medical costs are known and leveling out.

IBNR reserves are subject to statutory accounting regulations for insurance carriers, captive insurance companies, and qualified self-insurers. Reserve inadequacy, particularly because of IBNR claims, will subject the organization to heightened regulatory scrutiny.

## Knowledge Check



**Directions:** Fill in the chart below.

As the risk manager at Uno's Fine Foods, you have completed your initial investigation. Explain what steps you would take during the evaluation phase of the claims management process for each of the following topics.

<b>Coverage</b>	
<b>Liability</b>	
<b>Damages</b>	
<b>Reserve</b>	

## Resolution

### Learning Objective

5.4 Discuss the resolution step of the claims management process, including the four types of alternative dispute resolution (ADR) methods.

During resolution, the investigator should identify potential issues that will influence resolution, such as the presence of a claimant's attorney or advocate, public opinion, likely publicity, and jurisdictional issues. After identifying these issues, the next step would be considering options for resolving the claim. In total, there are five non-mutually exclusive possibilities for the resolution of claims: payment in full, negotiated settlement, denial, litigation/alternative dispute resolution, and subrogation/recovery.



Payment in full is most often seen in first-party claims, as there is no adversarial investigation and evaluation of liability. If a home burns to the ground—through no fault of the insured—the insurance company pays the full policy limits, less any deductible, as there is no question regarding damages.

## Section 5: Claims Management

Negotiated settlements occur in both first-party and third-party claims. Negotiation is the process of preparing the facts and law, exploring the parties' positions, exchanging offers and counteroffers, and eventually reaching closure or agreement, followed by a settlement or resolution.

Denial may be issued by the insurer because there is no coverage. This may arise from:

- Application of an exclusion
- A claim that is not covered by the policy
- A claim against an individual that is not insured by the policy
- A claim where there is no liability on the part of the person being pursued

Denials may also be issued when damages are not proven, although this is less likely to occur.

Denial is an unpleasant action for both the adjuster and the claimant and is frequently the impetus for litigation. Consequently, denial requires a higher standard of investigation and evaluation to avoid allegations of bad faith or deceptive claims practices. Even when the claim is denied, it is essential to maintain good communication, as subsequent information may arise that might alter the original decision to deny the claim. Related to that is the need for the adjuster or claims representative to keep an open mind.



### Alternative Dispute Resolution

While litigation is a method of resolving claims, the process is often prolonged and expensive. Alternative dispute resolution offers a way of resolving disputes without the need for costly litigation. The four types of alternative dispute resolution approaches are mediation, arbitration, mini-trials, and summary jury trials.

#### Mediation



This is the least formal of the approaches. No evidence (in the legal sense of “evidence”) is presented. A neutral third party acts as a facilitator to explore settlement between the disputing parties. However, this mediator has no power to impose a decision.

In the usual mediation setting, the parties will meet to voice their positions and then retire to separate rooms. The mediator will start with one party, attempting to determine points that are firm and those that are flexible or negotiable.

The mediator will then meet with the other party for the same purpose. During the second round of meetings, the mediator suggests areas that might be investigated with the intent of bringing the parties closer together. During the entire process, the mediator has the

## Section 5: Claims Management

ethical obligation to disclose no specific positions or matters that either party advances but only to facilitate discussion and movement to a common ground.

### Arbitration

Arbitration is a semi-formal process. Summary or documentary evidence is provided, as opposed to testimony. Each party selects an arbitrator to negotiate on their behalf (presumably with their interests foremost in the arbitrator's mind), and the arbitrators select a neutral third arbitrator, sometimes called an umpire. When arbitration of this type is written as part of a resolution in an insurance policy, the agreement between any two parties will often be binding. In more complex issues, a panel of arbitrators may be used in lieu of a single individual. If the parties agree, the arbitrator's decision may be final and binding, but in some instances, the decision is advisory only, with the parties reserving the right to litigate. In practice, arbitrations often end with the arbitrators taking each party's position and finding the middle value or position.

### Mini-Trials and Summary Jury Trials



Occasionally, the dispute may be resolved by either a mini-trial or a summary jury trial. These are the most formal alternative dispute resolution types, as they are conducted in a quasi-judicial format. Evidence and testimony are presented but in an abbreviated or summary format. In a traditional courtroom, the fact finder is the jury or, in a bench trial, the judge. However, in a mini-trial or summary jury trial, the fact

finder is a mini-jury or a magistrate. A mini-jury comprises fewer jurors, while a magistrate is a lower-ranked judicial officer elected or appointed (depending upon state statute), with jurisdiction limited to the county or parish over which the magistrate presides.

Generally, the finding of a mini-trial is final, but the finding in a summary jury trial is not, unless agreed to by the parties prior to the summary jury trial. Summary jury trials are sometimes referred to as mock trials, where the parties test their theories and evidence to determine what might happen if the dispute were traditionally litigated as an aid to reaching a mutual settlement without the delay, expense, and risk of a traditional jury trial.

### Subrogation

Subrogation is a resolution to the claims process as the insurer settles with the insured by paying the claim and then attempting to recover their losses from another responsible party. The broad definition of subrogation is “the legal right of one who has paid another’s obligation to collect from the party originally owing the obligation.”



The insurance definition of subrogation is “the insurer’s right to recover from another responsible party the amount that the insurer paid to (or for) its insured for a covered loss.”

## Section 5: Claims Management

Overall, there are two main types of subrogation: equitable and contractual. Equitable subrogation arises from the common law right to recover damages from another party who caused the loss. Contractual subrogation arises from a contract provision that authorizes a right of subrogation. In risk management, both types of subrogation are considered. However, contractual subrogation is the most familiar as most insurance policies contain right of subrogation provisions, and many non-insurance contracts include waiver of subrogation provisions.

Subrogation minimizes an organization's the total cost of risk by recovering from negligent third parties the amounts paid for losses, including the portion of an insured loss that falls under the deductible or retention.



For example, an organization has a \$1,000 deductible on its automobile physical damage coverage, and one covered vehicle suffers \$5,000 collision damage from a negligent third party. The insurance company will pay the insured organization \$4,000 for the claim and pursue recovery of the total amount (\$5,000) from the third party. In most instances, if the subrogation attempt is successful, the insurance carrier must repay the recovered deductible to the insured organization, often subtracting a fee for its efforts, thus reducing the total cost of risk to the organization while also reducing the total cost of risk to the insurance company, which keeps the recovered \$4,000 it paid to its insured.



Subrogation possibilities create a special consideration for an organization whenever a legal relationship exists between the parties involved in a claim. Another example will illustrate this consideration.



Assume that Modern Builders has entered into a construction contract with Water Works. The contract includes a hold harmless agreement wherein Modern agrees to hold Water Works harmless from any and all loss arising out of the work contemplated by the contract. Modern also agrees to be fully insured for general liability.



During the work, a bystander is struck in the mouth and injured when a Water Works employee accidentally hits her with a shovel. The bystander sues Water Works, who tenders the claim to Modern under the hold harmless agreement, and Modern's insurance carrier pays for the bystander's bill under its policy's contractual liability wording. However, Modern's insurance carrier now attempts to recover from Water Works (the negligent entity) through subrogation.

Water Works says Modern agreed to hold it harmless in the construction contract and that a subrogation action would violate the spirit and letter of the hold harmless agreement. Thus, Modern's insurance company cannot recoup their claims payments.

### Recovery

Recovery is obtaining funds from another who bears some responsibility for or who also has coverage before the claim is settled. Examples of recovery sources include indemnification agreements, hold harmless agreements, joint venture agreements, and other insurance. Consider an example of recovery:



Using the Modern Builders and Water Works example, imagine if the hold harmless agreement contained a reimbursement clause. In this situation, Water Works would be responsible for paying the claim and then seeking recovery from Modern based on the hold harmless agreement.



### Special Concerns of Resolution



Regardless of the means of resolution, two important special concerns should be addressed. First, when a resolution has been established, the essential elements of the agreement must be reduced to writing immediately. Once the agreement is signed, it is binding on the parties. A common element of any resolution is a release, a legally binding agreement between the parties in which one party typically agrees to pay the other party for specified damages, and the other party promises to forgo further claims or litigation arising out of the event.

Second, how the payment is affected is critical. For the responsible organization, a lump sum settlement may be a poor decision as it loses the investment income on the settlement sum over future years.

There may be significant drawbacks for the claimant, as most large awards are squandered away within five years. Inexperience in money management, victimization by “advisors,” and poor financial discipline take their toll on lump sum awards. While the settlement amount is tax-exempt, the interest income on the amount invested (until it is squandered, that is) is taxable, thus adding to the financial drain.

Structured settlements can provide substantial advantages to both the claimant and the responsible party. First, for the responsible party, periodic payment settlements cost less than lump sum payments, as the responsible party has the opportunity to invest the funds not paid out immediately and earn income from those assets.

For the claimant (and family), periodic payments are not taxable as income, unlike the interest earned on an invested lump sum settlement. There is less possibility that the entire proceeds will be squandered early, as only small amounts are available at any one time. However, this advantage can be destroyed if the claimant succumbs to advertisements targeting recipients of lump sum settlements, as organizations state they are willing to purchase structured settlements “so you can get what you deserve now.”



## Section 5: Claims Management

Naturally, the purchase amount will be a lesser amount because of the time value of money, so the claimant has a smaller sum to squander, and any interest earned on that amount is now taxable.

For both the claimant and the responsible party, a structured settlement schedule of payments can be tailored to meet the claimant's personal and family needs. For example, if a claimant has young children, the settlement payments can be structured to provide additional funds for college years.



For the claimant's counsel, a structured settlement helps the attorney meet moral and ethical fiduciary obligations to the claimant, i.e., to secure funds for future years to meet future needs. Some attorneys prefer the entire legal fee to be paid immediately and the residual settlement amount to be paid out in a structured schedule, while others will take a structured payment to ease their tax burden. Again, these choices will affect the organization's cost of loss.

### ▶▶ Knowledge Check



**Directions:** Answer the question below.

You are the risk manager for Uno's Fine Foods. After investigating, you've found that several students under the age of 18 became ill after dining at Uno's restaurant. What would be an appropriate way of bringing this claim to its resolution?

---

---

---

---

---

---




# Types of Claims Management Plans

## Learning Objective:

5.5 Analyze the three types of claims management plans and the considerations that should be made when selecting a plan.

As part of the claims management process, the risk manager needs to understand the organization's type of insurance plan and any of its additional claims-related services. In total, there are three types of claims management plans.

- 1 **Insured Plan**
  - 2 **Third-Party Administered Plan**
  - 3 **Self-Administered Plan**
- 

## A Word About Deductibles



Before discussing the specifics of the different types of claims management plans, it is important to understand a few key points about deductibles. Nearly all insured plans have deductible options, but the deductible is “small.” Small in this context is a relative term. One common “small” deductible is a maintenance deductible, designed to avoid insurance carrier involvement in claims of a trivial size relative to the organization. This is the most expensive kind of claim because

of the high fixed cost compared with the settlement amount and one generally required by the insurance carrier.

These deductibles can reach several thousands of dollars, sometimes tens of thousands, when the insured is willing to assume more of the smaller-sized (and probably highly predictable) losses in exchange for premium savings.

Typical examples might include a \$500 or \$1,000 deductible on automobile physical damage, \$5,000 on property coverage, or \$25,000 per occurrence on general liability or products liability coverage. In general, however, a “small” deductible is the term used to describe a “small”—relatively speaking—deductible elected by the insured to reduce the premium by retaining smaller, more predictable losses.



## Section 5: Claims Management

Third-party administered plans might have a deductible that starts at \$5,000 or \$10,000 when there are a large number of claims (also highly predictable) that the insured organization wishes to outsource or where an independent claims adjuster brings objectivity and distance into the settlement process, such as under workers compensation coverage. Self-administered plans usually still have higher deductibles and retentions, even to the point where a deductible might equal the policy limit.



Keep in mind that there is a subtle but essential technical difference between deductibles and retentions, even though many in the risk management and insurance industry use these terms interchangeably.



From a purely technical viewpoint, in a **deductible plan**, the insurance carrier provides all policy services from the first dollar of loss. In the case of the elected deductible, the insurance carrier then bills the insured organization after payment of the loss, seeking reimbursement for the costs falling within the definition of the deductible. Thus, the insured organization's total cost of risk is sensitive to loss but delayed, and the claims services are the insurance carrier's responsibility. When a deductible on a first-party insurance policy is a maintenance deductible, the insurance

carrier applies the deductible to the total value of the claim, paying the net amount to the insured; there is no "payment in full, reimbursement to follow."

The insurance carrier has no obligation to provide any claims management services with a self-insured retention, commonly called an SIR, including payment of losses and defense costs, until the SIR assumed by the insured organization has been satisfied. In other words, the insuring agreement has a dual or double trigger. For a loss to be covered by an SIR insurance policy, the event must be covered (peril, location, policy term, no exclusion or limitation, etc.), and the amount of the loss paid by the insured organization must exceed (or be reasonably expected to exceed) the SIR before the insuring agreement is triggered.

### Insured Plans (Guaranteed Cost Plan/First Dollar Plan)

In the insured plan approach, the insurer provides both insurance and claims management services. The features of an insured plan include the insurance carrier providing at least an annual "loss run" or a listing of all losses ("all" is defined by the reporting guidelines), either in print or through online access. A valuable expansion of this service is ad hoc reporting, or the ability of the insured organization to acquire loss runs on demand rather than periodically, such as ongoing online access or a monthly or quarterly printout.



## Limitations of Insured Plans

With an insured plan, the insured organization has little or no input regarding reserving philosophy or case reserves. The insurance carrier establishes reserves with the presumption that these are set to protect the interests of the insurance carrier, even in a loss-sensitive plan.



Additionally, the insurance carrier determines and controls the staffing of its claims department. Some insurance adjusters are competent, some are mediocre, and a few are very inadequate. Depending on the size of the deductible or SIR and the influence of the insured organization, it can work with the insurance carrier to reassign staff or have a dedicated claims team, but direct control is always the prerogative of the insurance carrier.

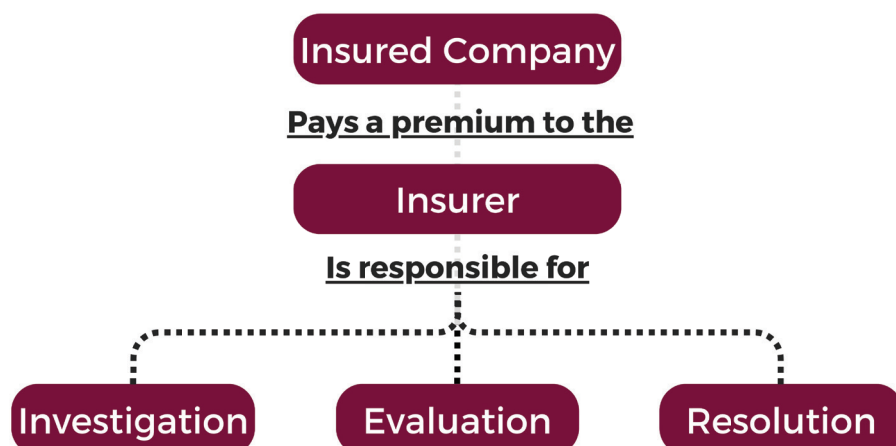
Another problem with insurance carrier staff is that the insured organization's geographic operations and sources of loss may not coincide with the insurance carrier's claims presence. It is generally preferential to have claims resources near the insured's exposures to loss.

Involvement with claim reviews again depends on the size of the deductible or SIR and the influence of the insured organization. Even then, the insured will have minimal input related to the resolution and settlement process.

The feature that often creates the most dissatisfaction with insured plans is the process of resolution and settlement. The insurance carrier directs resolution and settlement with the goal of protecting the insurance carrier's profit and stakeholder value. Insured organizations frequently accuse insurance carriers of wasting the organization's premium or funds by paying non-meritorious claims or by freely paying "nuisance value" claims to avoid the expense of litigation. In most cases, the insurance carrier utilizes in-house or staff counsel for routine litigation.



## Insured Plan Structure



## To Bundle or Unbundle?



The process of an organization outsourcing claims administrative services is commonly known as “unbundling.” Unbundling is generally the separation of insurance (an insurance carrier’s external risk financing) from loss control and/or claims administration. In a typical unbundled insurance arrangement, the insurance carrier continues to provide all other policy management services, including filing proof of coverage with state agencies when required and reporting claim and loss data to insurance rate-making authorities such as the National Council on Compensation Insurance (NCCI) and other state and federal agencies. When others require proof of coverage, the insurance carrier may provide certificates of

insurance or evidence of insurance coverage or delegate that authority to the agent or broker.

During the risk financing decision-making process, one consideration in evaluating risk financing plans involves whether to use internal department resources or the use of outside services to handle claims management.



There are several reasons why an organization would elect not to use its insurance carrier’s claims management services. First, it may be more cost-effective for organizations to handle claims internally or through an independent third party than when claims services are performed by the insurance carrier and included as part of the premium. Further, with an inside or independent claims manager, the focus of the claims settlement process (or other services) is on the organization’s best interests, not the insurance carrier’s profit and stakeholder value.

While there are benefits to unbundling, not every organization is a candidate for unbundling of the claims handling function. Generally, unbundling requires the organization to assume a much larger portion of the risk than organizations using a loss-sensitive program in which the insurance carrier plays a greater part in claims handling. Also, the annual insurance premium for traditional insurance product lines (general liability, products and completed operations liability, workers compensation, and automobile physical damage) must be large enough to justify the insured’s assumption of risk and administrative services and still be attractive to target insurance markets (some markets prefer to keep the control they have in handling claims).

Further, the organization must have a greater risk tolerance for higher self-insured retentions, frictional costs (transactional costs), and management costs, as well as being prepared to accept a potentially different array of services under an unbundled program compared to traditional insurance placements.

Most importantly, the organization’s financials must support the anticipated total cost of risk associated with claims administration. The risk manager must consider the nature of the traditional insurance product line and associated factors such as the development of claims in future years,



## Section 5: Claims Management

the impact of inflationary trends on claims costs, market risk, interest rate risk, general economic patterns, and the increase in the level of uncertainty over time.

If an organization decides to unbundle claims services, it may still participate in an insurance program, even though the retention level is high, to reduce its risk from catastrophic claims or aggregation of losses. To a greater degree, the organization controls its own destiny when it assumes the claims administration function through unbundling without assuming the administrative burden associated with compliance with state self-insurance applications and reporting requirements.



Occasionally, an organization using self-insurance in some areas of exposure operates or expands into a state that does not permit self-insurance in another area of exposure, or its operations in a state do not meet the minimum requirements for self-insurance, including small operations that cannot be economically self-insured. An unbundled insured program provides a good alternative in those instances.

Perhaps most importantly, unbundling may avoid problems associated with a “run-off” situation created when the organization changes insurance carriers. If the organization provides its own claims management or purchases the services from a third-party administrator, continuity of dedicated claims handling is maintained despite the change in carriers.

### Third-Party Administered Plan

A third-party administered (TPA) plan usually entails a combination plan, using a deductible or sizable retention and an excess insurance policy issued by an insurance carrier that does not provide claims services. The insured organization hires an independent third party to provide claims services and possibly other services that insurance carriers traditionally provide.

The size of the deductible or retention usually is larger than those found on traditional insurance plans, although there is no specific retention amount that is needed to qualify a program for third-party administration. Like in an insured plan, loss information can be provided on a regular basis or an ad hoc basis. The ability to access loss information in real time via the internet allows the organization to obtain information on an inquiry basis.



Third-party administered plans also offer the insured greater control of reserving and claims management. Reserves reflect the TPA’s reserving practices and may vary widely from office to office. However, since the TPA is chosen through a selection and negotiation process (and the interests of the insured organization are ostensibly paramount), the insured organization has more input into the process than in a traditional insured plan. The organization must plan for resources to regularly monitor and audit the TPA reserves as necessary. One critical aspect of the reserving process is determining who will notify the excess carrier when stipulated claims thresholds are met. The TPA service agreement must clearly state who is

## Section 5: Claims Management

responsible for notice to the excess insurance carrier when claims reach or are expected to reach the amounts stated in the excess policy.

These plans also offer the insured greater choice over TPA staffing during the selection process. During TPA selection, it may be possible to designate specific adjusters to handle the insured's account. However, if designated staffing is not negotiated during the selection process, the TPA staffing issues are like those underinsured plans. Also, geographic issues and concerns are like those found in insured plans.



The process of settling claims is more flexible under a TPA plan than under an insured one. Since claims within the retention amount are the insured organization's complete responsibility, the risk manager's input carries more weight than under an insured plan. The loss payment procedure is determined by both the primary layer of insurance and the insured organization's retention policy. The TPA administers payments within the retention amount, although consultation with the client organization for approval prior to settlement is customary.

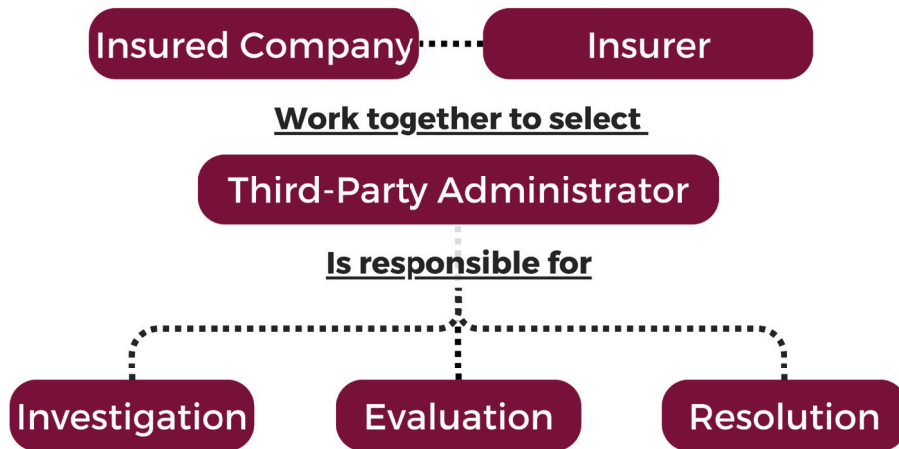
Claim reviews are typically performed when stipulated in the contract or when the insured deems it necessary. These reviews provide a good way for the risk manager to determine the effectiveness of the adjusters.

Overall, outsourcing the claims administration to a TPA provides the insured with control of the claims management function without the administrative burden of complying with state self-insurance application and reporting requirements. It is also a good alternative for organizations that cannot economically justify or do not meet minimum requirements for self-insurance in all states of operation. In addition, it allows continuity of the claims management function when problems are created by "run-off" situations when insurers are changed. With a TPA plan, the insured can change insurers without changing TPAs.



It is important to note that excess insurance policies have requirements for reporting claims of a defined nature (e.g., loss of a limb, sight, hearing, or disfigurement) or of a stated amount that is within the retention amount but less than the attachment point of the excess coverage (this is the dollar amount where the excess carrier becomes responsible for paying the loss). Approval or authorization of the excess insurance carrier is typically required prior to settlement activity on these types of claims as there is a chance that, if settlement efforts are unsuccessful, the claim may end up being more costly and in excess of the attachment point. Also, many excess insurance policies have so-called "hammer clauses," which stipulate that if the insured organization refuses to approve a settlement recommended by the carrier and acceptable to the injured party, the insurance carrier's liability is limited to the amount for which the claim could have been settled.

### TPA Plan Structure



### Self-Administered Plans

As mentioned previously, the deductible or retention in a self-administered plan usually is substantial, perhaps even reaching policy limits. In some instances, there may be no excess insurance coverage purchased, as the entire exposure may be retained. These plans have several advantages.

First, a self-administered plan provides the greatest flexibility of options for the loss runs. Generally, a self-administered plan will feature the organization assuming responsibility for data management by using a risk management information system (RMIS). This includes the costs of system acquisition, set-up, maintenance, and operation. Thus, the self-insured organization can design and obtain loss runs regularly or on an ad hoc basis, with the ability to customize reports or search and monitor for specific problems or issues on a virtually instantaneous basis.



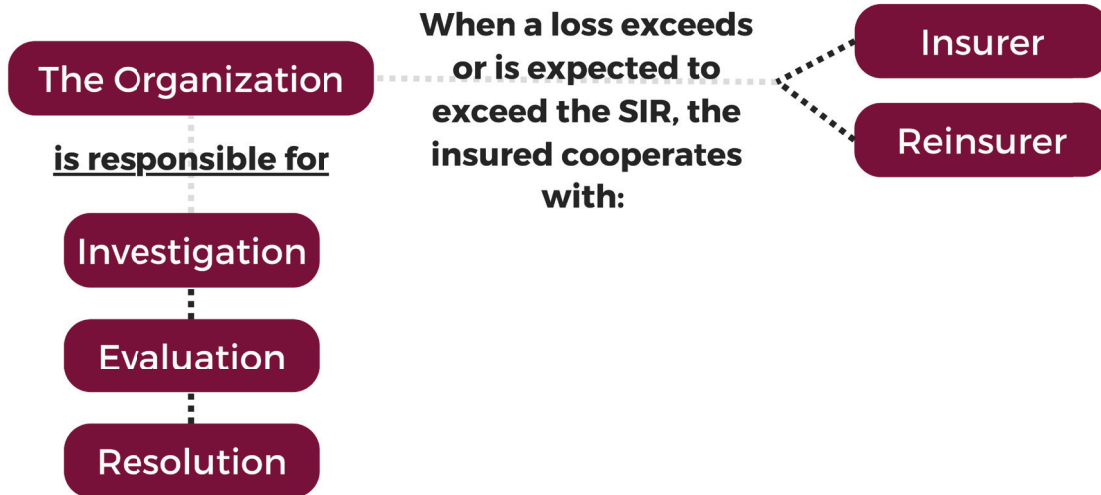
Reserving is the total responsibility of the organization. There is a significant incentive to be accurate and to maintain appropriate internal funding and/or credibility, especially when reinsurance carriers are involved. Unfortunately, there can be a tendency of upper management to keep reserves low and reduce the apparent total cost of risk, thus freeing available financial resources for other uses. Self-administration requires careful monitoring of claims and reserves as part of the financial auditing process.

The self-administered organization has ultimate control over the entire claims staff. However, there are restraints, as the staff must satisfy reinsurance carriers and state regulatory authorities in licensing, administrative, and continuing education requirements (where applicable).







Similarly, the self-administered organization has ultimate control over settlements. Cases with catastrophic potential may still require coordination with reinsurance carriers and cash flow, and cash management issues require the risk manager's proactive attention throughout the settlement process.

### Self-Administered Plan Structure







## Selecting a Claims Management Plan

When selecting a claims management plan, there are many differentiators to consider and decisions to be made to find the plan that best suits an organization's business needs. Review the table to see the areas that should be considered when selecting a plan.

	What is it?	Why it matters
<b>Loss Sensitivity</b> 	The degree of the insured's financial participation in a claim; its risk appetite and risk-taking ability	Some organizations may be more financially affected by losses, while others are more resilient.
<b>Loss Runs</b> 	A list of reported claims providing such information as the names of insurers and/or claimants, the date of occurrence, type of claim, amount paid, and amount reserved for each as of the report's valuation date	Organizations should consider how easily loss run data can be accessed and who owns the data based on the plan type.
<b>Loss Reserves</b> 	The amount of money earmarked for a loss or claim	Organizations need to decide how much control they need over setting loss reserves.
<b>Staffing</b> 	The personnel who are handling the claims	Staffing is important because it can present quality control issues. The level of experience, capabilities, and workload of staff can impact claims handling.



## Section 5: Claims Management

	What is it?	Why it matters
<b>Settlement</b> 	The terms reached to close out a claim	Different plans grant organizations different levels of control over the settlement process. An organization may desire to have more direct authority over settlement decisions.
<b>Litigation Management</b> 	An organization's process of managing legal services and costs, or their principles regarding the use of outside legal services	In some plans, the insurer is primarily responsible for selecting defense counsel and determining how aggressively a claim is fought. This may not be preferable for some organizations.
<b>Bundling vs. Unbundling</b> 	Bundling provides a group of services as part of a package. In an unbundled plan, the insurer allows an organization to select only the services they need.	Not all organizations have the financial ability, expertise, and resources to benefit from an unbundled plan.
<b>Claims Audit</b> 	Evaluation of the claims handling process through a detailed review of claims files and records	Who conducts it, and who gets to see the results?

## Section 5: Claims Management

Review the following table for more information on how these considerations vary between the different plan types.

Characteristic	Type of Plan		
	Insured	Third-Party Administered	Self-Administered
<b>Loss Sensitivity</b>	<p>Usually low</p> <p>Guaranteed cost; dividend; small deductible</p> <p>Deductible – The insurer provides all policy services from the first dollar and bills the insured post-payment.</p> <p>SIR – no obligation by the insurer until the satisfaction of the SIR amount by the insured</p>	<p>Moderate</p> <p>Includes larger deductible or larger SIR</p>	<p>Extremely high</p> <p>Very large SIR or no excess insurance coverage</p>
<b>Loss Runs</b>	<p>Online access with some ad hoc reporting</p>	<p>Loss info is available in real time; ad hoc reporting is available</p>	<p>The insured controls reporting. The insured is responsible for data and use of the RMIS and can customize reports for specific problems or loss exposures.</p>
<b>Reserving</b>	<p>Insurer controls</p> <p>The insured has little input regarding philosophy or case reserves.</p>	<p>TPA controls</p> <p>Reflects TPA's reserving philosophy; notification to the insured when the reserve exceeds a set amount; RM resources required to monitor and audit</p>	<p>Insured controls</p> <p>There is a tendency for reserves to be set too low; monitoring is part of the auditing process; credibility with reinsurers must be maintained.</p>

## Section 5: Claims Management

Characteristic	Type of Plan		
	Insured	Third-Party Administered	Self-Administered
<b>Staffing</b>	No control	Some control  Most TPAs are responsive to staffing requests and preferences of the insured.	Ultimate control  Must adhere to regulatory requirements (licensing, CE issues)
<b>Settlement</b>	Insurer has control	Greater control within SIR  Approval/ authorization of the insurer is typically required prior to payment on larger cases.	Ultimate control  Settlement authority is often obtained from senior management; cash flow/cash management issues require proactive attention.
<b>Claims Audit</b>	Insurer seldom shares results	Internal audits are rarely shared	Internal audits are critical; full feedback
<b>Litigation Management</b>	The insured has little or no influence over the insurer.	More responsive to the insured's philosophy	High control; generally more willing to litigate
<b>Bundling</b>	Bundled	Some unbundling available	Unbundled

## ▶▶ Knowledge Check



**Directions:** Answer the question.

The CFO of Hometown Bank wants an insurance plan that provides stability and 100% external financing. What type of plan should he select? Why? What would be some disadvantages to the plan?

---

---

---

---

## Claims Audits

### Learning Objectives:

5.6 Describe the components, requirements, and possible findings of a claims audit.

### The Risk Management Function of Claims Audits

A claims audit is a systematic review of open and closed claims files to evaluate the adjuster's competence and performance. Claims audits are valuable because they eliminate surprises and disclose whether the insurer, TPA, or in-house claims administrator uses best practices. In addition, the audit helps identify problem claims, the need for additional investigation, areas of frequency or severity concerns, duplicate or frivolous payments, and the potential cost of loss issues while simultaneously avoiding difficulties arising out of claimant complaints, settlement costs that exceed case reserves, unexpected increases in reserves, and claims going to trial without adequate preparation. A claims audit also enables the risk manager to confirm that contribution is being sought from subrogation, excess coverage, and reinsurance carriers.



Claims audits are a proper and necessary risk management function. The claims audit process requires a regular and ongoing verification of the status of all outstanding claims. Regardless of the type of claims administration, the risk manager or risk management audit team must regularly conduct claims audits. The only difference between the audits of each type of claims management approach is the risk manager's degree of involvement and responsibility.

When preparing to conduct a claims audit, the risk manager must consider the composition of the audit team. The expertise of risk management and claims professionals is important, but cross-functional participation increases the credibility and acceptance of the claims management process. Another decision to be made is the audits' frequency and degree of depth. Naturally, due to the types of claims administration approaches, there will be variations in the audit process.



### What Is Reviewed During an Audit?



Audits cover a range of operations that impact the claims management process. The following lists contain items that will be reviewed during an audit under the different types of claims management plans.

#### Carrier Audits

During an audit, insurance carriers will review:

- Employee compliance with internal processes and service standards
- Claims technical work product. This refers to the quality of claims handling work the claims adjuster does. Are benefits paid promptly? Are claims resolved equitably? Was correspondence received in a timely fashion?
- Employee statutory compliance
- Financial integrity
- Vendor management and cost control

#### TPA Internal Audit (or Carrier Audit of TPA)

TPAs will review:

- Employee compliance with internal processes and service standards
- Claims technical work product
- Reserving practices
- Employee compliance with client-specific service standards
- Employee statutory compliance
- Financial integrity
- Vendor management and cost control
- Carrier reporting requirements

### Self-Administered Plans

When an organization controls its own claims management, they should audit:

- Employee compliance with internal processes and service standards
- Employee statutory compliance
- Financial integrity
- Vendor management and cost control
- Carrier reporting requirements



### Actions for Claims Service Purchasers

When an organization purchases a claims service, there are several actions that they should take.

First, organizations should obtain a copy of their claims service provider's best practices or service standards. If the claims service provider is a TPA, these standards should be incorporated into the contract.



Other account-specific service standards the organization needs should be negotiated, agreed upon, and reduced to writing by the provider. These standards should then become part of the audit.

Furthermore, an organization should reserve the right to audit claims with reasonable notice. They should also require a copy of the completed audit report whenever their claims files are audited—whether by the claims office, adjuster, or specific accounts.

If the audit is not at 80% compliance or better, the organization should require an action plan detailing improvements the provider will make. Never accept an adjuster who has failed the audit. Instead, request that they be removed from the account and replaced.

## Possible Audit Findings

Audits will identify potential areas of concern. The following table presents a range of the various regions that audits should review, as well as potential issues that could be revealed through an audit.

Claims Audit Area	Possible Findings
<b>Claims Payment Issues</b>	<ul style="list-style-type: none"> <li>• Duplicate payments</li> <li>• Overpayments</li> <li>• Frivolous payments (e.g., paying for unrelated treatment or medications)</li> </ul>
<b>Claims Handling and Reserving Practices</b>	<ul style="list-style-type: none"> <li>• Poor reserving (i.e., stair-stepping or repeatedly spending down the reserve and then increasing it, using the reserve like a checking account)</li> <li>• Failure to pursue subrogation</li> <li>• Failure to seek contributions from excess and reinsurance carriers</li> <li>• Failure to watch and track policy aggregate limits</li> <li>• Allowing claims to go to litigation when resolution was possible</li> </ul>
<b>Procedural Issues</b>	<ul style="list-style-type: none"> <li>• Evidence that phone calls, emails, etc., are not receiving prompt responses</li> <li>• Failure to obtain releases</li> <li>• Improper application of statutes, such as incorrect temporary total disability (TTD) rates</li> </ul>
<b>Proper Documentation of the Claims File</b>	<ul style="list-style-type: none"> <li>• Failure to document</li> <li>• Incomplete or inadequate documentation</li> </ul>
<b>Other Concerns and Red Flags</b>	<ul style="list-style-type: none"> <li>• Increased litigation</li> <li>• Complaints about adjusters from insured's brokers, underwriters, etc.</li> </ul>

## ▶▶ Knowledge Check



**Directions:** Answer the question below.



Shania is the risk manager for Red Rock Manufacturing. Red Rock has operations in 16 states. She is preparing a claims audit of her TPA. Shania asks them to pull a representative sampling of workers compensation files for her review. When she arrives at the TPA's offices, she is shown to an office with eight files on the desk. Her account manager tells her there are two open "lost time" files from each of the adjusters managing her workers compensation claims. Shania is surprised because she knows Red Rock has over 200 claims a year.

Explain why Shania will not be able to conduct an effective claims audit. Include an explanation of how Shania could have avoided this issue during the audit of the TPA.

---

---

---

---

---

---

---

---



## Third-Party Administration (TPA) Selection

### Learning Objective:

5.7 Explain the role of a third-party administrator (TPA) and the major considerations of the selection process.

### The Role of the TPA

Before discussing the considerations when selecting a TPA, it is essential to understand the role the TPA fulfills for an organization. The TPA is usually retained by the individual organization, which is responsible for paying its fees.

In certain instances, carrier approval may be required. In those circumstances, there may be an approved list of TPAs that the carrier maintains and from which the organization may select a service provider. Typically, those TPAs on the list are well-versed in the carrier's reporting requirements and have a history of successful claims resolution. TPAs have a fiduciary responsibility to both the carrier and the organization and should advise both the organization and the carrier when claims should be accepted and denied. It is important to note that the TPA may not issue a reservation of rights/denial letter since this would be the carrier's responsibility.

The TPA is responsible for investigating and resolving claims within the organization's self-insured retention or large deductible. The insured organization extends the dollar amount of settlement authority and often payment authority. The frequency and nature of reporting on claims progress are established during the interview process.

The TPA is also charged with reporting to the excess carrier on high-value claims expected to exceed the retention. This is typically done when the incurred losses reach 50% of the retention or immediately on "red flag" claims such as brain injury, significant burns, fatalities, etc. Ideally, the carrier approves the TPA to continue managing the claim after the retention has been met. This ensures that there are no transition issues or delays in claims management. In those circumstances, the TPA will request reimbursement from the carrier for funds spent in excess of the retention on reimbursement policies. Alternatively, the carrier will have established a claims fund from which the TPA may make payments, again with approval from the carrier.

## Major Considerations for Selecting a TPA

After an insured organization has decided that hiring a third-party administrator is the appropriate choice for claims management, several important factors must be considered in the selection process.



**Accessibility**



**Systems compatibility**



**Flexibility in account handling**



**Staffing**



**Best practices and quality control**



**Industry experience and reputation**



**Additional services**



**Pricing and Contract**

### Accessibility

The claims adjuster or team must be readily accessible. Accessibility means not just the number and location of claims offices but the risk manager's ability to communicate with each claims office. Claims reporting and communication should be straightforward and can be facilitated using the internet. Another critical aspect of accessibility is the willingness and ability of claims personnel to conduct file reviews, have meetings with clients to discuss all aspects of the claims process, and be available for physical inspections, etc. Other aspects of accessibility include the assignment of an account manager and a dedicated claims team.

### Systems Compatibility

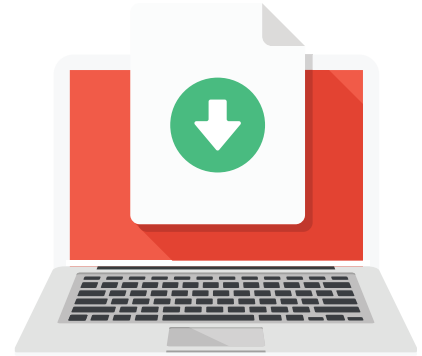
The information system and other proprietary claims management software used by the third-party administrator should support meaningful risk management analysis by using revenue codes, divisions, departments and locations, special client-specific coding, and statutory reporting required fields such as NCCI codes, NAICS (formerly SIC) codes, and OSHA codes.

The information system must be able to convert existing carrier claims data to the administrator's system. The administrator should have experience with the current format and timelines. The system should enable easy extraction of data. It is also beneficial if it provides internet access aids for:

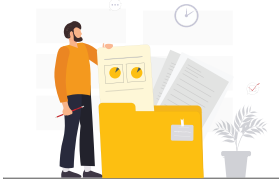
## Section 5: Claims Management

- Ad hoc reporting
- Drive-down capabilities
- Entering claims notes and financial reports
- Reporting packages online or by email
- Exporting data to excess carriers
- Downloading and reporting formats

Accessing data in real time means that financial information can be and must be accurate, that overall financial exposures are quantifiable, and that funding needs and requirements are handled on a timely basis. The extent of inquiry capabilities should include the use of claim notes, claim financials, rollbacks, and “as of” values. The system should also be loss-detail driven, with data accessible for analysis in multiple formats and criteria. Optical character reading (OCR) and scanning capabilities can help facilitate entering data into the information system. For security purposes, the information system must include firewall levels, both internal and external.



### Flexibility in Account Handling



The administrator must provide flexibility in account handling because claims, as routine as they may seem, are never exactly the same. Customized claims handling instructions, particularly for claims within the retention or deductible, should be created and accepted by both the claims administrator and the client.

Claims handling instructions encompass:

- Notice of large losses to the risk manager
- Settlement authority limitations
- Quarterly (or more frequently when indicated) claims reviews
- Regular claims audits
- Monthly reporting packages
- A negotiable fee structure
- Reserve and payment authority limitations
- Selection of counsel procedure
- An assigned account manager and dedicated claims team
- Banking assistance
- Ability to design a program to match needs and objectives
- Ability to continue handling a claim if it exceeds the attachment point and penetrates the excess coverage

In case of a necessary move from a TPA to an insurance or excess carrier or another TPA, there should be a detailed transition plan for the orderly takeover of claims with minimal disruption of services to clients and/or claimants.

### Staffing

During the selection process, the TPA recommends claims personnel that they believe are an optimal match for the insured organization. The organization is also involved with shaping the service team. Thus, the risk manager can request and review professional bios and interview the candidates for the claims team. The turnover rate for the TPA and any involved branch offices should be examined, as a high turnover rate suggests a possibility of inconsistency of staffing in the assigned team or overall management.



Experience is an important consideration when choosing the TPA. Risk managers should also consider the longevity of the TPA, the assigned staff, and the firm's overall experience in handling the lines of business specific to the organization's industry type.

A list of carrier and client references, from both past and present clients, facilitates the verification of the TPA's expertise and performance on service commitments. Each staff member's workload of both newly reported and pending claims is also critical to good service and quality control.

### Best Practices and Quality Control



Related to the professionalism of the TPA is the existence and use of "best practices" and quality control procedures. If there is a written best practices policy or a minimum claim standards policy, it must reflect current industry standards, address technical and system competencies, and include a compliance review. In addition, the TPA must be willing to incorporate best practices or quality control commitment into the service agreement as a material performance element.

The service agreement should also indicate how performance and quality control are measured. The measurement parameters may include the following:

- An internal audit process
- The identification of the auditors
- How well the audit worksheet and criteria reflect best practices
- The frequency of audits
- The sufficiency of the sampling of claims files results
- An action plan to correct deficiencies
- Compliance and improvement elements
- The willingness to provide audit reports to the client

Further, the risk manager should determine the administrator's position on independent or outside claims audits and establish the expectation that the client or its representative will also be allowed to perform audits.

### Industry Experience and Reputation

Industry experience and an excellent reputation are needed to secure the optimal settlements. If the closest or most practical TPA is unknown to the risk manager, colleagues and industry resources may know this vendor. The risk manager should view websites and promotional materials, keeping in mind that these may not accurately represent the reliability of a TPA.



As in the case of hiring internal staff, contacting references is critical, and when calling them, the risk manager must be prepared with specific questions framed to determine capabilities and experience in the needed areas. Additionally, it is appropriate to ask the TPA for its benchmarking statistics so the risk manager can measure the results of the vendor's work compared to national and state-wide standards, across industry groups, and by the type of insured organization. If the vendor does not produce its benchmark data, the risk manager must ask how the TPA measures financial performance and results against the administrative services marketplace.



When the search comes to the point of interviewing the TPA, a portion of the interview process should be directed to inquiries about lost clients, canceled contracts, financial status, longevity, and professional liability insurance limits, as well as the existence of any pending litigation against the vendor. While details may not be provided, a request can be made to counsel to search legal databases for filed suits to verify the accuracy of responses.

Also, it is important to ask about ownership involvement in the day-to-day operations of a TPA. The size of the vendor matters, as the corporate administrator with many distant owners may not have the same sense of urgency in handling client affairs as the smaller vendor whose ownership is present, easily accessible, and involved in day-to-day operations.

### Additional Services

One of the underlying reasons for selecting third-party administration as a claims management approach is the ability to unbundle services, moving from a *prix fixe* (fixed price) insurance carrier-dictated service menu to the ability to select needed services *à la carte*. Thus, the administrator must be willing to allow the insured organization to select only the services the organization wants and to work with existing service providers on other matters. The risk manager should determine whether the TPA can provide services beyond the current program, perhaps expanding into loss control and medical case management with preferred provider organizations (PPOs) or managed care organizations (MCOs).



Another significant issue is transparency, in which the administrator will disclose any ownership interests in recommended services, such as when a bill review company is a subsidiary of the TPA or owned by the vendor's principals.

## Section 5: Claims Management

The risk manager should confirm pricing for bundled and unbundled services, particularly allocated loss adjustment expense (ALAE), an important component in the total cost of risk. The risk manager should know if any subcontractors will be providing work for the administrator, with the necessity of approving those subcontractors, as well as obtaining proof of insurance coverage, including additional insured status in favor of both the TPA and the insured organization.



Determine other services that might be provided. For example, the administrator may offer consulting services to develop specific risk management or claims management programs for the organization (e.g., a drug-free workplace or transitional duty program) or training programs for pertinent issues like employment discrimination, harassment, or lockout and tag-out programs. The TPA may also offer to design safety programs or assist with safety initiatives specific to locations, operations, or loss types.

Another optional service is the design of internal forms and processes to streamline the claims reporting and claims management processes, particularly in the areas of data capture, recording, and reporting. Related to the reporting service would be an analysis of claims by type, loss causes, frequency, or severity, as well as consulting to improve results.

### Pricing and Contract



The risk manager must be satisfied that the pricing and value-added services are appropriate. It should be noted that even “free” services have a cost buried somewhere.

The risk manager must be careful when evaluating proposals, as the “cheapest” is not always the best. Services and selection criteria must be evaluated along with the indicated pricing. Whenever possible, the pricing of competing vendors must be compared on the proverbial “apples to apples” basis.



Flexibility and transparency in pricing is a major factor to consider. Options for close evaluation will include fees per claim, annual flat fees, quarterly payments, reconciliations, or virtually any combinations the parties can imagine. The service agreement must precisely define what the services agreement covers, as well as the amount of the annual administration fee or annual management fee. Related to this is a definition of the allocated expense categories. It is imperative that the parties confirm their agreement on this matter.

Specific to claims management administration services is the need to compare how per-claim pricing is developed, as it might be based on a two or three-year planned life of a claim or “cradle to grave.” “Cradle to grave” must be further defined in terms of continuation of the administrative services contract. Some “grave” definitions refer to the end of the claim regardless of the administrative service contract, while others have the caveat that the services contract must be in force.

## Section 5: Claims Management

Two last considerations when selecting a TPA are the availability of the TPA to attend industry meetings and seminars or other educational events and providing refresher systems training for the internal staff of the insured organization. As mentioned at the beginning of this section, this multitude of optional services may be presented as “free” or as value-added services, but the astute risk manager knows that everything has a cost, even if it is not clearly indicated, and will ask specific questions.

### Contractual Considerations

The service agreement should specify that the TPA will indemnify its client for its own negligence. For example, if the TPA incorrectly calculates the wage benefits for an injured worker and a court imposes a fine on the organization for the shortfall, the TPA should reimburse the organization for the fine. The risk manager should carefully review the service agreement typically prepared by the TPA for other indemnification issues in the service agreement, which may require discussion and/or negotiation.



Another area of concern is ownership of the claims data and claim files. It should be established at the outset that they are the organization’s property. This should be done to avoid a situation where a decision to change TPAs is made, and the existing TPA holds the claims files “hostage” until all billings are paid.

Finally, the service agreement should provide for terminating the relationship. The notice period should be established—usually 60 to 90 days—and the manner of transitioning the files and data should be established. Any costs associated with the transfer of data or files should be clearly laid out.

To summarize, selecting a third-party administrator to handle the organization’s claims requires consideration of several factors. Each factor will have a different weight depending on the type of organization, the nature of its operations, and the anticipated claims volume. The key elements include accessibility of the claims handlers and ease of communication, whether in reporting claims or discussing cases. The claims staff’s experience, expertise, and professionalism are also important factors. Since the claims handler is the “voice” of the organization when dealing with claimants, they must be knowledgeable about its business operations and industry.

Contractual considerations and pricing structure also play a role in the decision-making process, as well as the comfort level the risk manager has with the TPA and its ability to manage claims.



## Knowledge Check



**Directions:** Answer the questions below.

1. One consideration in TPA selection is the qualifications of their staff. List four additional considerations that should be carefully evaluated during the TPA selection process.

---

---

---

---

2. Describe at least two TPA staff qualifications that should be reviewed as part of selecting a TPA.

---

---

---

---



# Selecting Defense Counsel

## Learning Objective:

5.8 Explain the considerations when selecting defense counsel for an organization.

The legal practice, like medicine, has become more specialized over the years. The general legal practitioner still has a place in providing legal services, but the number and complexity of laws, regulations, and industry practices have led to narrow and specific legal practitioners with specialty training and experience. Review the considerations that should be made when selecting defense counsel.



**Management  
Profile**



**Workloads**



**Size of Firm**



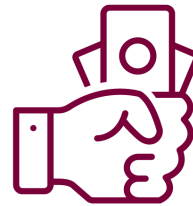
**Client Base**



**Experience Level**



**Reputation in  
Industry**



**Fee Structure**

## Management Profile

When selecting defense counsel, reviewing the management profile of the law firm is an essential first step. Consider whether the managing partner is present and engaged in firm's day-to-day activities. Ideally, the partner should be an active force in the litigation of cases.

## Workloads and Size of Firm

The risk manager should also inquire about and consider the workload of the lawyer or legal team, particularly in contrast to the size of the firm. Small boutique firms may have a high level of expertise, but only in a narrow range of practice with a very limited number of practitioners. Large caseloads may spread the capabilities of these firms too thin. In a very large firm, cases might not get the attention the risk manager and stakeholders desire. The risk manager must be comfortable with the size of the firm and its ability to provide the needed defense services.



## Client Base

An inquiry into the client bases is also advisable. It should be determined if the firm represents competitors and whether this will create potential conflicts of interest in representing the organization. Furthermore, whether the attorney will need access to proprietary information or trade secrets that might be disclosed to an organization's competitors should be considered.

## Experience and Reputation



A firm's extensive expertise, experience, and industry-related training create a solid support team for any retained individual lawyer. Counsel should be familiar with the industry the organization is in. They should have handled similar businesses and issues.

The risk manager should consider the experience level, education, and training of the individuals who will be assigned to the organization's claims. They must also be comfortable that the legal team and the organization's risk management or claims

management staff can relate effectively with one another.

Further, the risk manager should ascertain the law practice's and individual team members' reputation in the insurance and/or business community, especially among the attorney's or law firm's current and past client base. For example, the law firm's history of litigation or settlement is one crucial consideration a risk manager should analyze.

## Fee Structure

The risk manager must also consider the fee structure and how billing will occur. Most law firms have differentiated fees or rates for senior partners, junior partners, associates, counsel lawyers, investigators, paralegals, secretaries, and any other function so enumerated. The concern is not the absolute value of the rate, as that is a function of experience, education, training, specialty, and geography. The real issue is clearly defining who will perform what activity or what levels of activities will be performed by each fee strata. Often, it is very costly and very ineffective and/or inefficient to have a senior partner billing at \$500 an hour for legal research that a paralegal could do at \$75 an hour.



The risk manager must also identify the minimum charge increments. Some firms charge by 0.10-hour or 0.15-hour blocks, so a one-minute telephone call costs the same as a five-minute call. The differences between these two schedules can significantly affect the total billable hours and associated fees charged for frequent short-duration projects.



In addition, the risk manager must identify other possible charges. Some firms charge for time spent with a client at lunch or dinner, perhaps for the entire time at dinner, even though some of that time is spent eating and socializing. Other litigation costs that may appear on an invoice for legal services are court reporter fees, photocopying costs, overnight delivery fees, courier fees, travel time and expenses, and usage charges for the law firm's computer hardware and software.

Fees for and the utilization of these services should be established and agreed upon before retaining counsel. For example, hardware and software are typically seen as an operating expense of the firm and not billable to the client. An exception may be when the case involves a matter of first impression (a novel case that is new and has not arisen before). Similarly, a large volume of overnight delivery or courier fees may indicate a timeliness issue on the part of the law firm in meeting legal deadlines.

Because of the multiple opportunities for charges to be created, any good litigation management plan will have an activity review function. An activity review function will match billings to activity reports and provide information to the risk manager or claims manager regarding those findings.

Billing agreements delineate in advance how the legal services invoices will be generated. These agreements can be grouped into three broad approaches: hourly rates, flat fees, and contingent fees.

## Section 5: Claims Management



Hourly rate invoices are generated by multiplying the number of billing units (e.g., .10 hour, .15 hour, 1.5 hours) per staff member times the specified unit rate for that staff member. The hourly charges are added, and the total is the amount shown on the invoice for legal services. Other options under the hourly rate approach are the use of a negotiated discounted rate, wherein the rates charged to a particular client are discounted to reflect a volume of legal work from that client, or a negotiated hourly limit, where the maximum time to be spent on a particular activity is limited.

The flat fee approach may consist of a flat fee per claim or a flat fee for all claims. When a flat fee for all claims approach is used, the law firm virtually becomes the in-house counsel.

The last fee is a contingent fee base. This is a common approach for billing by the plaintiff's counsel, particularly in personal injury cases, where the attorney's fee is stated as a percentage (30%, 33%, 40%, etc.) of the damages recovered. If the plaintiff receives nothing, the lawyer earns nothing. This approach does not work well for defense counsel. However, if the organization is the plaintiff, it can expect to see this type of billing arrangement. It is important to note that defense counsel and plaintiff's counsel are "two different animals," and that a single lawyer rarely fills both roles.



## Summary

Effective claims management is a vital part of a risk control program, as it reduces the organization's overall total cost of risk, driving dollars to the bottom line. The role of a risk manager in this process is essential.

It is clear that a risk manager's tasks in claims management or assignment of claims management and follow-up are varied, involve outlays of cash, and may include personnel retention. The risk manager should also employ their expertise to make decisions on claims management plan structures based on the organization's risk appetite and risk-taking ability.

When a decision is made to use an unbundled insurance plan, the risk manager will participate in the selection of a third-party administrator (TPA) to handle claims on behalf of the organization. There are several considerations in the selection of the TPA. These are accessibility, systems compatibility, flexibility in account handling, staffing, best practices and quality control, industry experience and reputation, additional services, and pricing and contract considerations.

The risk manager will also be involved in selecting defense counsel for the organization and will use a similar set of criteria to qualify counsel and find those most likely to benefit the organization.

## Section 5 Self-Quiz

**Directions:** Answer the questions below.

1. Which of the following statements about claims management are true? **(Select all that apply.)**
  - ☐ Claims management aims to resolve claims promptly and at an optimal cost.
  - ☐ Claims management only applies to self-insured organizations or those that use a TPA.
  - ☐ Strong claims management programs focus on resolving claims solely through litigation.
  - ☐ Enforcing contractual obligations during claims management can reduce the total cost of risk.
2. Why is effective claims management beneficial to a risk control program?
  - ☐ An effective claims management plan can improve an organization's customer service.
  - ☐ An effective claims management plan can reduce or mitigate damages.
  - ☐ An effective claims management plan improves communication within an organization.
  - ☐ An effective claims management plan improves an organization's communication with external stakeholders.
3. ABC Construction recently completed an office building. Throughout the construction, several specialized subcontractors were used. One of the tenants of the building is severely injured after being shocked while using an electrical outlet. The tenant sued, alleging that ABC's negligence in construction led to her injury. What question(s) should the risk manager ask during the investigation phase of managing this claim? **(Select all that apply.)**
  - ☐ Could the defective work of a subcontractor be the cause of the injury?
  - ☐ Was the injured tenant wearing rubber-soled shoes at the time of the incident?
  - ☐ Was the tenant using a defective electrical device that could have caused the shock?
  - ☐ Did the injured tenant recently move from another state?
4. A non-waiver agreement is unilateral and only protects the interests of the insurance carrier.

True

False

## Section 5: Claims Management

5. An individual files a claim against Super Fun Theme Parks. The facts show that the theme park failed to train employees in safety measures, resulting in unsafe practices leading to the individual's injury. Did the park behave negligently?
- Yes No
6. The degree of liability Super Fun Theme Parks has for the accident has little impact on the total value of the claim.
- True False
7. The severity of the injury does not impact the damages the theme park can expect to pay.
- True False
8. Which one of the following definitions correctly describes the individual case method of evaluation?
- ☐ This method involves a value being assigned to a claim by an adjuster based on an investigation and past experience with that type of claim.
  - ☐ This method relies on past experience for specific categories of claims (such as physical auto damage) to project reserves.
  - ☐ This method is best used in claims in which a disability percentage, mortality, morbidity, and remarriage rates are established.
  - ☐ This method involves an outside investigation of the claim's value and is typically used when fraud is suspected.
9. Which one of the following is an example of a pure IBNR claim?
- ☐ A grocery store patron slips and falls on spilled milk but quickly leaves because they are embarrassed. After going to their doctor, they realize they are injured but decide not to pursue a claim against the grocery store.
  - ☐ A grocery store patron slips and falls on spilled milk. The incident is documented immediately, and the patron refuses to sign a release. The store attempts to settle, but ultimately, the patron pursues litigation against the company.
  - ☐ A grocery store patron slips and falls on spilled milk. The manager immediately documents the incident. The patron ultimately signs a release after the company makes an *ex gratia* payment.
  - ☐ A grocery store patron slips and falls on spilled milk but quickly leaves because they are embarrassed. Six months later, a doctor tells them they have three slipped disks from the fall. A year later, they file a suit against the grocery store.

## Section 5: Claims Management

10. Which one of the following best illustrates why alternative dispute resolution (ADR) could be preferable to traditional litigation?
- ☐ ADR provides an opportunity for public exposure and media coverage, ensuring a swift resolution to a dispute.
  - ☐ ADR offers a structured and formal legal process, ensuring the involvement of multiple judges for unbiased decision-making.
  - ☐ ADR typically results in lower costs and potentially faster resolution than traditional litigation.
  - ☐ ADR allows for the appeal to higher courts, offering parties a chance to challenge decisions they disagree with.
11. Which of the following statements about settlements are true? **(Select all that apply.)**
- ☐ Structured settlements can avoid the issue of the claimant squandering the settlement due to inexperience in money management.
  - ☐ A lump sum payment is preferable for an organization since it can save more money to invest in other assets in the long run.
  - ☐ Lump sum payments generate interest income, which is taxable. This can contribute to the claimant's financial drain.
  - ☐ Structured settlements violate an attorney's fiduciary obligations to the claimant since they secure less money in the short term for the client.
12. The right-hand column describes types of organizations. Based on its need, match each organization to the type of claims management plan it would most likely benefit from.

<b>A. Fully Insured</b> <b>B. Self-Administered</b> <b>C. Third-Party Administered</b>	_____ A company wants complete control over its settlement procedures and wants to use its own in-house counsel for all claims-related matters.
	_____ A company wants more input on its own risks but lacks the resources and financial throughput to manage its own claims entirely.
	_____ A small start-up wants to purchase a stable and externally financed insurance plan. The goal is to be able to budget based on an annual premium.



## Section 5: Claims Management

13. Which of the following are components of a claims audit of a TPA? **(Select all that apply.)**
- ☐ Financial integrity
  - ☐ Claims technical work product
  - ☐ Marketing practices
  - ☐ Reserving practices
14. After an audit, an organization finds that its TPA has repeatedly failed to pursue subrogation and has also allowed claims to go to litigation when resolution was possible. These audit findings indicate issues with:
- ☐ Claims payment
  - ☐ Claims handling
  - ☐ Procedural issues
  - ☐ Documentation issues
15. Which contractual considerations should a risk manager make when selecting a TPA?
- ☐ Does the TPA specify in the service agreement that they will indemnify the organization when the TPA is negligent?
  - ☐ Is the TPA's size appropriate for the organization, and is the TPA's management readily available?
  - ☐ Does the TPA have accurate promotional materials on its website?
  - ☐ Does the TPA allow for flexibility in account handling, or does it use a cookie-cutter approach?
16. A risk manager is working with a law firm. Why would it be in the risk manager's interests to clearly define which law firm members will participate in certain legal activities?
- ☐ Doing so will be more cost-effective if experienced law firm members conduct activities like research since this will reduce the total billable hours.
  - ☐ Doing so will ensure a higher quality of casework if the organization can avoid having paralegals or junior associates perform tasks.
  - ☐ Doing so will be more cost-effective if law firm members with lower fees (like paralegals) conduct basic activities like legal research.
  - ☐ Doing so will ensure the law firm rotates lawyers between tasks frequently, ensuring that there is no burnout while working the case.

## Set Yourself Up for Success!

### Visit the “Resources” Webpage at [RiskEducation.org/RCresources](https://RiskEducation.org/RCresources)

For valuable reinforcement, be sure to visit the “Resources” webpage. This webpage contains a variety of materials that will help you absorb the course material *and* set you up for success on the Final Exam. You’ll find:

#### Study Guide

Download a copy of the Study Guide. It contains all the Check-In questions, Knowledge Checks, and Self-Quizzes contained in this Learning Guide in a format that makes it easy for you to practice and check your answers.

#### Flash Cards

Play an interactive vocabulary game with a study set of digital flashcards to enhance your learning of the insurance and risk management terms used in this course.

#### Review Game

Use a fun, trivia-style review game to test your knowledge and prepare for the Final Exam.

#### Video Clips

View a video clip about an important concept related to one of the learning objectives in this section.



Claims Management

#### Downloadable Article

Read “Claims Audits—A Value-Added Service,” by Sarah Warhaftig, J.D., CRM.

## In Addition...

#### Appendix

The Appendix of this Learning Guide contains a Glossary of terms as well as tips for study techniques and sample test questions that will help you prepare for the Final Exam.

# Appendix

---

## Preparing for the Final Exam

For many learners, test preparation is stressful. Please keep in mind that the most important measure of your knowledge will be witnessed in your service to your organization. Think of a test as a tool. Use it to come to an understanding of what you know, how it affects your work, and what more you would like to know to have even greater success in the workplace.

The testing period for the Final Exam is 2 ½ hours long. The test itself is composed of 17–21 short-answer questions for a total of 200 possible points. Questions appear in the order of presentation of the topics.

Remain aware of the time as you take the test. Pace yourself and be aware that unanswered questions are considered incorrect.

## Study Techniques

There are some techniques you can use to help you prepare for the end-of-course test. Apply the same techniques to each chapter in your Learning Guide.

1. Review the Section Goal.
2. Review each Learning Objective.
3. Change each header and subhead into a question. Then answer the question. For example,  
Header: Components of a Formal Training Plan  
Question: What are the components of a formal training plan?
4. Review each diagram, graph, and table. Interpret what you see. Ask yourself how it relates to a specific Learning Objective.
5. Check your answers to each Check-In. Correct your original answers, if necessary.
6. Check your answers to each Knowledge Check. Consider ways to improve your original answers.
7. Re-read the summary at the end of each section.
8. Check your answers to each question in the Self-Quizzes at the end of each section. Correct your original answers, if necessary.
9. Review any comments, highlights, or notes you made in each section.

## Appendix

10. Rewrite important ideas in your own words. Find ways to connect those ideas to your own work experiences.
11. Make flash cards to help you review important vocabulary.

### Sample Test Questions

1. The Americans with Disabilities act of 1990 established several definitions crucial to understanding Employment Practices Liability. One of those is disparate impact. Please provide that definition.

#### Sample Answer:

A practice that appears to be a neutral employment practice but has an otherwise unjustified adverse impact on individuals within a protected class.

2. A crisis will typically have four distinct phases. Please identify and describe those phases in the correct order.

#### Sample Answer:

- a. **Threat** – There is a likely probability of occurrence, but it has not yet happened.
- b. **Warning** – The occurrence is imminent.
- c. **Event** – The event occurs at a specific time and place with a potential adverse effects.
- d. **Impact** – This is the effect of the event after it has occurred.

# Glossary of Terms

## Section 1: Risk Management Concepts

**accident** – an unexpected and unintentional event that tends to result in damage or injury

**avoidance** – eliminating an activity or exposure, thereby removing the chance of a loss

**claim** – a demand for payment or an obligation to pay as the result of a loss. Claims can be paid by the insurance company or an individual/organization.

**duplication** – a risk control technique that aims to reduce the overall severity of a loss by using back-ups for critical systems or operations

**ergonomics** – 1) the applied science of equipment and workplace design intended to maximize productivity by reducing operator fatigue and discomfort; 2) fitting the work environment to the person rather than expecting the person to adapt to the physical work environment

**expected losses** – a prediction of the frequency and severity of losses based on loss history distributions and statistics

**exposure** – a situation, practice, or condition that may lead to a loss. Activities, resources, and assets are also viewed as exposures.

**frequency** – the number of incidents, accidents, occurrences, or claims in a given time period, usually a policy year or calendar year

**hazard** – a condition or circumstance that makes a loss from a given peril more likely or more severe

**incident** – an unplanned event that may lead to a loss or a claim

**loss** – a decrease in the value of an asset

**occurrence** – an accident without a time constraint

**peril** – the cause of loss

**prevention** – a risk control technique that attempts to reduce the frequency of types of claims that cannot be eliminated by breaking the sequence of events that leads to a loss or by making a loss event less likely

**pure risk** – a situation whose only outcome can either be loss or no loss

**qualitative risk analysis** – a type of risk analysis used to look at possible risks and how an organization might be impacted by them

**quantitative risk analysis** – a type of risk analysis that uses numerical values to predict the likelihood and severity of a risk

## Appendix

**reduction** – a risk control technique that attempts to reduce the severity or financial impact from losses that are not prevented

**risk** – the possibility of a positive or negative outcome arising from a given set of circumstances

**Risk Administration** – the implementation of the risk management program's policies and procedures and the ongoing monitoring of their success

**Risk Analysis** – the process of assessing the potential impact exposures may have on an organization

**risk appetite** – an organization's willingness to accept or tolerate risk

**Risk Control** – any conscious action or inaction to minimize at the optimal cost the probability, frequency, severity, or unpredictability of loss

**Risk Identification** – the identification and examination of all an organization's exposures, perils, and hazards

**Risk Financing** – acquiring funds to pay for losses an organization experiences

**risk-taking ability** – the financial capacity an organization has for assuming risk

**risk transfer** – a risk control technique that attempts to reduce or prevent loss by transferring some or all of the risk to another organization

**segregation** – the isolation of an exposure from other exposures, perils, or hazards

**separation** – the spread of exposures or activities over several locations

**severity** – the dollar amount of a single loss or the total value of all losses in a given time period

**speculative risk** – the possibility of loss or no loss; however, it also presents the chance of a gain

**Total Cost of Risk (TCOR)** – the sum of all costs and expenses associated with risks and risk management within an organization. The formula follows: 1) Insurance costs + (2) retained losses + (3) risk management department costs + (4) outside service costs + (5) measurable indirect costs = TCOR

## Section 2: Risk Control and Mitigation – Human Resources

**Days Away, Restricted, and Transfer Rate (DART)** – A Bureau and Labor statistics measure of injury and illness cases involving days away, restricted duties, or transfer to other duties during the return-to-work phase; calculated with the following formula:

$$\frac{\text{\# of DART cases} \times 200,000}{\text{\# of hours worked by all employees in a given year}}$$

**Total Recordable Injury Rate (TRIR)** – a formula applied to any work-related injury beyond first aid; calculated with the following formula:

$$\frac{\text{\# of cases of injury and illness} \times 200,000}{\text{\# of hours worked by all employees in a given year}}$$

## Section 3: Risk Control and Mitigation – Property and Liability

**COPE** – an acronym referring to a structure’s construction, occupancy, protection and exposure

**disabled individual** – any individual who has a physical or mental impairment that substantially limits one or more major life activities

**discriminatory treatment** – situations in which an individual is treated differently from other similarly situated persons because of that individual’s protected status

**disparate impact** – a practice that appears to be a neutral employment practice but has an otherwise unjustified adverse impact on individuals within a protected class

**exculpatory agreements** – pre-event exoneration of the fault of one party that results in any loss or specified loss to another

**hold harmless agreement** – the affirmative assumption of the financial consequences for liabilities of another party through a contract between and indemnitor and indemnitee

**hostile or offensive work environment** – an environment that exists when unwelcome sexual conduct, overt or subtle, has the effect of unreasonably interfering with an individual’s work or performance or creates an intimidating, hostile, or offensive working environment

**Incident Response Plan** – A set of protocols and instructions for responding to and mitigating a cyber-attack

**indemnitee** – the one who is owed the obligation from another

**indemnitor** – the one who owes the obligation to another

## Appendix

**invasion of privacy** – The intrusion upon the privacy and personal information of another by a person or entity without permission or just cause

**limit of liability or liquidated damages clause** – pre-event limitation of the amount, type, or method of calculation of damages available by one or both parties to an agreement

**maximum possible loss (MPL)** – the total value at risk at a single location regardless of protective measures. The amount is limited only by adequate separation between structures.

**multifactor authentication (MFA)** – a security layer that requires the user to provide two or more pieces of evidence to be authenticated

**privileged access management (PAM)** – a security technology that allows differing levels of access within an organization

**probable maximum loss (PML)** – the amount of loss expected from a specific peril given some level of impairment or delay in protection. PML is expressed as a percentage of the total values. Unless noted, PML refers to the peril of fire.

**reasonable accommodation** – any modification or adjustment to employment, an employment practice, or the work environment such that a qualified individual with a disability has an equal opportunity to obtain and hold that employment

**retaliation** – occurs when an organization makes an adverse employment decision or action against an employee who files a complaint, grievance, or lawsuit alleging injury from an employment practice

**sexual harassment** – unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature

**telematics** – systems that use a mobile device to send and receive data from vehicles to a server

**waiver of subrogation** – a pre-event agreement to waive the right to seek recovery from a responsible party's insurance carrier for loss payments made to the insured

**wrongful termination, discharge, or dismissal** – when an employee's contract of employment is terminated by the employer, and the termination breaches one or more terms of the employment contract or an employment law

**zero trust architecture** – a security measure that requires the continuous validation and monitoring of a user's privileges and those associated with their device

## Section 4: Crisis and Disaster Planning

**business continuity** – the ability of an organization to perform critical operational tasks during and following a disruptive event



**crisis management** – The act or process of managing a crisis to prevent a catastrophic loss, if possible, and reduce the impact of catastrophic losses on the organization, including its reputation and brand

**disaster recovery** – Maintaining the consistency and performance of vital resources, technology, and infrastructure during and after a disruptive event and returning to regular operations

## Section 5: Claims Management

**arbitration** – a meeting of the parties in a forum to encourage a resolution or force a resolution without entering into litigation

**assignment** – a situation where the insurance carrier assumes a cause of action that its insured has against a third party. The insured “assigns” the cause of action to its insurer.

**alternative dispute resolution** – a way of resolving disputes without the need for expensive litigation. Examples include mediation, mini-trials and summary jury trials.

**claims management** – the prompt resolution of an organization’s losses subject to insurance or an active retention program, including claims by other individuals or entities to which it may be legally bound or ethically responsible

**contractual liability** – the theory of liability that is established by the body of contract law

**declaratory judgment** – a legal proceeding asking the court to resolve the issue based on the law rather than the facts

**deductible plan** – an insurance plan in which the insured agrees to reimburse the insurer for a specified amount for each claim

**IBNR (incurred but not reported)** – represents the liability for unpaid claims not reflected in the case reserve estimates for individual losses. The two components to IBNR reserves are pure IBNR and broad or bulk IBNR; pure IBNR are those claims that have occurred but have not yet been reported as of the evaluation date; and, broad or bulk IBNR is the additional development on known claims or the increase in reserve value as the claim are investigated and settled.

**insured plan** – a plan where the policyholder (individual or employer) pays a defined premium to an insurer and does not share in the risk associated with actual claims

**mediation** – a meeting of the parties in a forum to encourage a resolution or force a resolution without entering into litigation

**mini-trial** – a quasi-judicial format in which abbreviated testimony/evidence is presented and presided over by a mini-jury or magistrate. A mini-jury is comprised of a smaller number of jurors. Mini-trial results are generally final.

**negligence** – the failure to act as a reasonably prudent person would under the same set of circumstances

## Appendix

**negligent entrustment** – the entrustment of a dangerous object—usually a vehicle, boat, or piece of mobile equipment—to anyone the owner knew or should have known was not sufficiently capable of operating it in a safe manner

**negligent supervision** – the failure to supervise or regulate the behavior of a person whom the supervisor knows or should have known was a danger to themselves or a danger to a third party

**non-waiver agreement** – a bilateral (two-sided) agreement protecting the rights of both the insurance carrier and the insured. It is the result of both parties discussing the case and recognizing that there may be coverage issues.

**recovery** – obtaining funds from another who bears some responsibility for or who also has coverage for the claim

**regulatory or statutory liability** – liability established by legislation or regulation

**reservation of rights letter** – a letter sent by the carrier to an insured party indicating that a claim may not be covered under a policy. It is a tool to avoid the repercussions of estoppel or waiver arguments.

**self-administered plan** – a plan in which the organization assumes responsibility for claims management and claims data management using internal staff

**self-insured plan** – a plan in which an organization makes a conscious decision to not purchase insurance and to pay certain claim amounts using 100% internal funding

**subrogation** – the insurer's right to recover from another responsible party the amount the insurer paid to (or for) its insured for a covered loss

**summary jury trial** – a quasi-judicial format in which abbreviated testimony and/or evidence is presented and presided over by a mini-jury or magistrate. Summary jury trials are not binding if not agreed to in advance by the parties.

**third-party administered (TPA) plan** – an independent third-party administrator (TPA) is hired by the insured to provide claims services and possibly other services that insurance carriers traditionally provide

**tort** – a civil wrong, other than a breach of contract, for which the court may award damages

