



# **CERTIFIED RISK MANAGERS**

## **Control of Risk**

The National Alliance  
2021 Online Learning Guide



# **CERTIFIED RISK MANAGERS INTERNATIONAL**

## **Control of Risk Table of Contents**

**1 — RISK CONTROL AND MITIGATION - HUMAN RESOURCES**

---

**2 — RISK CONTROL AND MITIGATION - PROPERTY & LIABILITY**

---

**3 — CRISIS & DISASTER PLANNING**

---

**4 — CLAIMS MANAGEMENT**

---





## A Letter from William J. Hold, CEO

We know that choosing the right professional development programs to strengthen your career can be challenging. There are many options for you to choose from; so how can you be sure that your time, efforts, and money are being invested and not wasted?

By becoming a committed participant of The National Alliance, you can rest assured that you are also making the best educational choice for your career—no matter what step of your learning path you are on.

For the last 50 years, our designations have been regarded throughout the industry as symbols of quality and trust. Our practical insurance and risk management courses are taught by active insurance practitioners, include polices and forms currently used in the field, and guide you through real-world scenarios to give you a deeper understanding of what your clients are facing today. The knowledge and skills you develop in any one of our courses (or designation programs) can be put to use immediately.

You will build long-lasting relationships with your clients, stay ahead of industry trends, emerging risks, and products that are constantly evolving in our dynamic market. You will have access to the industry's latest learning materials and will be the first to hear about new courses. With a learning path customized to fit your needs, you will be better equipped to protect your clients.

Have no doubt that your success is our priority. Whether you are new to your career, or a seasoned professional, you are about to embark on a wonderful professional development journey. Thank you for choosing The National Alliance for Insurance Education & Research as your guide toward a thriving career.

Let's take the first step.

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





# Certified Risk Managers

*a proud member of The National Alliance for Insurance Education & Research*

## Section 1

# **Risk Control and Mitigation - Human Resources**





## Resources

[Key Terms](#)



## Risk Control & Mitigation - Human Resources

### Learning Objectives

1. Define risk control and describe its purpose and scope.
2. Know the reasons why organizations should focus on risk control.
3. Identify and apply the five primary types of risk control techniques to a scenario.
4. List the root causes of accidents and injuries.
5. Identify and apply the six basic steps of accident prevention.
6. Identify and explain the elements of a health and safety program.
7. Discuss the risk factors associated with ergonomics.
8. Identify the risk factors and risk control measures associated with manual material handling and lifting.
9. Describe the benefits and possible legal problems associated with a workplace substance abuse program.
10. Name the risk factors and risk control measures used to prevent or reduce workplace violence.

Exposures to loss that have been identified in the risk identification step of the risk management process must be controlled. Successful risk control programs are based on careful risk identification and risk analysis. Administration of a risk control program requires prioritization, implementation, coordination, follow-up, and communication throughout the organization.

---

### **Learning Objective 1:**

Define risk control and describe its purpose and scope.

---

**Definition:** Any conscious action or inaction to minimize, at the optimal cost, the probability, frequency, severity, or unpredictability of loss

**Purpose:** To take action by focusing on solutions that will prevent, mitigate, avoid, or eliminate risk

**Scope:** It is a people process in which individuals within the organization must be involved in all aspects of an effective risk control program

### **Learning Objective 2:**

Know the reasons why organizations should focus on risk control.

---

#### **It's Good Business**

##### **To Reduce Costs:**

1. Insurance, Total Cost of Risk, etc.
2. Prevention measures generally cost less than paying for a loss

**For Compliance** – It's the law – OSHA, DOT, workers compensation statutes, etc.

**For Care and Concern** – Of the health and well-being of employees and the general public

##### **To Protect Reputation and Brand Name**

## Five Primary Risk Control Techniques

---

**Learning Objective 3:**  
Identify and apply the five primary types of risk control techniques to a scenario.

---

### Avoidance

1. Precludes or discontinues an activity to avoid the chance of loss, eliminating both positive and negative outcomes
2. Avoidance is a self-supporting risk control technique that may be:
  - a. Proactive – conscious decision to avoid exposure to loss by not doing the activity in the first place
  - b. Passive – discontinuing or abandoning an operation or activity that carries significant exposure to loss
3. Avoidance may not totally control exposure to loss from past activities (e.g., discontinued products still in the marketplace or in the hands of consumers)
4. Avoidance may be difficult to sell to management
  - a. May be in conflict with goals and profit motives of the organization
  - b. Activity may be inherent to the organization's identity or mission
  - c. Risk manager may lack appropriate decision-making authority

## Prevention

1. Reduces the frequency of losses
2. Prevention involves an action taken to break the sequence of events leading to a loss or an action that makes the loss less likely
3. Allows entities to conduct operations that might otherwise have been avoided

## Reduction – Pre-Loss and Post-Loss Activities

1. Reduces the severity of financial impact from losses
2. **Pre-Loss** – reduction activities applied *before* the loss  
Example: installing fire suppression equipment
3. **Post-Loss** – reduction activities applied *after* the loss  
Example: claims administration including prompt response, early intervention, rapid claim closure

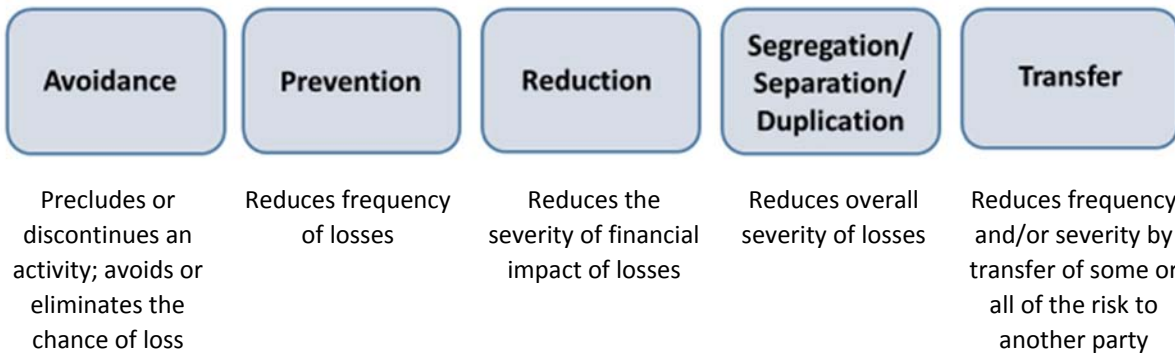
## Segregation/Separation/Duplication – reduces overall severity

1. **Segregation** – an isolation of an exposure from other exposures, perils, or hazards, e.g., having a dedicated computer room
2. **Separation** – the spread of exposures or activities over several locations
  - a. Divides a single asset or operation over two or more locations or activities
  - b. If one asset or operation suffers a loss, the other(s) must have sufficient capacity to meet the needs of all
3. **Duplication** – the use of backups for critical systems or operations
  - a. Duplicate asset or activity kept in reserve
  - b. Duplicate asset or activity not exposed to the same loss

## Transfer

1. Reduces frequency and severity of losses by transferring some or all of the risk to another party
2. **Physical transfer** – shifts some or all of an operational function or exposure to an outside source
3. **Contractual transfer** – shifts responsibility of certain liabilities to another party

## Risk Control Techniques



## Risk Control Technique Examples

### Avoidance

- Drug manufacturing company terminates the manufacturing of a medication due to its adverse side effects (bodily injury)
- Home builder ceases to purchase wooden trusses used in home construction from an international supplier due to the collapse exposure (defective product)
- Hoverboard manufacturing company ceases the sale and distribution of its highly popular hoverboard product line due to explosion hazard (faulty design)
- Produce grower recalls tomatoes from grocery store shelves due to listeria outbreak. (product contamination)
- Destination resort closes its beaches due to seasonal shark infestation endangering its guests
- Concert management company cancels a concert due to the threat of terrorism that could potentially injure thousands of patrons
- Restaurant chain ceases the sale of alcoholic beverages near college campuses
- Toy store discontinues importing and selling a popular wooden doll house painted with lead paint

### Prevention

- Long-haul trucking company hires expert driver training company to conduct comprehensive driver training of all drivers
- Highway construction company inspects and conducts maintenance checks of heavy equipment to ensure that it is operational and safe
- Fireworks manufacturing company labels products to thoroughly explain safe use and safety hazards
- 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
- Bread manufacturing plant installs sprinkler systems in all of their buildings



## Reduction

### Pre-loss reduction activities

- Retail strip center installs firewalls throughout buildings to reduce the spread of fire
- Candy wholesale distributor installs fire suppression equipment in their warehouses
- Youth hockey organization requires coaches and players to wear helmets with eye shields while on the ice

## Reduction

### Post-loss reduction activities

- Initiate a crisis management policy with emergency procedures in place for post-loss activities (evacuation plans, communication trees, securing property, etc.)
- Claims administration program is initiated to provide prompt response to accidents and incidents, early intervention, rapid claim closure, etc.

## Segregation/Separation/Duplication

### Segregation

- Computer room is designated as a high-risk exposure and is located on the bottom floor of the building with controlled access
- Spa manufacturing plant builds a storage building 500 yards away from the main manufacturing building to store flammable cleaning solvents (acetone)

### Separation

- School district decentralizes storage of its fleet of buses by setting up three separate garage locations in different parts of the city
- Appliance store splits unsold inventory between two separate warehouses 20 miles apart

### Duplication

- Heavy equipment leasing company keeps an inventory of spare parts in readiness for breakdown of equipment
- Organizations store duplicate copies of computer backups offsite
- Printing company enters into a mutual aid agreement with competitors to use one another's facilities in case of loss

## Transfer

### Physical Transfer

- Using a common carrier to distribute manufactured goods rather than buying trucks to transport products
- Organization leases employees rather than hiring employees
- Window distributor hires independent contractors to install windows rather than hiring employees

### Contractual Transfer – These will be discussed in detail Section III

- Hold harmless or indemnity agreements
- Exculpatory agreements
- Waivers of subrogation
- Limit of liability clauses

### Combination

- A combination of control techniques may be needed to address an exposure or activity
- Successful risk control programs incorporate all five risk control techniques or a combination of techniques

## Human Resources as an Exposure

In any organization, people pose the greatest risk. To control frequency and severity of losses, an organization must address all human resource exposures. This section will address some of the most frequent human resource-related control measures.

1. Health & Safety Programs
2. Ergonomic Risk Factors
3. Material Handling & Lifting
4. Substance Abuse
5. Workplace Violence

### **Learning Objective 4:**

List the root causes of accidents and injuries.

---

The root cause of accidents must be determined in order to effectively apply risk control techniques.

#### **Unsafe Acts or Behaviors**

1. Unsafe work is faster, more convenient, 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 risk of accident is low

Example: An employee attempts to change a light bulb while using a swivel chair instead of a ladder.

#### **Unsafe Conditions**

Example: Inadequate scaffolding for high-rise window washing collapses and causes the worker to fall multiple stories to his death.

## Uncontrollable Events

Example: A bridge collapses during an earthquake causing multiple injured drivers and damaged vehicles.

## Lack of Communication and Training

1. Never told, no reminders, no feedback
2. Lack of training, insufficient training, and unaware behavior was unsafe

Most unsafe behaviors and conditions are observed one or more times before an accident occurs. Behaviors and conditions left unchanged will eventually result in accident or injury.

Root cause analysis lays the foundation for preventing future accidents and injuries.

**Learning Objective 5:**  
Identify and apply the six basic steps of  
accident prevention.

---

*Listed in order of effectiveness, if implemented alone:*

**Eliminate the Hazard** – similar to the risk control technique of avoidance

**Substitute a Less Hazardous Substance or Process**

**Apply Engineering Controls** – physical modifications designed to reduce the potential for injury

**Utilize Administrative Controls** – rules or procedures that management undertakes to reduce the degree of or the potential for injury, i.e. safety meetings, job rotation, supervision, or safety rules

**Provide Effective Personal Protective Equipment**

**Train Employees** – Health and safety



## PRACTICE EXERCISE

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 under each step for actions you could take to prevent accidents.

**Eliminating the Hazard**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

**Substituting the Hazard**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

**Engineering Controls**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

**Administrative Controls**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

**Personal Protective Equipment**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

**Training**

- 1. \_\_\_\_\_
- 2. \_\_\_\_\_

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 OSHA standards.

**OSHA – Occupational Safety and Health Administration** – U.S. Department of Labor  
([www.osha.gov](http://www.osha.gov))

1. Develops industry standards
  - a. OSHA Employer’s General Duty Clause – “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.”
  - b. OSHA Employee Responsibility – “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.”
2. OSHA jurisdictions
  - a. Cover private sector employees
  - b. Excludes self-employed, family farmworkers, and government workers (except in State Plan states)
  - c. Approve and monitor 28 state plans which cover private and public-sector employees
  - d. Assist federal agency programs



### 3. OSHA enforcement

#### a. Inspections

- Conducted without advance notice
- On-site inspections or phone/fax investigations
- Use highly trained compliance officers

#### b. Inspection priorities

- Imminent danger/catastrophes/fatalities
- Worker complaints and referrals
- Targeted inspections, high injury/illness rates, severe violations
- Follow-up inspections

#### c. Citations and penalties

4. Recordkeeping and reporting
  - a. Required by OSHA to affirm compliance – OSHA Regulation 29 CFR 1904
  - b. Annual posting of a summary of injuries and illnesses for the prior year
  - c. Failure to document efforts to comply is treated the same as not undertaking the efforts
  - d. Records must be kept at least five years
  
5. OSHA consultation
  - a. Resource for safety program development
  - b. Occupational Safety and Health Consultation (OSHCON) program offers free and confidential services to help identify and control occupational hazards. In many states, OSHCON cannot issue citations.
  - c. Safety & Health Achievement Recognition Program (SHARP) – small business consultation (fewer than 250 onsite employees and fewer than 500 corporate-wide employees)
  - d. Voluntary Protection Program (VPP) – exempts employers who have implemented effective safety and health management systems and maintain low injury and illness rates below national averages from programmed inspections
  - e. Outreach Training Program – resources and grants for training and outreach

### Examples of Other Sources of Legislation

- Mine Safety Health Administration (MSHA)
- Department Of Transportation (DOT)
- State specific statutes, e.g., safety and workers compensation

## OTHER SAFETY-RELATED AGENCIES AND ORGANIZATIONS

<p style="text-align: center;"><b>National Institute for Occupational Safety and Health (NIOSH)</b></p> <ul style="list-style-type: none"> <li>• Certifies respiratory protective devices</li> <li>• Recommends occupational exposure limits for hazardous materials</li> <li>• Assists with research</li> </ul>	<p style="text-align: center;"><b>American Conference of Governmental Industrial Hygienists (ACGIH)</b></p> <ul style="list-style-type: none"> <li>• Publishes Threshold Limit Value (TLVs) guidelines</li> <li>• Recommends exposure limits for chemicals in the workplace</li> </ul>
<p style="text-align: center;"><b>American National Standards Institute (ANSI)</b></p> <ul style="list-style-type: none"> <li>• Sets personal protective equipment standards</li> <li>• Establishes consensus standards such as Reduction of Musculoskeletal Problems in Construction (ANSI/ASSE A10.40-2007)</li> </ul>	<p style="text-align: center;"><b>National Fire Protection Association (NFPA)</b></p> <ul style="list-style-type: none"> <li>• Promotes fire protection and prevention</li> <li>• NFPA 101 - Life Safety Code</li> <li>• NFPA 70E - Standard for Electrical Safety in the Workplace , adopted by OSHA as a consensus standard</li> </ul>
<p style="text-align: center;"><b>National Safety Council (NSC)</b></p> <ul style="list-style-type: none"> <li>• Statistics</li> <li>• Education</li> </ul>	<p style="text-align: center;"><b>Underwriters Laboratory (UL)</b></p> <ul style="list-style-type: none"> <li>• Standards</li> <li>• Testing</li> </ul>
<p style="text-align: center;"><b>International Safety- Related Agencies</b></p> <ul style="list-style-type: none"> <li>• EU-OSHA - European agency for safety and health at work</li> <li>• Mexico - Secretary of Labor and Social Welfare (STPS)</li> <li>• Canada - Canadian Centre for Occupational Health and Safety (CCOHS)</li> <li>• United Nations Economic Commission for Europe (UNECE) - Developed Globally Harmonized System (GHS) for classification and labelling of chemicals, vehicle regulations, transportation standards for dangerous goods and other agricultural and environmental standards adopted by 56 countries throughout Africa, the Asia-Pacific region and Latin America</li> </ul>	

**Learning Objective 6:**  
Identify and explain the elements of a  
health and safety program.

---

*Effective health and safety programs include the following elements:*

- A. Management Leadership
- B. Accountability, Responsibility, and Authority
- C. Employee Participation and Involvement
- D. Hazard Assessment and Control
- E. Employee Information and Training
- F. Accident Reporting, Investigation and Analysis
- G. Post-Injury Management
- H. Quality Control – Evaluation of Program Effectiveness

## **Management Leadership**

**Establishes a written health and safety policy statement** – signed by CEO or president

**Provides top management leadership and involvement** – management must “walk the walk” and integrate safety into business practices

**Establishes goals and objectives** – written program showing realistic and attainable safety policies and goals

**Assigns responsibilities and defines accountabilities** – of all levels of management, supervisors and employees

**Provides adequate authority, information, training, and resources** – to fulfill responsibilities

**Evaluates the effectiveness of the program**

## **Accountability, Responsibility, and Authority**

**Activity-oriented** (training meetings, newsletters, etc.)

**Results-oriented** (reduction in frequency and/or severity)

**Safety goals and objectives** – should be addressed in performance reviews

**Authority** – includes responsibility for safety issues for each position

**Individual accountability** – for actions, behaviors, and conditions

## **Employee Participation and Involvement**

*Program success requires:*

### **The establishment, implementation, and evaluation of the program**

#### **Safety committees**

*Safety committees, mandated by some states, should have:*

1. Organizational legitimacy or charter
2. Cross-departmental representation, including equal numbers of management and front-line employees
3. A chair who is not the safety manager or coordinator
4. Regular meetings with agenda and minutes maintained

#### **Safety inspections**

#### **Communication**

1. Between employer and employee
2. Ability to be involved in exposure assessment and control
3. Ability to report injuries, illness, occupational exposures, and recommend control methods without fear of recrimination
4. Prompt responses to reports and recommendations
5. Encouragement from management to participate in the program

## Reward vs. discipline

1. Reward, recognition and praise
  - a. Can be an incentive for safe employee behavior
  - b. Produces:
    - Extra effort toward risk control
    - High morale
2. Discipline
  - a. Should be fair and consistent
  - b. Used only as a last resort
  - c. Produces:
    - Minimal compliance
    - Low morale



## **Hazard Assessment and Control**

**Causes of accidents** – unsafe acts or behaviors, unsafe conditions, or uncontrollable events

### **Existence of unsafe behavior and conditions**

- Supervisors may have time to correct unsafe behaviors and conditions before an accident occurs

### **Systematic identification and assessment of workplace hazards**

1. Audits identify weak management practices
2. Inspections identify unsafe conditions and behaviors
3. Job Safety Analysis (JSA) or Job Hazard Analysis (JHA) identifies unsafe work methods
4. Behavior-based safety results identify unsafe acts
5. Incident reporting identifies unsafe acts, behaviors, conditions, work methods and management practices
6. Regulatory and consensus standards identify hazards and perils
7. Documentation – records of activity, exposures, and corrective action

## **Employee Information and Training**

### **Specific training for each exposure**

1. Nature of exposure and how to recognize
2. Employer control measures
3. Protective measures employee must follow
4. Provisions of applicable standards and regulations

### **When and how to train**

1. When
  - a. At hire, before initial job assignment
  - b. Periodically to maintain awareness and competency
  - c. Change in workplace injury exposure (new equipment, technology, arrangement of facility or equipment, etc.)
  - d. Change in job assignment
2. How
  - a. Formal meetings or training classes
  - b. Informal talks or regular reminders on the job

## **Accident Reporting, Investigation and Analysis**

**Investigate all accidents and incidents** that cause or could cause property damage or bodily injury, including OSHA recordable injuries, and/or first-aid cases.

### **Reasons for investigating accidents and incidents**

1. Identify causal factors involved in the incident and any needed changes in behavior or conditions
2. Reduce the potential for recurrence of similar incidents
3. Reduce employee and equipment downtime and expense

### **Conducting the investigation**

1. As soon as possible after the event
  - a. Visit and secure accident site, if possible; use photographs when an on-site investigation is not feasible
  - b. Facts are clearer and include more detail
  - c. Evidence and causal factors may still be present, and circumstances may be more apparent
  - d. Limits time for weather to affect evidence
  - e. Limits time for creating excuses and assigning blame

## 2. Investigators

- a. Supervisor – knowledge of job conditions and procedures and has primary responsibility for safety
- b. Employee – best account of accident, but may be biased to avoid discipline or maintain relationships
- c. Safety Committee (or Accident Review Committee) – unbiased search for cause
- d. Management – ultimate responsibility
- e. Outside authorities and OSHA – will investigate independently if accident results in a fatality or serious injury

## 3. Interviewing

- a. Potential interviewees
  - Those who saw events leading up to accident
  - Those who actually saw or were involved in event
  - Those who came to the scene immediately after event
  - Those who have information about work habits of injured employees or have knowledge about equipment involved in the accident

b. Witness perspectives

- Most witnesses are not trained observers – may see little and imagine the rest
- Personality and perspective may distort account
- Intentional misstatement to protect self or fellow employee

c. Guidelines

- Emphasis on fact-finding, not fault-finding, word questions carefully to get the information you need; conclude by emphasizing the need for prevention, not fault-finding
- Use open-ended questions that cannot be answered with a simple “yes” or “no”
- Ask for suggestions to prevent future incidents

**Report back to management**

1. Insight as to causation
2. Recommendations for prevention
3. Documented follow-up mechanism
4. Audit process

## **Benefits of a well-performed investigation**

1. Reduces or prevents accident/incident patterns, trends, and economic impact of accidents
2. Pinpoints safety program flaws to improve current job procedures and identify training needs
3. Shows concern and commitment to safety

## **Post-Injury Management**

### **Participants in the process**

1. Supervisor/managers
2. Human resources
3. Employee
4. Medical provider
5. Claims adjuster (claims management) and Workers Compensation carrier, if applicable

## Written policy and procedure

1. Ongoing employee training
  - a. Accident reporting procedures
  - b. Medical provider procedures
  - c. Modified duty procedures
2. Prompt reporting procedures to claim administrator/workers compensation carrier
3. Use of established medical providers
  - a. May be impacted by workers compensation system
  - b. Familiarity with operations
  - c. Directing or soft channeling
  - d. Treatment and return-to-work philosophy is compatible

4. Return-to-work
  - a. Restricted duty and job modifications, e.g. light duty, limited duty, etc.
  - b. Alternate duty – transfer to a job that meets medical restrictions
  - c. Resources available
    - Department of Labor return-to-work toolkit (<https://www.dol.gov/odep/return-to-work/>)
    - JAN Job Accommodation Network ([www.AskJAN.org](http://www.AskJAN.org))

### **Benefits of Post-Injury Management**

1. Reduces health care costs
2. Reduces workers compensation costs (Experience Modification Rate – EMR)
3. Reduces lost work time
4. Improves employee morale
5. Addresses legal issues (ADA, FMLA, etc.)





## PRACTICE EXERCISE

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?

A server burns her arm and hand while on the job. Until the burn is completely healed, she will not be able to carry any heavy trays. What job accommodations could be made for the server to return to work?

An assembly line worker in a manufacturing plant has a lower back injury. He is unable to sit or stand for long periods of time without taking a break. He has lifting restrictions in place and will be unable to operate certain pieces of equipment. What types of accommodations could be made for this employee?

## Quality Control – Evaluation of Program Effectiveness

### Affirm the program is effective and appropriate

1. Formal process
2. Use of internal and external resources

### Measurements

1. Insurance and information, such as credits/debits, experience modifiers, loss rates, and frequency/severity
2. OSHA or Bureau of Labor Statistics (BLS) incidence rates

- Total Recordable Injury Rate (TRIR) any work-related injury beyond first aid =

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

- Days Away and Risk 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 return-to-work phase =

$$\frac{\text{(# of cases of injury and illness with days away, restricted or transfer x 200,000*)}}{\text{\# of hours worked by all employees in a given year**}}$$

Note: DART is an acronym for Days Away from work, of Restricted duty, and days of job Transfer 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 rate to others.

\* 100 full-time equivalent workers or 100 workers × 40 hrs/wk × 50 weeks (number of weeks usually worked in a year)

\*\* Number of full-time equivalent workers × 40 hrs/wk × 50 weeks

3. Accident and injury trends and benchmarking
  - a. Frequency trends (causes, locations, etc.)
  - b. Severity trends (treatment costs, lost workdays, etc.)
  - c. Internal comparison over time
  - d. External comparison to similar organizations or BLS/OSHA rates

Bureau of Labor Statistics provides a calculator and comparison tool (<https://data.bls.gov/iirc/calculate.do>)

4. National Safety Council (NSC) statistics
5. Behavioral observations with documentation
6. OSHA citations and fines

In addition to health and safety, substance abuse and workplace violence, another important aspect in controlling the frequency and severity of losses an organization must address is ergonomics: A significant human resource exposure.

---

### **Learning Objective 7:**

Discuss the risk factors associated with ergonomics.

---

**Definition:** *Ergonomics is the applied science of designing and arranging equipment and the workplace to maximize productivity by reducing operator fatigue and discomfort. “The laws of work.”*

### **General Ergonomic Risk Factors**

1. Repetition
  - a. Performing the same motion every few seconds or the same task for hours at a time
  - b. Job task cycle time with inadequate recovery or rest periods
  - c. Injury types – Cumulative Trauma Disorder (CTD) and/or Repetitive Stress Injuries (RSI)
2. Excessive force/load
  - a. Lifting or pushing heavy loads
  - b. Isolating muscle groups when performing a task
  - c. Injury types – upper extremity and other muscle strains

3. Awkward or deviated posture (including reaching)
  - a. Deviations from the neutral position (body properly aligned, placing minimal stress on joints, muscles tendons and nerves) puts additional stress on the body
  - b. Extreme ranges of motion - Overhead and extended reaching also creates an awkward posture.
  - c. Injury types – Musculoskeletal Disorders (MSDs) such as carpal tunnel syndrome, sciatica, or tendonitis
4. Static load
  - a. Discomfort, tension, and fatigue is created by maintaining a constant posture or position during a physical exertion that stresses muscles and tendons
  - b. Common sources include using hands as a fixture (e.g., as a vice, clamp, or wrench) or standing in a fixed position
  - c. Injury types – Muscle strain and fatigue

5. Personal risk factors
  - a. Contributing factors such as physical conditions (hypermobile joints, diabetes, etc.), fitness, and outside activities
  - b. Improper work methods, physical or emotional stress make some individuals more prone to injury.
  - c. Increased frequency and severity of strain-related injuries
  
6. Environmental risk factors
  - a. Extreme temperature and vibration
  - b. Other environmental risks – loud noises, lighting, poor air quality, inappropriate equipment, etc.



## GENERAL ERGONOMIC RISK FACTORS

### REPETITION



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

### EXCESSIVE FORCE/ EXCESSIVE LOAD



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.

### AWKWARD OR DEVIATED POSTURE (INCLUDING REACHING)



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

### STATIC LOAD



Discomfort, tension, and fatigue is created by the physical exertion of maintaining a constant posture or position.

### PERSONAL RISK FACTORS



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

### ENVIRONMENTAL RISK FACTORS



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

Technology is now a common 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.

### **Common Issues Related to Prolonged Computer Usage**

1. Repetitive stress injuries – like carpal tunnel syndrome and texting thumb that lead to pain, numbness, stiffness, etc.
2. Vision problems – eye strain, dry eye, blurred vision, and Computer Vision Syndrome (CVS)
3. Headaches – caused by posture, vision strain, stress, etc.
4. Sedentary lifestyle – can lead to medical problems like obesity and deep vein thrombosis (blood clots due to immobility)
5. Musculoskeletal – stress on hands, shoulders, neck, back, legs
6. Fatigue and stress disorders – impact on behavior and emotions, work pressure, job environment
7. Sleep disorders – too much artificial light from computers and cell phones affect the bodies melatonin production and natural sleep/wake cycles



## Ergonomic Risk Control Measures for:

1. Repetitive tasks
  - a. Use automation, including robotics, when feasible
  - b. Job rotation (moving through different tasks)
  - c. Job enlargement (extension of job duties and responsibilities)
  - d. Work breaks (shorter, frequent breaks better than one long break)
2. Excessive force/load
  - a. Use mechanical aids when possible
  - b. Use large muscle groups when muscular force is required
3. Awkward or deviated posture
  - a. Workstation assessment
  - b. Design office workstation for proper posture with worker in mind
    - Use ergonomic chairs – adjustable for height, armrests, back angle, swivel seat and lumbar support
    - Keep joints at midpoint in range of motion (wrists straight, knees and elbows at 90-degree angles)
    - Use adjustable work stations – sit/stand desks, position of monitors
    - Use adjustable mouse and keyboard
  - c. Avoid vertical reach below the knees or above the shoulders

4. Static load
  - a. Use fixtures for holding instead of hands
  - b. Proper posture and workstation design
5. Personal risk factors
  - a. Stretching and strengthening exercises
  - b. Stress reduction measures and relaxation techniques
6. Environmental risk factors
  - a. Education
    - Recognition of risk factors
    - Proper work methods
    - Incident reporting procedures
  - b. Monitor work environment
  - c. Shock absorption to eliminate vibration
  - d. Noise control – noise absorbent materials, noise cancelling headphones, etc.
  - e. Adequate lighting and glare control – wattage of lights, screens, and shades



## PRACTICE EXERCISE

Here are some sample risk control measures that can be implemented to reduce ergonomic-related injuries in the workplace. Please place them in the chart next to their appropriate risk technique. Are there any others you would suggest?

Adjust chair, desk height, computer screen height, location of keyboard and mouse, etc.

Take mini breaks, rest your eyes, stretch and take a short walk.

Set time limits for screen time.

Avoid additional computer time outside of office hours.

Use of robotics for certain tasks.

Other?

Risk Control Techniques	Sample Risk Controls
Avoidance	
Prevention	
Reduction	
Segregation/Separation/Duplication	
Transfer	

## Learning Objective 8:

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

**Both Cumulative Trauma Disorder (CTD) and injuries from single events arise from manual material handling and lifting**

1. Low back strains and sprains
2. Shoulder strains and sprains
3. This exposure and these injuries ultimately lead to increased costs for workers compensation; medical coverage, lost wages, etc.

### Risk Factors

1. Frequency of lift or move
2. Load weight – the heavier the load the greater the force required to move or lift the material
3. Awkward posture – arises out of the shape and size of the load as well as the location of the load before the move and the location of the final placement of the load
4. Improper lifting techniques – NIOSH lifting equation

Frequency	Horizontal distance	Vertical distance
Travel distance	Asymmetry	Coupling strength

5. Personal risk factors – age, physical condition, mental condition, and physiology

## Risk Control Measures for Manual Material Handling and Lifting

1. Plan before the move or lift
2. Limit both frequency of move or lift and range of motion
3. Adhere to recommended maximum weight limits – using NIOSH Lifting Equation
4. Use mechanical aids – conveyors, hand trucks, robotics etc.
5. Redesign job – handle materials one time instead of three times, replace with lighter materials, outsource logistics and material handling operations, etc.
6. Implement job rotation
7. Consider additional risk control techniques – elimination, engineering, administration, substitution, training, personal protective equipment (back belts)

## Substance Abuse in the Workplace

The scope of substance abuse in the workplace is not limited to illegal drug use, it also includes prescription and over-the-counter medications. Additional risks may exist related to use outside of work, as well as former abuse.

### Commonly Abused Substances

Type of Drug	Number of People
Alcohol	17.7 mil
Marijuana	4.3 mil
Pain Relievers	2.06 mil
Cocaine	1.12 mil
Depressants	.76 mil
Heroin	.47 mil
Hallucinogens	.33 mil
Inhalants	.16 mil
<i>Source:</i> National Institute on Drug Abuse (NIDA) <a href="http://www.drugabuse.gov">http://www.drugabuse.gov</a>	

## Issues in the Workplace

Drug and alcohol use may cause a variety of impairments; such as altered judgment, reduced perception, lack of attention, loss of physical control, drowsiness, agitation, nervousness, and even hallucinations. These impairments can create problems across an organization.

### **Safety**

1. Increased number of accidents and injuries
2. Place other employees at risk

### **Productivity & Job Performance**

1. Absenteeism
2. Increased errors and reduced output

### **Morale**

1. Damaged relationships with co-workers
2. Management and other employees are affected

### **Theft and Violence**

### **Legal Liability**

1. Medical privacy concerns with use of prescribed medications
2. Providing a safe workplace
3. Regulatory compliance (Department of Transportation, OSHA, etc.)

## Implementing a Substance Abuse Program

Implementing a substance abuse program requires clearly stated policies and procedures.

### Testing

1. Clearly stated protocols – pre-employment, post-accident, reasonable suspicion/just-cause, random
2. Non-discriminatory

### Prevention

1. Substance abuse program training for managers and supervisors
2. Employee education
3. Employee Assistance Programs (EAP)
4. Provide short-term counseling, assessments and referrals
5. Provide health benefits for substance abuse disorders

### Disciplinary and Corrective Actions



## **Learning Objective 9:**

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

---

### **Benefits:**

1. Increased attendance and productivity
2. Fewer accidents and reduced workers compensation costs
3. Reduced number of employee-related crimes
4. Insurance premium credits and lower healthcare costs
5. Compliance with legislation – ADA guidelines, legalization of marijuana, etc.

### **Possible legal problems:**

1. Inadequate chain of custody of specimens or results of testing
2. Discrimination in testing or application of provisions (fit for duty)
3. Slander and defamation
4. Breach of confidentiality and breach of privacy
5. Failure to act (reasonable suspicion)
6. Inadequate recordkeeping
7. Illegal procedures

## Risk Control Techniques for Workplace Substance Abuse

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

**Learning Objective 10:**

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

---

**Sources of Workplace Violence**

1. Internal – employee against employee or employee against non-employee
2. External – non-employee against employee or non-employee against non-employee

**Possible Exposures**

1. Contact with public
2. Cash handling activities
3. Certain goods and services
4. Working alone, late at night, outside of normal business hours, in areas with poor visibility, or in high-crime areas
5. Emerging risks such as, cyberbullying, political unrest, active shooter, and open carry and concealed weapon laws

## **Risk Factors/Flags**

1. Drug or alcohol use
2. Fixation with weapons, frequent or graphic talk of violence, or violent acts
3. Social media activity – negative or threatening posts, pages followed, etc.
4. Instability (mental, financial, medical, familial, behavioral, etc.)
5. Insubordination
6. Employment issues: Long gaps between employment, inability to obtain references, or negative responses received

## **Risk Control Measures for Workplace Violence**

1. Physical controls – devices and construction techniques that prevent or reduce the likelihood of incidents
2. Hiring practices – thorough interview process including background checks, etc.
3. Administrative measures – written program including a statement of management commitment and employee involvement
4. Purchase workplace violence insurance policies
5. Training – emergency response procedures and ways to diffuse violent behavior
6. Program evaluation – to identify program deficiencies and to ensure compliance (OSHA)



## PRACTICE EXERCISE

***Read through the control measures below and discuss which type of risk control technique they might represent.***

Physical controls include alarms, metal detectors, video surveillance with continuous recording, shatterproof glass, enclosures and safe rooms, door locks, key-card systems, and identification badges, adequate lighting, and mirrors in blind walkways.

Hiring practices include thorough job interviews, reference checks, identity and criminal background checks, verification of employment history and credentials, cognitive testing, and pre-hire drug tests.

Administrative measures include a written program, a zero-tolerance for violence statement, an anti-retaliation policy, a prompt reporting process with comprehensive investigation, a mechanism for anonymous reporting, proper recordkeeping, commitment to adequate security, site access control procedures, liaison relationships with police and other first responders, escorts to remote parking, and a buddy system for employees working in isolated areas.

Training should be conducted on identification of risk factors and early recognition of possible violent behavior, emergency response procedures, ways to diffuse violent behavior before it escalates, and the location and operation of automatic locking devices and safe rooms.

Program evaluation includes a thorough review of OSHA compliance, medical and incident records, worksite assessments, employee reports, surveys and questionnaires, and a record of training activities.

Risk Control Techniques
Avoidance
Prevention
Reduction
Segregation/Separation/Duplication
Transfer

## **Possible Legal and Financial Problems with Workplace Violence**

1. Employer may be held legally liable for actual damages, pain and suffering and punitive damages
2. Negligent hiring claims due to lack of documentation of thorough pre-employment screenings (Fair Credit Reporting Act, ADA, criminal background checks, etc.)
3. Workers compensation claims for injuries from on-the-job violence
4. Negligence claims for lack of safety training and security procedures
5. Impact of workplace violence on insurance costs

## **Emerging Risks Related to Workplace Violence**

1. Cyber-bullying
2. Political unrest
3. Open carry and concealed weapon laws
4. Active shooter situations

## Review Of Learning Objectives

1. Define risk control and describe its purpose and scope.
2. Know the reasons why organizations should focus on risk control.
3. Identify and apply the five primary types of risk control techniques to a scenario.
4. List the root causes of accidents and injuries.
5. Identify and apply the six basic steps of accident prevention.
6. Identify and explain the elements of a health and safety program.
7. Discuss the risk factors associated with ergonomics.
8. Identify the risk factors and risk control measures associated with manual material handling and lifting.
9. Describe the benefits and possible legal problems associated with a workplace substance abuse program.
10. Name the risk factors and risk control measures used to prevent or reduce workplace violence.







# Certified Risk Managers

*a proud member of The National Alliance for Insurance Education & Research*

## Section 2

# **Risk Control and Mitigation - Property & Liability**



[Key Terms](#)



## Risk Control & Mitigation - Property and Liability

### Learning Objectives

1. List the common sources of employment practices liability exposures.
2. Identify and describe risk control measures to treat common sources of employment practices liability exposures.
3. Identify the common types of fleet exposures and hazards.
4. Identify administrative controls used to handle fleet exposures.
5. List and gives examples of controls for hazards related to walking surfaces.
6. Identify and describe the key property exposure terms.

7. Name the hazard controls programs related to property.
8. Describe the common business applications using technology that create a cyber exposure.
9. List and describe cyber risk exposures created by e-business or cyber activities.
10. Know the considerations related to cyber risk insurance.
11. List and explain the four types of contractual transfer.
12. Identify the three types of hold harmless agreements.

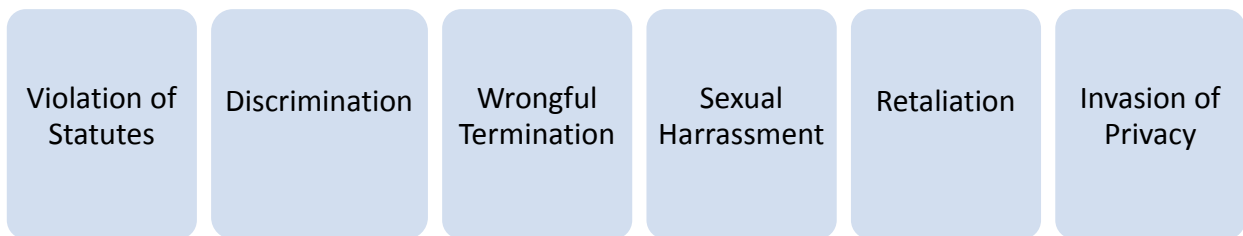
---

### **Learning Objective 1:**

List the common sources of employment practices liability exposures.

---

Common sources of employment practices liability exposures:



1. Violation of statutes
2. Discrimination
3. Wrongful termination
4. Sexual harassment
5. Retaliation
6. Invasion of privacy

**Note:**

In depth discussion of statutes is beyond the scope of this course. Further, the goal of reviewing these laws is not to apply the laws to the named insured or the named insured's workplace but to understand the exposure to which EPLI may apply.

**Violation of Statues** – (statutory liability) widely ranging federal, state and local laws protecting the rights of individuals

Agencies at every level of government are tasked with investigation, evaluation, and adjudication of complaints regarding employment practices and the protection of rights.

1. US Equal Employment Opportunity Commission (EEOC) – federal agency that administers and enforces civil rights laws against workplace discrimination
2. US Department of Labor (DOL) – federal agency that fosters, promotes, and develops the welfare of wage earners, job seekers, and retirees
3. Fair Employment Practices Agencies (FEPAs) – state and local agencies who work with the US and state EEOC to enforce federal requirements
4. Civil Rights Act of 1964 – prohibits discrimination in employment based on race, color, religion, sex or natural origin
5. Family and Medical Leave Act of 1993 (FMLA) – entitles eligible employees to take unpaid, job-protected leave for specified family and medical reasons with continued health benefits

- 6. Americans with Disability Act of 1990 (ADA) – prohibits employment discrimination on the basis of disability in hiring, including all terms, conditions and privileges of employment. It guarantees that people with disabilities enjoy equal employment opportunities.

The ADA of 1990 requires employers to fully understand the following definitions:

<p><b>Disability:</b> a physical or mental impairment that substantially limits one or more major life activities, a person who has a history or record of such an impairment, or a person who is perceived by others as having such an impairment.</p>
<p><b>Physical or Mental Impairment:</b> any physiological, mental, physical, or psychological disorder or condition that limits “substantially limits” one or more major life activities or operation of a major bodily function which may include but, are not limited to: neurological issues, inability to care for oneself, performing manual tasks, walking, etc.</p>
<p><b>Reasonable Accommodation:</b> any modification or adjustment to an 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.</p> <p><b>Note:</b> An employer has an affirmative obligation to make a “reasonable accommodation” for a disabled applicant or employee unless the employer demonstrates that doing so would be an “undue hardship”.</p>
<p><b>Disparate Impact:</b> indirect discrimination resulting from a neutral employment practice that has an otherwise adverse impact on individuals within a protected class. For example, a written test, educational requirements, height and weight requirements, etc.</p>

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

7. Court decisions – local, state, federal, including appellate and supreme court

Example:

Young vs. United Parcel Service (March 25, 2015) – case amended the definition of “sex discrimination” in Title VII of the Civil Rights of 1978 to include pregnancy

8. International Liability, Standards, and Regulations

- International Labor Standards – establishes a worldwide minimum level of protection from inhumane labor practices (workplace discrimination, bullying, workplace violence, gender inequality)
- International Labour Organization – codifies, implements, and enforces international labor laws
- World Trade Organization – enforces international labor laws through trade sanctions

**Discrimination** – federal and state laws prohibit discrimination

1. Based on race, religion, color, sex, pregnancy, national origin, ethnicity, ancestry, citizenship, disability, military service, AIDS and HIV status, genetic information and age
2. Based on familial status, marital status, domestic partnership status, sexual orientation, blood trait, liability for military service, etc.
3. Categories of prohibited discrimination
  - Individual discriminatory treatment – an individual is treated differently from other similarly situated persons because of that individual’s protected status
  - Group discriminatory treatment – a protected group is adversely impacted by an organization’s policy or practice that may be neutral on its face but has the effect in practice of adversely impacting the group (disparate impact)



**Sexual harassment** – submission to or rejection of unwelcome sexual conduct by an individual used as a basis for employment decisions affecting an individual

1. Occurs in a variety of circumstances
  - a. Victim or harasser may be male or female and does not have to be of the opposite sex
  - b. Harasser can be the victim's supervisor, an agent or client of the employer, supervisor in another area, a co-worker, or a non-employee
  - c. Victim could be anyone affected by the offensive conduct (does not have to be the victim harassed)
  - d. An organization may be held vicariously liable for conduct taking place within the organization of which it is completely unaware, or which is a random act, including acts committed by non-employees
  - e. Unlawful sexual harassment may occur without economic injury to or discharge of the victim
2. Common characteristics of sexual harassment
  - a. Overt harassment – overt, visible behaviors that frequently involve unwanted physical contact are viewed as “quid pro quo” (“this for that”) or “crossing the line” which is often difficult to clearly define
  - b. Hostile or uncomfortable work environment – unwelcome sexual conduct, overt, or passive, which has the effect of unreasonably interfering with an individual's work or performance and creating an intimidating, hostile, or offensive working environment
  - c. A single event, such as a joke, remark, cartoon, or photo, etc. that may be sexually offensive to one person in a group and not be offensive to everyone in the group does not constitute a hostile workplace sexual harassment situation

**Wrongful termination, wrongful discharge, wrongful dismissal** – arises when an employee’s contract of employment is terminated by the employer and the termination breaches one or more terms of the employment relationship or an employment law

1. Employment contracts can be written, oral, or a combination of both
2. Employment-at-will does not apply if an impermissible or discriminatory motive for discharge can be established
3. Precedent, what an employer does in practice, outweighs written policy; consistency matters
4. Remedies for a proven wrongful termination
  - Reinstatement of the dismissed employee
  - Monetary compensation – wages, commissions, bonuses, profit sharing, etc., the employee would have earned
  - Penalties – dependent on the offense committed
  - May vary by jurisdiction

**Retaliation** – the organization’s management or other employees retaliate against an employee who files a complaint, grievance, or lawsuit related to an employment practice

1. Retaliation is intentional therefore, settlements are more costly than the original EPLI allegation
2. Examples:
  - Transferring the employee to a less desirable position
  - Verbal or physical abuse
  - Increased scrutiny
  - Less favorable performance evaluation

**Invasion of Privacy** – violation of the employee’s right to privacy

1. Electronic surveillance monitoring issues – use of cameras, phone recordings, smart security, etc. There is a fine line between the employer’s right to protect buildings, office equipment, etc. and the employee’s privacy rights in the workplace
2. Examples:
  - Inappropriate access and actions taken in response to an employee’s personal emails, Facebook account, text messages or other social media
  - Release of an employee’s or job applicant’s personal or private information

### **Learning Objective 2:**

Identify and describe risk control measures to treat common sources of employment practices liability exposures.

---

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

#### **Establish policies and procedures that are:**

1. Addressing all applicable laws
2. Communicated to all personnel, clearly understood and universally applied; not adhering to a policy is worse than not having a policy
3. Constantly reiterated and supported by management through written statements, meetings and by its own conduct
4. Followed and compliance is verified
  - Employee questionnaires, “hot lines,” blind surveys, open door policies and review of complaints
  - Managing by walking around
  - Retaining objective and confidential written records on all personnel, with a periodic review of those records

## Hiring Practices

The organization must establish a written hiring and recruiting process that is clearly defined and consistent in practice.

1. Care must be taken in the design and use of employment documents – job postings, position descriptions, applications, the interview process, background checks, job offers, and the employee handbook
2. Avoid discussing discriminatory subjects in interviews and discussions with employees – age, marital status, ethnicity, religion, nationality, disabilities, etc.
3. Properly train managers and supervisors, to include:
  - Employment laws and employment practices exposures
  - Supervisor and management training – interviewing, hiring, and conducting performance evaluations, firings, etc.
  - Handling disciplinary issues
  - Harassment prevention and control measures – education and training, learning to identify the exposures

## Manage Employee Turnover

Establish a strong organizational culture and atmosphere in which employees are motivated, engaged, loyal, and aligned in achieving the organization’s vision, mission, and goals.

## **The Risk Manager's Role**

The risk manager must ensure that proper resources are assigned to conduct a prompt, complete, and documented response to all allegations or grievances. The risk manager is a recorder of the facts and must be objective and not act as the judge.

1. Disciplinary action must be appropriate to the individual situation and consistent with action taken in previous situations involving substantially the same set of facts
2. Thoroughly document everything, including training, communication and management support

## **Employment Practices Insurance Considerations**

### Employment Practices Liability Insurance (EPLI) Policies

1. Insurance Service Office (ISO) EPLI form is available, but most EPLI Policies are written on non-standard, non-ISO forms
2. Key elements of the Insuring Agreement of EPLI policies – most are written to provide coverage for claims filed by employees (or job applicants) against the organization because of an employment-related incident
3. Policy language and conditions vary by policy however, they typically are written on a claims-made basis and include coverage for judgements/settlements, pre- and post-judgment interest, and other items. Coverage for punitive damages may be included as determined by state statute.
4. Separate coverage may be available for claims filed by third parties such as individuals that the business or business' employees have contact with such as vendors, independent contractors, volunteers, volunteers or other non-employees

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). In order to properly utilize specific risk control techniques, the type of fleet must be determined.

**Common Types of Fleets** – Fleets vary by the type and nature of use of the vehicles (service, retail, commercial)

1. Long-distance cargo transportation (owned goods of others) – large vehicles with longer trips; trucks, tractor-trailers, trailers
2. Service and delivery – smaller vehicles used for intermediate and scheduled routes; pickup trucks, vans
3. Private passenger – not used to transport goods or services (used by sales personnel, taxis)
4. Buses, vans, shuttles – transport high numbers of passengers; livery vehicles
5. Non-owned vehicles of any type – rented or owned by others

### **Learning Objective 3:**

Identify the common types of fleet exposures and hazards.

---

#### **Drivers**

1. Driving history and experience
2. Physical condition and ability to operate a vehicle
3. Safety orientation and training – observance of traffic safety laws

#### **Impaired Driving**

1. Distracted driving
  - Cell phone use – hands free or handheld (calls, texting, emails, reading, playing games, etc.)
  - Operating navigation systems/maps, sound systems, climate controls, etc.
2. Under the influence of drugs and/or alcohol, etc.
3. Fatigue



## Vehicle

1. Size and value
  - Larger vehicles may be more hazardous than smaller ones – the weight of a fully loaded extra heavy truck will have a greater physical impact with high potential for damage
  - Smaller vehicles have a greater potential for passenger injuries when involved in a collision with a larger vehicle
  - Customized equipment and additional attached equipment – mechanized lifts, booms, etc.
2. Number of vehicles – on the road exposure for the operation of multiple vehicles at one time and the concentration of vehicle property values at the garage location
3. Vehicle maintenance and condition
4. Loss of use of vehicles – physical damage to key vehicles or the entire fleet

## Cargo Exposures

1. Type of cargo – hazardous chemicals, livestock, flammables, etc.
2. Theft, vandalism, physical damage
3. Value of the cargo – high value property, replacement cost, contractual obligations for damaged property, etc.

## **Routes and Traffic**

1. Radius of use
2. Traffic patterns (urban, rural, highways, congestion)
3. Long-haul routes (miles driven, more time on road)
4. Scheduled or on-demand deliveries

## **Unsafe Road Conditions**

1. Weather-related – flooding, snow, ice, etc.
2. Construction activities – road maintenance, lane closures, detours, etc.
3. Other unexpected conditions – sinkholes, potholes, poor signage, objects in roadway, etc.

## Fleet Risk Categories, Exposures, and Hazards

<i>Risk Category</i>	<i>Risk Exposure</i>	<i>Hazard</i>	<i>Result</i>
<b>Property</b>	<b>Unsafe Road Conditions</b>	Garbage truck overturns when it hydroplanes due to wet and slick roads (Business Auto Physical Damage)	Physical Damage to the Owned Vehicle
	<b>Cargo</b>	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
<b>Liability</b>	<b>Impaired Driving</b>	Due to long hours behind the wheel, the driver falls asleep, veers off the road and causes a collision with another vehicle injuring its passengers (Business Auto Liability)	Injury or Harm to Third Parties
	<b>Poor Vehicle Maintenance</b>	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
<b>Human Resources</b>	<b>Routes and Traffic</b>	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
	<b>Drivers</b>	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
<b>Net Income</b>	<b>Loss of Use</b>	Rental car company shuts down operations due to hurricane damage to all its rental car fleet	Physical Damage and Loss of Rental Income
	<b>Vehicle Value</b>	Manufacturer recall on high value vehicles with specialized equipment installed	Increased cost to secure replacement vehicles

## **Auto Liability**

1. Bodily injury and property damage coverage – for injuries to third parties and/or for damage to the property of others (vehicles, building, etc.)
2. Negligent entrustment – if an owner of a vehicle is found to have negligently entrusted a vehicle to a driver who caused an accident, he may be liable for compensatory damages and pain and suffering

## **Auto Physical Damage**

1. Collision damage to vehicle/trailer – with another vehicle, object, or thing
2. Damage Other Than Collision (Comprehensive Coverage) – theft, vandalism, fire, wind, flood, hitting an animal, falling objects, etc.

## **Hired and Non-Owned Liability and Physical Damage**

**Cargo** – damages or losses to freight in transit

**Workers Compensation** – Injury to employed driver and passengers within their scope of work

### **Driver rules**

1. License requirements – Commercial Driver’s License (CDL)
2. Hours of service or operation recordkeeping
3. Drug and alcohol laws

### **Vehicle Requirements**

1. Roadside inspections for safety, cargo, and weight limits
2. Maintenance recordkeeping
3. Vehicle marking/signage requirements

### **Penalties for Non-Compliance**

1. Fines
2. Removal from service or operation
3. Typically administered by state police, Department of Public Safety officers, Department of Transportation (DOT) (both state and federal)

The FMCSA is within the Department of Transportation and provides regulation for the trucking industry. The FMCSA outlines requirements for:

### **Driver qualifications and training requirements**

**Hours of service** – e.g. 11-hour driving limit after 10-hour break, 60/70-hour limit in 7/8 consecutive day period

### **Routing regulations and interstate operations**

### **Cargo rules**

### **Hazardous material restrictions**

---

### **Learning Objective 4:**

Identify administrative controls used to handle fleet exposures.

---

There are several hazard and administrative controls that can be used to prevent or lessen the impact of fleet accidents. Because the physical condition of the fleet can be as much a factor in accident prevention as safe operation of the vehicles, hazard control mingles with administrative control of fleet risks.

#### **Fleet Safety Policy**

1. Management policy statement – outlines driver responsibility and accountability
  - a. Authority to drive
  - b. Rules and regulations – a company may have more restrictive regulations than those set forth by the federal or state government
2. Drug and alcohol policy
3. Vehicle responsibility
4. Vehicle inspection and maintenance program

#### **Driver Qualifications**

1. Employment applicant vs. existing driver
2. Valid driver's license for class of vehicle
3. Written criteria for "qualified driver" status; e.g. acceptable driving record criteria, number of years experience, etc.
4. Commercial Driver Pre-employment Screening Program (PSP) – Federal Motor Carrier Safety Administration (FMCSA) sets forth general qualifications of drivers as well as maintaining records detailing driver crash and inspection history

## **Driver Evaluations**

1. Driver meetings – supervisors and drivers meet to discuss news and issues
2. Driver performance reviews – periodic, structured reviews by supervisors
3. On-road performance evaluations – supervisors ride along to monitor driver performance and assess whether procedures are being followed
4. Commercial driver recordkeeping and documentation (driver files)
5. Point systems – internal method for monitoring driver performance
6. Disciplinary procedures

## **Driver Training**

1. New driver orientation
2. Driver training specific to the type of vehicle driven – tractor-trailer rigs, buses, heavy load units, cement mixer trucks, etc.
3. Defensive driving
4. Commercial driver rules and regulations
5. Specific areas of awareness/exposure – cold weather driving, hazardous materials, distracted driving, etc.

## **Vehicle Inspection and Maintenance Program**

1. Pre-trip/on-the-road/post-trip inspections
2. Scheduled preventive maintenance
3. Documented corrective action



## Response to Accidents

1. Rules for reporting
2. Investigation forms/procedures
3. Trending of accidents
4. Accident review committees – tasked with determining what can be done to prevent similar future accidents

## Monitoring and Surveillance

1. Telematic devices electronically monitoring performance
  - a. GPS technology
  - b. Real-time monitoring of in-vehicle operations – speeds, hard braking, routing, etc.
  - c. Dash cameras
  - d. Identify areas for improvement – real-time driver coaching, alerts for driver behavior
  - e. Improve fuel-efficiency – monitoring speeds, idle times, etc.
  - f. Decrease overall expenses – maintenance, repair, reduce wear and tear
2. Public reporting – bumper stickers
3. Commercial vehicle driver Electronic Logging Devices (ELD) – track driver hours of service and driving time

## Top 10 Causes of Accidents

source: Department of Transportation

<https://www.transportation.gov>

The Driver	The Vehicle	Other Events
<ol style="list-style-type: none"> <li>1. Driver fatigue</li> <li>2. Rear-end a stopped vehicle</li> <li>3. Driving off the side of the road</li> <li>4. Speeding</li> <li>5. Loss of control</li> <li>6. Lane drifting</li> </ol>	<ol style="list-style-type: none"> <li>7. Mechanical failure</li> <li>8. Shifting cargo</li> </ol>	<ol style="list-style-type: none"> <li>9. Debris on the road</li> <li>10. Poor road conditions due to bad weather or maintenance</li> </ol>

## Sample Risk Controls

Avoidance	<ul style="list-style-type: none"> <li>• Not hiring the driver with DUI violations</li> <li>• Limiting radius of operations to 200 mi. from garage locations</li> </ul>
Prevention	<ul style="list-style-type: none"> <li>• Use of tracking devices to minimize driver fatigue</li> <li>• Regularly scheduled maintenance and inspections</li> </ul>
Reduction	<ul style="list-style-type: none"> <li>• Use of seat belts</li> <li>• GPS device use</li> </ul>
Segregation/Separation/Duplication	<ul style="list-style-type: none"> <li>• Separation of fleets into multiple garage locations</li> <li>• Designate backup vehicles for key vehicles so there is no disruption to operations should they be unavailable due to repair or need to be replaced</li> </ul>
Transfer	<ul style="list-style-type: none"> <li>• Purchase physical damage insurance with a \$1,000 Comprehensive deductible</li> <li>• Contract trucking company to transport goods to designated locations</li> </ul>

---

### **Learning Objective 5:**

List and give examples of controls for hazards related to walking surfaces.

---

Slips, trips, and falls are the leading sources of injuries to employees and the public.

#### **Exposure assessment**

1. Self-inspection
2. Incident/accident investigation

#### **Hazard exposures and controls**

1. Surface materials – high, moderate, or slight hazard
  - a. Avoid or replace slippery surfaces with slip resistant material
  - b. Reduce slip exposure by wearing slip-resistant footwear
  - c. Increase surface coefficient of friction with cleaning and maintenance or non-slip strips
  - d. Utilize entrance runners for water and snow
2. Surface continuity
  - a. Anticipated walking surface continuity
  - b. Repair holes and cracks
  - c. Eliminate raised edges
  - d. Housekeeping

3. Illumination and visibility
  - a. Minimum standards – depending on location, e.g. stairs, warehouse (measured in foot candles or lumens)
  - b. Floor markings in walkways and work areas
  
4. Stair design
  - a. Maintain standard width and height of risers
  - b. Avoid steep stairways (greater than 40% elevation)
  - c. Visible or contrasting color
  - d. Nonslip surface
  - e. Handrails
  
5. Spill control
  - a. Warning signs
  - b. Immediate clean-up
  - c. Floor gutters and drains

6. Maintenance and inspection
  - a. Building and equipment (e.g. leaks)
  - b. Planning and capital budgeting (e.g. carpeting)
  - c. Documented procedures and records
  - d. Trained staff in hazard recognition
  - e. Work order system for repairs
  
7. Insurance considerations
  - a. Slips, trips and falls lead to claims
  - b. Financial impacts on Workers Compensation and Commercial General Liability insurance

### **Learning Objective 6:**

Identify and describe the key property exposure terms.

---

#### **COPE**

1. **Construction** – the material used to construct the building
  - a. Frame
  - b. Joisted masonry
  - c. Non-combustible
  - d. Masonry non-combustible
  - e. Modified fire resistive
  - f. Fire resistive
  
2. **Occupancy** – the occupants or operations in the building
  - a. Plastic storage
  - b. Aerosols and flammables in plastic containers

Examples:  
residential, office, restaurant, manufacturing, etc.

3. **Protection** – safeguards, equipment, and measures provided by the building owner or occupant to minimize hazards

Examples:

automatic sprinkler systems, fire and smoke alarms, fire doors, fire walls/curtains, special hazards protection – gaseous suppression (computer rooms) and automatic shutoffs (flammable liquids and ventilation systems), fire brigades, housekeeping, etc.

4. **Exposures** – sources of potential damage external to the building

Examples:

fire – proximity to other structures or activities, brush; explosion – nearby chemicals plants, gas lines; natural perils – flood plain, earthquake fault line, etc.

**Maximum Possible Loss (MPL)** – amount subject to loss; total value at risk at a single location regardless of protective measures; amount subject is limited only by adequate separation between structures

**Probable Maximum Loss (PML)** – amount of loss expected from a specific peril given some level of impairment or delay in protection (definition varies by insurance carrier); PML is expressed as a percentage of the total values; unless noted, PML refers to the peril of fire

## Exposures to Loss

1. Human perils – those caused by human activity; e.g., electrical fire, theft
2. Economic perils – those caused by general economic activity; e.g., property damage to supplier or customer that causes you an economic loss, loss of market, delays in transportation
3. Natural perils – those caused by natural forces; e.g., wind, hail, flood, lightning
4. Factors affecting exposures to loss
  - a. Geographic location
  - b. Building and equipment maintenance
  - c. Storage practices
  - d. Special hazards of occupancies and exposures; e.g., welding, cooking, cutting



---

### **Learning Objective 7:**

Name the hazard control programs related to property.

---

#### **Management Programs**

1. Facility inspections
2. Housekeeping
3. Facility maintenance
4. Special hazard policies

#### **Fire Protection Services**

1. Internal – fire brigades
2. External – fire departments
  - a. Protection class – proximity to service, water, access
  - b. Volunteer vs. full time
  - c. Capabilities in equipment and personnel

#### **Automatic Sprinkler System**

1. Design density specific to occupancy
2. Water supply pressure and flow rate
3. Maintenance procedures
4. Impairment procedures

## **Fire Alarm System**

1. Central station versus local alarm
2. Smoke detection
3. Heat detection
4. Water flow detection

## **Security Protection**

1. Physical barriers such as safes, locks, bars, bulletproof glass, etc.
2. Lighting
3. Alarm systems
  - a. Local
  - b. Central station

Almost all organization use technology to conduct business, and cyber risk continues to evolve and emerge as one of the top ten global risks for business entities. The ever-increasing number of cyber-attacks and breaches threatens to have an adverse impact on the financial assets of these organizations and emphasizes the need to control cyber risk exposures.

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, smart phones, smart watches, the Internet of Things (IoT) and third-party locations such as the Cloud.



### **Learning Objective 8:**

Describe the common business applications using technology that create a cyber exposure.

---

#### **Data collection and storage**

1. Use of virtual server resources (i.e. “the Cloud”) for data storage, backup and management (paperless world)
2. Shared private networks connected through the internet or other electronic business systems
3. Collection of private and highly sensitive information on employees, clients, vendors, etc.; e.g., medical information including patient data, research data for individuals

#### **Business transactions**

1. Downloading information and digital applications
2. Purchasing of goods and services, document transfers, and contract bidding
3. Conducting webinars, meetings and training

## **E-commerce**

1. Online payment card industry (PCI) protocols
2. Electronic purchasing and payments using electronic bank transfers, credit and debit cards, Bitcoin, Google Wallet, PayPal
3. Electronic advertisements

## **Communications**

1. Emails
2. Websites
3. Social media presence; including bulletin boards, blogs, forums and any communication done through these channels

## **Electronic publishing**

**Internet of Things (IoT)** – devices with communications systems and transmitting chips – e.g. smart home devices and applications

### **Learning Objective 9:**

List and describe cyber risk exposures created by e-business or cyber activities.

---

#### **“First Party” Cyber Risk**

1. Impact on the organization
  - a. The possible reduction in value of an organization’s stored data – records, research and development, pricing strategies, or strategic plans
  - b. Costs incurred to collect, manage, analyze and store data, and to respond to an unauthorized breach of data security
2. Common “first party” cyber risks
  - a. Breach or loss of data
  - b. Breach or loss of proprietary information and trademark infringement
  - c. Unauthorized use of technology resources

#### **“Business Interruption” or “Net Income” Cyber Risk**

1. Impact on the organization – the organization can suffer a loss of revenue, a reduction or complete interruption of business, and may have increased expenses to stay in business
2. Common “business interruption” or “net income” cyber risks
  - a. Denial of service attacks and system corruption resulting in loss of service
  - b. Harm to brand and reputation
  - c. Loss of credibility and trustworthiness
  - d. Hardware taken out of service by law enforcement (for investigation)

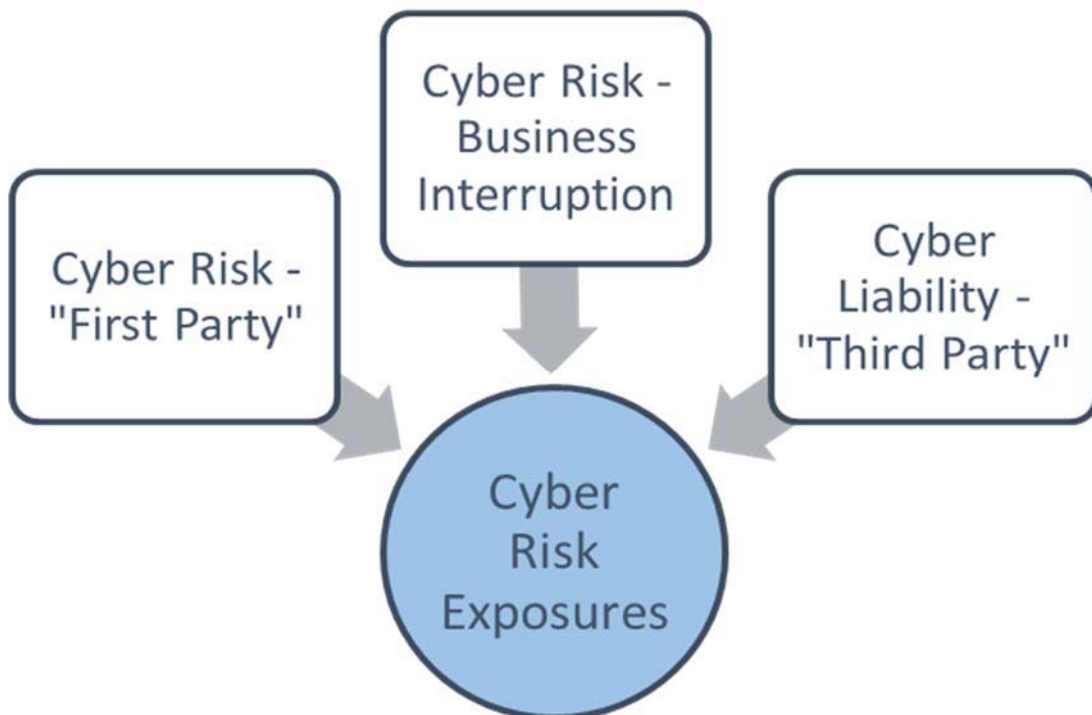
## “Third Party” Cyber Liability Risk

1. Impact on the organization – when the data stored on an organization’s computer is “personal data” belonging to an outside party or parties, the organization has a duty to protect that party from harm and a breach of that duty
  
2. “Personal data” is any information that can be used to distinguish or trace an individual’s identity, such as:
  - a. Name, social security number, date and place of birth, mother’s maiden name, or biometric records;
  
  - and**
  
  - b. Any other information that is linked or linkable to an individual; such as medical, educational, and employment information
  
  - c. Any financial data; such as account numbers, credit card numbers, security codes, etc.
  
3. Common “third party” cyber liability risks
  - a. Breach of personal data
  
  - b. Unintended transmission of a malicious code or virus
  
  - c. Copyright violations
  
  - d. Other protected rights violations
  
  - e. Personal injury – libel, defamation, etc.
  
  - f. Contractual performance
  
  - g. Unauthorized actions of employees can create liability, as well as compliance failures

4. Cyber liability breach of duty exposures for inadequate security of data
  - a. Unauthorized disclosure of customer personal data
  - b. Failure to provide secure transactions that comply with PCI (payment card industry) protocols
  - c. Failure to prevent or react to unauthorized intrusions to the data, including non-compliance with breach notification statutes
  - d. Failure to protect web-based storage and databases from unauthorized access and distribution
  - e. Failure to exhibit "due diligence" in development and implementation of new applications, systems, procedures, etc.

**Note:**

Courts are reluctant to limit liability for a client if they fail to provide adequate security controls.





## Cyber Risks That Could Lead to a Loss

Type of Cyber Risk	Examples
<b>First Party</b>	Insufficient security system allows for 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
	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 guest personal information, the reputation of an international resort is damaged and reservation numbers are down
	A business is required to take down their website due to copyright infringement for using unauthorized images
	A cyber-criminal hacks a smart home security system causing it to malfunction therefore resulting in loss of income 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 that 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 that contains a virus to their company’s client list

Sound risk control measures begin with risk identification and analysis to characterize the organization's cyber exposures, hazards, and potential perils that threaten the organization.

### **Cyber Risk Identification Measures**

1. Perform a cyber security 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
3. Advise management of the scope of the organization's cyber exposure and associated regulatory obligations
4. The risk manager should continuously communicate with the information security department and top management regarding cyber risks

### **Cyber Risk Control Techniques**

All five risk control techniques – avoidance, prevention, reduction, segregation/separation/duplication, and transfer will be used to control cyber risk. Avoidance, prevention, and segregation are the most often used.

1. Avoidance – Unless it is critical to the organization, personal data should not be stored on any computer that can be accessed from another source. If the data is not stored, it cannot be stolen or corrupted from an external source.
2. Separation/segregation/duplication – Perform regular backups of all important files and store them on separate storage devices and in locked containers.

### 3. Prevention

#### a. Design a cyber risk and security program

- Assign a cyber risk or information security manager or department
- Protect electronically stored information, networks, and computer systems
- Adopt policies to ensure compliance with cyber risk controls; use compliance audits and corrective actions
- Ensure that core systems are protected with multi-factor authentication

#### b. Establish protocols

- For collection, storage, access, dissemination and protection of electronically stored information
- For encryption – determine what data must be encrypted for storage and/or transmission of any type
- Implement minimum data security, encryption, and access policies for mobile devices

#### c. Protect the system hardware and media

- Require users to turn off or log out of computers when not in use
- Hardware and media slated for disposal or recycling should be reformatted or physically destroyed
- Ensure current versions of software are being run on all internet-connected devices; run updates immediately when they become available

- d. Establish an email management policy
- Never open emails and/or attachments or click on hyperlinks unless the sender is known and trusted
  - If the subject matter of the email seems strange, alarming, or urgent, delete the email unless you know and trust the sender and can tell their address has not been cloned or compromised
  - Do not access controlled networks or send sensitive information and emails via public WiFi
- e. Manage accounts and passwords
- Limit administrator access for installation of software
  - Ensure that only authorized personnel have access to computers and do not allow sharing of computer user accounts or login credentials
  - Use layered access levels for sensitive electronic system information
  - Implement strong password policies that require defined complexity and regular intervals for changing them
  - Limit the amount of data on a laptop and other devices

- f. Protect systems and processes
  - Utilize software that continuously scans downloads, documents, websites, and systems for malicious content, viruses, malware, etc.
  - Where feasible, prohibit access to copy or download sensitive information and applications to/from mobile devices and portable storage devices
  - Develop data retention policies for electronically stored information and rigorously enforce them
  
- g. Create a culture of awareness
  - Conduct regularly scheduled training related to the organization’s cyber risks and legal duties
  - Teach employees to be alert to possible security breaches
  - Teach proper methods for managing credit card data and all personal private information



## Social Media Risk Control Measures

**Have a social media and social networking policy** – Policy should be included in the employee handbook and communicated to all employees. Review and modify the policy to keep it current.

**Apply appropriate site security measures and settings**

**Regularly monitor sites** – Remove inappropriate postings by participating users

**Conduct regular searches** – Look for defamatory and disparaging comments and respond accordingly

**Protect private information and images** – Obtain written consent prior to any posting

**Respond to adverse comments** – Responses should aim to protect the organization’s reputation and brand, customers, current and former employees, etc.

**Include a disclaimer** – Sample: “Opinions expressed on this site are the opinions of the participating user. XYZ Company provides this site for online distribution of user-submitted content and does not endorse any user-submitted content nor assume liability for any actions of participating users.”

**Emergency planning for a data breach** – Assign roles, identify resources, and develop protocols in advance

**Isolate the source** – Find the source of the breach and remove it from the affected systems

**Determine the scope** – What systems were breached and to what degree and the exact type of data involved

**Maintain compromised hardware** – Law enforcement may need it for a forensic evaluation

**Determine notification requirements** – Did the nature and scope of the breach trigger any statutory notification requirements

**Initiate required notifications and any additional mitigation steps** – Offering of credit monitoring services, etc.

**Ensure security changes are implemented** – Goal is to prevent reoccurrence

### **Learning Objective 10:**

Know the considerations related to cyber risk insurance.

---

In addition to other risk control techniques, risk financing through insurance can be effective in treating cyber risk exposures. However, loss of data may not be covered by conventional property insurance.

1. Includes, but is not limited to businesses that have a computer system, use the internet to transact business or download information, online sales, conduct webinars, blogging, social media, bulletin boards, contract bidding, etc.
2. Coverage varies by carrier but often provides protection for lost data, security breach liability, privacy liability, business interruption, denial of service attacks, restoration costs, network security, media liability, and care, custody or control of data exposures for others is often included.
3. Designed to protect against liability (third party) and first party claims that occur as a result of damages arising from an insured's cyber exposures; many Cyber Policies exclude Errors and Omissions coverage due to programming, consulting, and other related services.



Contractual transfer is the reduction of an organization's liability exposure through the proper structure of contracts and other agreements; i.e. relationships between general contractors and subcontractors, landlords and tenants, etc.

---

### Learning Objective 11:

List and explain the four types of contractual transfer.

---

*The four types of contractual transfer are:*

1. **Hold harmless or indemnification agreement** – Assumption of the financial consequences for liabilities of another party through a contract between the indemnitor and indemnitee; i.e. a tenant holding the landlord harmless for a slip and fall injury on their premises  
  
Indemnitee – the one who is owed the obligation from another  
  
Indemnitor – the one who owes the obligation to another
2. **Waiver of subrogation** – Pre-event agreement to waive the right to seek recovery from a responsible party's insurance carrier for loss payments made to the insured; i.e. a subcontractor waives the right for their insurer to collect from the general contractor's insurance carrier, even though their employee is injured due to negligence by the general contractor
3. **Exculpatory agreement or clause** – Pre-event exoneration of the fault of one party that results in any loss or specified loss to another; i.e. parking garage will not be responsible for damage or theft of your vehicle
4. **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; i.e. airline will only be responsible for a maximum dollar amount for lost luggage

## Contract's Effect on Tort Liability

Tort liability is liability for negligence. How do the four types of contracts effect tort liability?

**Hold harmless agreements** do not absolve the indemnitee from its tort liability to a third party.

**Waiver of subrogation** does not absolve tort liability of the parties, but prevents insurers from any recovery of loss payments based on such tort liabilities

**Exculpatory agreement** absolves the tort liability between one or both parties but does not apply to third parties

**Limit of liability clause** does not absolve the tort liability of one or both parties, but it caps or limits the recovery of damages to the amount specified in the agreement

## Funding Contractual Transfer

**Hold harmless agreements** require the indemnitor to be able to provide funding or financing of assumed liabilities

**Waiver of subrogation** is the same as exculpatory except the loss is absorbed by the insurer under an insurance contract

**Exculpatory clause** has no affirmative obligation to provide funding except that which is required to absorb loss

**Limit of liability** requires funding or financing of amounts payable for damages as defined in the contract

**Note:** Written contract may have bearing on how an insurance contract responds

## Statutory Limitations

2

**Hold harmless agreements** may be subject to anti-indemnity statutes depending upon the specific terms of the agreement and the jurisdiction.

**Waiver of subrogation** is not subject to anti-indemnity statutes.

**Exculpatory clause** is generally not subject to anti-indemnity statutes.

**Limit of liability clause** is not subject to anti-indemnity statutes.

## Creating a Risk Control Program for Contractual Review

Identify what contracts or agreements will be reviewed

Determine who will be responsible for reviewing which types of contracts

Ensure access to and review all appropriate contracts, incoming and outgoing

Monitor, evaluate and suggest revisions in contractual language to be consistent and compatible with risk management programs and to be in compliance with changes in the law

## Insurance Considerations for Contractual Risk Transfer

Contractual agreements must align with insurance provisions in order to be effective

Address ongoing and completed operations; i.e. additional insured endorsements

Primary and non-contributory

**Control of which party drafts the agreement**

**Input from the risk manager**

**Reasonableness of assumption of risk**

**Education and understanding** – Must have knowledge of contractual language and terms

**Attorney input is required** – Most attorneys are not experts in risk management or insurance terms, but are experts in legal terminology and liability

**Understanding and complying with insurance provisions** – Must understand what insurance provisions are outlined within the contract

**Proper risk transfer to lower-tiered subcontractors**

**Laws governing contractual interpretation are dynamic and may vary by jurisdiction;** e.g., safe workplace acts, sole negligence, and anti-indemnity statutes

**Contractual transfer attempts to shift risk** – Beware that the underlying risk still exists

## Comparison of Contractual Transfers

	<b>Hold Harmless Agreements</b>	<b>Exculpatory Agreements</b>	<b>Waivers of Subrogation</b>	<b>Limit of Liability Clause</b>
Definition	An assumption of the financial consequences for liabilities of another party through a contract between an indemnitor and indemnitee	Pre-event exoneration of the fault of one party that results in any loss or specified loss to another	Pre-event agreement to waive the right to seek recovery from a responsible party's insurance carrier for loss payments made to the insured	Pre-event limitation of the amount, type or method of calculation of damages available by one or both parties to an agreement
Tort	Does not absolve the indemnitee from its tort liability to a third party	Absolves the tort liability between one or both parties to contract – does not apply to 3 <sup>rd</sup> parties	Does not absolve 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 “caps” recovery amount of damages between the parties
Funding	Requires indemnitor to be able to provide funding/financing of assumed liabilities	No affirmative obligation to provide funding except that which is required to absorb loss	Same as exculpatory, except the loss is absorbed by insurer under insurance transfer	Requires funding or financing of amounts payable for amount of damages as defined in contract
Anti-indemnity Application	May be subject to anti-indemnity statutes	Not subject to most anti-indemnity laws	Not subject to anti-indemnity laws	Usually involves bills of lading, cargo, freight, or cartage
General Considerations	If too broad, may void entire indemnity obligation	May be construed as a waiver of subrogation if claim is brought by a party's insurer	Typically, must be entered into prior to any loss payment by insurer to be binding on the insurer	May be the exclusive remedy of a party for any/all claims under contract without regard to amount of true loss

## Hold Harmless Agreements

### Hold harmless agreements may:

1. Include the indemnitee's cost of settlements or judgments paid to a third party and/or the costs of defense or legal fees.
2. Require indemnification at the conclusion of a claim/suit or require the indemnitor to assume the indemnitee's actual defense obligation during the claim/suit
3. Be unenforceable if found to be against public policy; this may occur when there is a huge disparity in bargaining positions between the indemnitor and indemnitee and the terms of the hold harmless agreement are deemed to be unconscionable

**Anti-indemnity statutes may limit or prohibit contractual transfers, and differ by jurisdiction and type of hold harmless agreement.**

---

### Learning Objective 12:

Identify the three types of hold harmless agreements.

---

**Limited (mine)** – assumes responsibility for indemnitee's liability for indemnitor's negligence only

**Intermediate form (mine and ours)** – *Limited* + responsibility for full indemnification of the indemnitee if there is any negligence on the indemnitor's part or if the indemnitor is partially negligent, he/she pays 100%; this classification applies to agreements requiring indemnification for ALL occurrences arising out of the indemnitor's operations, excluding only the liability arising from indemnitee's sole negligence

**Broad form (yours, mine, and ours)** – *Limited* + *Intermediate* + indemnitor agrees to be responsible for indemnitee's sole negligence; can include other parties' negligence

# THREE CLASSIFICATIONS OF HOLD HARMLESS AGREEMENTS

## LIMITED



### Mine

Indemnitor assumes responsibility for indemnitee's liability for indemnitor's negligence only. This classification applies to agreements requiring indemnification for occurrences arising out of the indemnitor's operations.

Example: Party A reaffirms responsibility for his own negligent acts. Party B has acquired a contractual right to indemnity where the basic tort law of the jurisdiction may or may not entitle him to it absent contractual transfer.

## INTERMEDIATE



### Mine + Ours

Limited + responsibility for full indemnification of the indemnitee if there is any negligence on the indemnitor's part or if the indemnitor is partially negligent, he/she pays 100%; this classification applies to agreements requiring indemnification for ALL occurrences arising out of the indemnitor's operations, excluding only the liability arising from indemnitee's sole negligence.

Example: Party A reaffirms responsibility for his own acts and agrees to assume full responsibility for joint and/or concurrent negligence of both parties. In many such contracts (especially construction contracts), Party A will agree to assume responsibility for all events except those resulting from the sole negligence of Party B; i.e., 100%, for all concurrent negligence situations. Does not apply to events arising from the sole negligence of Party B or the negligence of another subcontractor or entity beyond indemnitor and indemnitee.

## BROAD



### Mine + Ours + Yours

Limited + Intermediate + Indemnitor agrees to be responsible for Indemnitee's sole negligence. Can include negligence of other parties. This classification applies to agreements requiring complete indemnification of the indemnitee for all occurrences without reference to negligence - can even include those situations arising from the sole negligence of another entity.

Example: Party A assumes responsibility for all liability without regard to fault of himself and/or Party B. Here Party A assumes not only the responsibility of his acts, plus any acts arising from joint and/or concurrent negligence of Party A & Party B, but also includes those situations that result from the sole negligence of Party B. This extreme variant may require Party A to assume responsibility for the negligent acts of some other entity, over whom Party A has no control, which results (or may result) in a claim being made on Party B.

### **Examples of contracts commonly containing hold harmless agreements:**

1. Construction agreements
2. Service contracts
3. Purchase orders
4. Usage permits
5. Leases and rental agreements

### **Contractual provisions requiring review and analysis**

1. Insurance clauses
2. Liability clauses
3. Hold harmless or indemnification clauses
4. Mutual release clauses
5. Waiver of subrogation clauses (including mutual waiver of subrogation)



## Review Of Learning Objectives

1. List the common sources of employment practices liability exposures.
2. Identify and describe risk control measures to treat common sources of employment practices liability exposures.
3. Identify the common types of fleet exposures and hazard controls related to fleets.
4. Identify administrative controls used to handle fleet exposures.
5. List and gives examples of controls for hazards related to walking surfaces.
6. Identify and describe the key property exposure terms.
7. Name the hazard controls programs related to property.
8. Describe the common business applications using technology that create a cyber exposure.
9. List and describe cyber risk exposures created by e-business or cyber activities.
10. Know the considerations related to cyber risk insurance.
11. List and explain the four types of contractual transfer.
12. Identify the three types of hold harmless agreements.





# Certified Risk Managers

*a proud member of The National Alliance for Insurance Education & Research*

## Section 3

# Crisis & Disaster Planning



## Resources

### [Key Terms](#)



### [Sample Disaster Plan](#)



### [Sample Disaster Checklist](#)



### [Emergency Resources List](#)



## Crisis & Disaster Planning

### Learning Objectives

1. Define a crisis, its characteristics, and the potential impact it may have on an organization.
2. Define crisis management and the principles of an effective crisis management program.
3. Identify the goals of crisis management before, during, and after a triggering event.
4. List the key steps of creating a crisis management plan.
5. Explain the four essential steps of the crisis management process.
6. Discuss the important considerations of reputation management during a crisis.

### **Learning Objective 1:**

Define a crisis, its characteristics, and the potential impact it may have on an organization.

---

**Definition:** A crisis is any critical incident that threatens or causes injury to people or a disruption of normal business operations; and/or, threat to the financial welfare and image of the organization.

#### **Characteristics:**

1. Has potential to significantly damage reputation
2. Affects one or more class of assets, e.g. people, property, income
3. Interrupts operations
4. May damage consumer, shareholder, and employee confidence, but if handled correctly may strengthen relationships
5. May involve multiple audiences and stakeholders
6. May be unique and entirely unpredictable or may be largely anticipated

#### **Potential impact of a crisis**

1. Disruption in operations, shutdown or possible bankruptcy
2. Serious bodily injury to customers, employees or other persons
3. Creates potentially damaging media attention affecting public opinion

### **Human**

1. Accidental, organized or deliberate
2. Difficult to avoid and very expensive to mitigate

### **Environmental (pollution, etc.) or natural (“acts of God”)**

1. Can be challenging or impossible to control
2. Can be widespread and far-reaching

### **Industrial, technological, or mechanical disasters**

1. Ranging from an exploding power plant to a failed system
2. Can be mitigated by segregation/separation/duplication
3. Infrastructure or transportation breakdowns

### **Biologic or pandemic disasters**

1. May be natural in origin or intentional
2. Global in scope
3. High uncertainty
4. Difficult to control new exposures

### **Political**

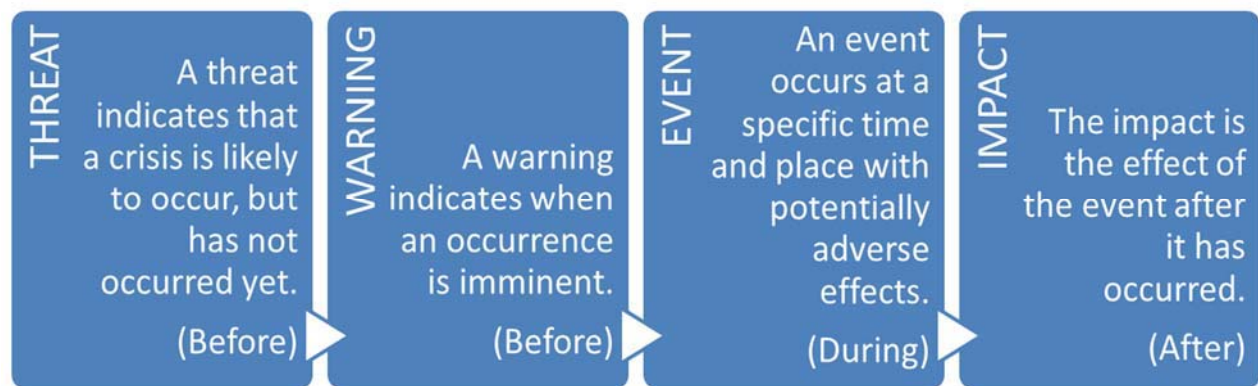
1. Changes in laws
2. Strikes, coups, etc.
3. Difficult to mitigate

## Major Phases of a Crisis

Effective crisis management goals before, during, and after a crisis must be aligned with the actions to be performed during the four major phases of a crisis: threat, warning, event, and impact.

Recognition of these phases helps the risk manager schedule specific pre-crisis activities, crisis response, and post-crisis activities.

### Phases of a Crisis



**Note:**

Not all crises have all of these phases. Some move directly to event and impact with little to no threat or warning; e.g., an active shooter situation.



## Example – Tropical Storm Margo Brewing in the Pacific Ocean

T H R E A T	<p><b>Threat:</b> A likely probability of occurrence, but, not yet an event for a resort located in Puerto Vallarta, Mexico. Monitoring of the projected path of the storm is required. Crisis management plan is in place and triggers activities such as purchasing materials for board up, testing emergency radios, collecting cots, gathering food supplies, etc. Resort employees are trained and there is effective communication throughout the resort. Resources have been adequately allocated.</p>
W A R N I N G	<p><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 outer bands of the storm being felt within a 200-mile radius of Mexico’s Pacific Coast. Activities include boarding up buildings, removing outdoor property, beginning evacuation of non-essential personnel.</p>
E V E N T	<p><b>Event:</b> Hurricane has struck land. Objective is to protect human life, maintain communications and continue to manage emergency priorities.</p>
I M P A C T	<p><b>Impact:</b> Continued protection of life and property is essential. Activities would also include cleanup and restoration, restoration of operations, reporting of insurance claims, securing funding for recovery, and maintaining a positive public image.</p>

## Learning Objective 2:

Define crisis management and the principles of an effective crisis management program.

**Definition:** Crisis management is the act or process of managing a crisis to prevent the occurrence of a catastrophic loss, if possible, and reduce the impact of catastrophic losses to the organization, including its reputation and brand.

### Principles of effective crisis management:

PRINCIPLE	IMPORTANCE
<b>Comprehensive</b>	To consider all hazards, all phases, all stakeholders and all impacts relevant to disasters
<b>Progressive</b>	To anticipate future disasters and formulate preventive and preparatory measures to build disaster-resistant and disaster-resilient plans and operations
<b>Risk-driven</b>	To use sound risk management principles to assign priorities and resources (hazard identification, risk analysis, and impact analysis)
<b>Integrated</b>	To ensure a unity of effort among all levels of the enterprise and all elements of customers, suppliers, government and community
<b>Collaborative</b>	To create and sustain broad and sincere relationships among individuals and organizations that encourage trust, advocate a team environment, build consensus, and facilitate communication
<b>Coordinated</b>	To synchronize the activities of relevant stakeholders to achieve a common purpose
<b>Flexible</b>	To use creative and innovative approaches to solve disaster challenges
<b>Professional</b>	To value a science- and knowledge-based approach based on education, training, experience, ethical practice, and continuous improvement

---

### **Learning Objective 3:**

Identify the goals of crisis management before, during, and after a triggering event.

---

The goal of crisis management is to effectively and economically minimize the operational and financial impact of the crisis.

#### **Before**

1. Crisis management plan in place
2. Effective communication and training
3. Adequate resources allocated

#### **During**

1. Protect human life
2. Maintain communication and coordination
3. Manage financial expenditures

#### **After**

1. Restore and/or maintain operations
2. Maintain a positive public image
3. Sustain profits and stable earnings
4. Review and improve crisis management plan

### **Learning Objective 4:**

List the key steps of creating a crisis management plan.

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. Crisis plans must be customized to the individual organization – as each has its own needs, goals, resources, and definition of what constitutes a crisis.

### **Key Steps**

- A. Establish the crisis management planning team
- B. Identify potential disasters or crises
- C. Conduct a vulnerability and/or disaster analysis
- D. Identify and prioritize critical business needs
- E. Assess and review internal resources
- F. Identify external resources
- G. Identify asset requirements
- H. Coordinate communication
- I. Develop the crisis management plan
- J. Write and distribute the plan
- K. Implement the plan
- L. Understand the obstacles

## **Establish the crisis management planning team, structure and responsibilities**

1. Select members of the planning team
  - a. Program coordinator/leader
  - b. All operational interests represented, from multiple levels of the organization, e.g., senior management, line management, support staff, etc.
  - c. Characteristics needed
    - Expertise
    - Authority/Access
    - Leadership skills
  - d. Define authority and limits and have backups available

### **Identify potential disasters or crises by examining:**

1. Those previously experienced by the organization
2. Geographic location – consider proximity of facilities to risk factors: highways, railways, rivers, chemical plants, military bases, airports, earthquake zones, tornado zones, hurricane zones, flood plains
3. Industry and type of operations
4. Hazards which may contribute to or cause a disaster or crisis – positively or negatively

**Conduct a vulnerability and/or disaster analysis – *where are you vulnerable and what are you vulnerable to?***

1. Consider all possible disasters and rank them based on probability and potential severity of impact
2. Considerations
  - a. Source – natural, human, emerging risks, etc.
  - b. Timing – length of warning, seasonality, business peaks
  - c. Impact – human, property, operations, public image, customers, etc.
  - d. Liability – what precautions need to be taken to avoid negligence?
  - e. Controls/mitigation – pre-loss and post-loss

**Identify and prioritize critical business needs**

1. Operations, equipment, personnel
2. Utilities – electricity, water, gas, telecommunications, Wi-Fi
3. Products and services – internal and external
4. Vendors, suppliers, and customer lists
5. Reciprocal agreements

### Assess and review internal resources

1. Key personnel from each operational unit
2. Backup personnel and services  
(provide additional training when necessary)
3. Available equipment and materials  
(fire suppression, communications, transportation, stockpiles)
4. Hazardous material and environmental policies
5. Safety & security procedures
6. Contracts
7. Fire prevention plans
8. Evacuation plans
9. Insurance programs  
(coverages, exclusions, limits, deductibles)

### **Identify external resources**

1. Disaster response organizations: e.g., FEMA/American Red Cross
2. Local/state associations
3. Utilities
4. Sheriff's office/police department/fire department
5. Local hospital/emergency clinics
6. IT services/vendors
7. Insurance agents/brokers
8. Remediation services

### **Identify asset requirements**

1. Supplies – water, first-aid, generators, gloves, etc.
2. Materials – sandbags, 2x4's, pumps, blocks, etc.
3. On-site versus off-site storage
4. Designate alternative premises for each operational location
5. Funding and sources



## Coordinate communication

1. Utilize automated, online phone tree to communicate with employees, customers, vendors, suppliers, etc.
  
2. Internally
  - a. Provide periodic contacts prior to crisis
  
  - b. Visitor communication
  
3. Externally
  - a. A key proactive crisis management step is to inform the public, customers, vendors and suppliers of what they can and cannot expect from the organization pre-crisis, including information on alternative premises and communications procedures that would be utilized in the event of a disaster
  
  - b. Media
    - Establish media contacts prior to the crisis and craft pre-written statements
  
    - Use the media to post disaster tips as a positive advertisement (public service announcements)

### **Develop the crisis management plan**

1. Based on type of risk, risk level, and risk impact
2. For each identified impact
  - a. Strategic plan
  - b. Emergency response procedures
  - c. Mitigation plan
  - d. Recovery plan
  - e. Supporting documentation

### **Write and distribute the plan**

1. Prepare and test the draft plan
2. Review and analyze the results
3. Revise the plan
4. Develop an executive summary
5. Seek feedback and buy-in

## Implement the plan

1. Conduct orientation and training
  - a. Tabletop exercises
  - b. Simulations or mini-drills
2. Integrate the plan into company operations
3. Coordinate with outside organizations

## Understand the obstacles

1. Financial constraints
2. Organizational resistance
3. Informational gaps
4. Communication difficulties, disruptions and failures
5. “Fog of war” factor – how people will perform under pressure
6. An unexpected event



**Learning Objective 5:**  
Explain the four essential steps of the  
crisis management process.

---



The crisis management team should identify activities or controls that can be put into place pre-event to reduce or eliminate the impact of a crisis.

**Design and implement prevention and control measures for potential threats** (fire, bomb threat, snow or ice, flood, active shooter, etc.)

**Establish a maintenance/safety program to prevent/mitigate potential impacts**

1. Building access and security – ID cards, key fobs, etc.
2. Safety programs – drug & alcohol awareness, employee screenings, fleet safety, EAPs
3. Hazard control programs
  - a. Sprinkler systems
  - b. Fire alarms
  - c. Other engineering controls
4. Facilities
  - a. Housekeeping, e.g., securing furniture or fixtures in an earthquake zone
  - b. Maintenance – HVAC systems, building structure, making prompt repairs
  - c. Inspections – to confirm engineering controls are operating as designed

## **Create a crisis management kit**

1. Operational components
  - a. Lists of contact information – team members, backup personnel, non-employees, and local emergency services
  - b. Aerial photo of site/GEO code for location
  - c. Assembly areas/on-site shelter locations
  - d. Area maps including evacuation routes and alternate routes
  - e. Information on how to activate emergency notification systems
  - f. Emergency procedures
  - g. Copies of pre-written, generic media statements for immediate response
2. Physical components
  - a. Master keys/codes
  - b. Communication equipment
  - c. Cameras
  - d. Battery-operated AM/FM radio, weather radio
  - e. Battery-operated lighting

No matter how well an organization plans, some crises are unavoidable. Therefore, the crisis management team needs to prepare the organization for worst-case scenario events. Investing the time and resources pre-event can be well worth the effort if it saves lives and reduces the overall impact.

### **Procedures**

1. Lockdown, evacuation, shelter-in-place procedures
2. Emergency shut-off procedures
3. Emergency response procedures
4. Practice drills – functional, evacuation, full-scale

### **Communication/Training**

1. Ensure effective and well-practiced emergency communication plans are in place (personnel and others inside and outside the organization). Remember to consider those with special needs.
2. Train all employees on reporting, how to use equipment/emergency supplies, etc.
3. Educate the team to understand what exposures exist, how to identify them, and what conditions surrounding them could lead to a crisis, e.g., hazardous chemicals, kidnap and ransom, product recalls, riots, labor strikes

## Resources

1. Emergency funding can be critical – make sure plans are in place for how/by whom funds will be obtained
2. Contractually arrange for back-ups (equipment, personnel, etc.)

Example: Back-up power source

- What type?
- What areas does it cover? What functions does it keep running?
- Maintained and serviced on a regular basis?
- Who do you call for service?
- Re-evaluated for adequacy when new operations or equipment is added?

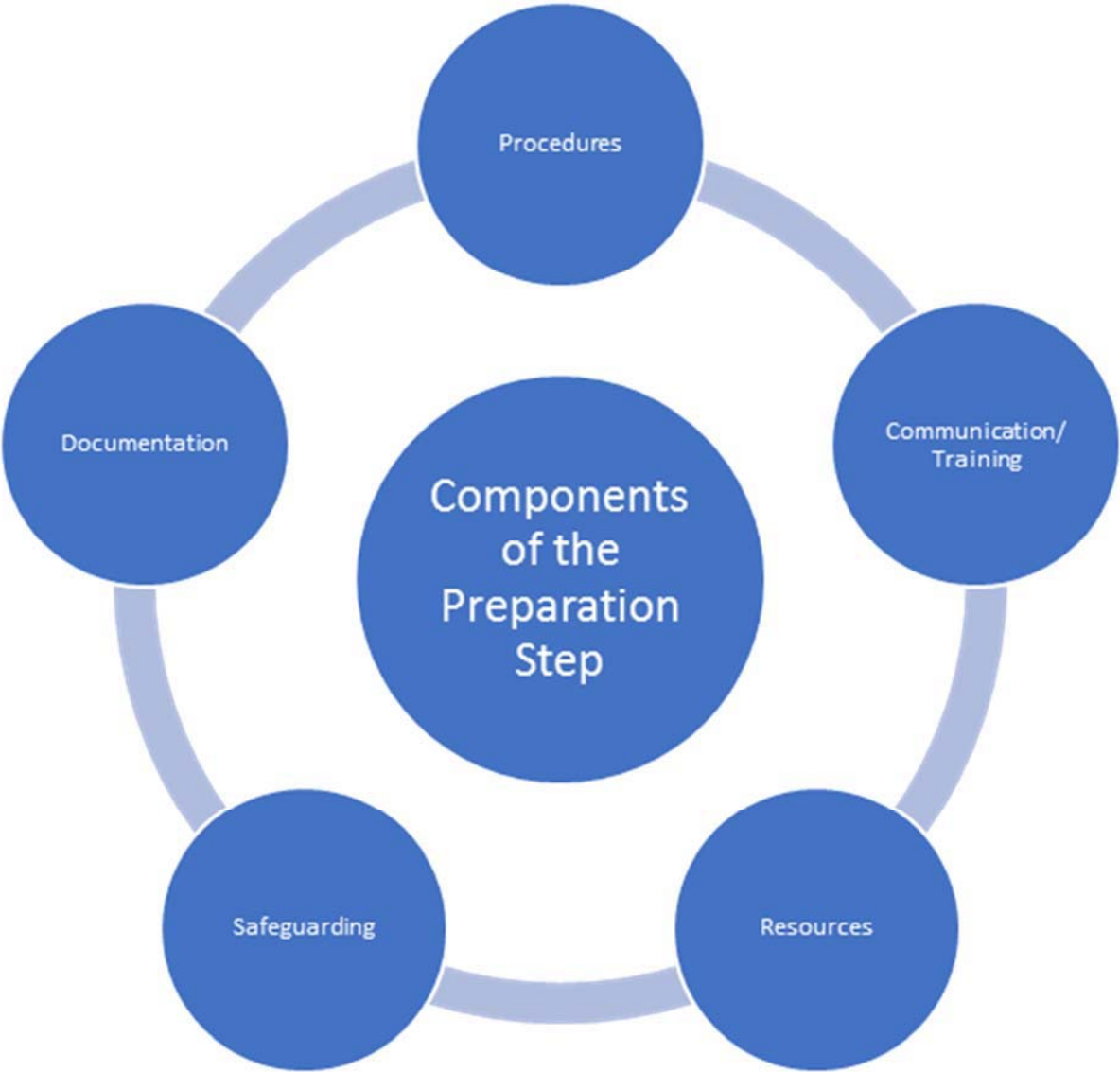
## Safeguarding

1. Contract with disaster recovery partners so that clean up, construction materials, etc. are readily available when needed
2. Ensure outposts are well stocked with all necessary supplies
3. Inspect and maintain production and support equipment



**Documentation**

1. Maintain inventory lists
2. Protect records – have multiple copies, fire safes, etc.  
**Note:** *Important to update all copies as data changes*
3. Document pre-loss conditions
  - Take photos of the facilities, equipment, furnishings, etc. to provide a point-in-time reference of condition and inventory
  - Store photos and a current fixed asset list at a separate secure location



The crisis management plan is put into action during an actual crisis. The ability to assess a situation and respond swiftly is crucial.

**Actions to take:**

1. Protect human life – this always comes first
2. Provide assistance - employee and family considerations
3. Notify emergency responders
4. Initiate communication efforts
5. Initiate a damage assessment
  - a. Document details, site access and status of utilities
  - b. Take photos and videos (current technology, i.e. drones)
  - c. Document damages and losses
6. Financial expenditures – a separate accounting code should be established for all expenses including all employee time utilized for clean-up, security, repair, etc. Are additional resources necessary?
7. Schedule media time
8. Utilize insurance partners

The primary goals after a crisis are restoring operations and ordinary business activities while maintaining profits and public image.

**Initial steps to take for effective recovery:**

1. Assign roles and responsibilities
2. Follow the hierarchy of priorities developed during the planning process
3. Identify and provide for essential personnel
4. Ensure chains of command are in place
5. Re-establish communications with customers, clients, and vendors

**Other steps to take as appropriate:**

1. Initiate employee support programs (needs will be relative to type of crisis)
2. Initiate mutual aid agreements
3. Secure the site, control access, and prevent subsequent damage or injury to property or people
4. If operations are to resume at existing premises, ensure the safety of returning persons
5. Initiate salvage efforts – coordinate with insurance carrier
6. Review recovery needs and timelines for each affected department
7. Resume limited operations to meet customer needs
8. Implement special accounting procedures

Remember, crisis management is a continuous process. An organization should always be evaluating and updating its plan. The plan may change based upon experience, industry research, or other changes in operations and personnel.



---

### **Learning Objective 6:**

Discuss the important considerations of reputation management 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*

#### **Important considerations:**

1. Reputation is a key corporate and strategic asset
  - a. Reputation management is strategic, proactive, and ongoing
  - b. Perception is everything in managing reputation risk
  - c. Reputation management is challenging because an organization does not wholly own or control its reputation

2. Reputation management requires specific goals
  - a. Eliminate misinformation and negative publicity by quickly and accurately addressing any issue that has potential to threaten the organization's reputation
  - b. Build a network of internal and external advocates
  - c. Establish sound relationships with the media in advance
  - d. Prevent an issue from escalating to a crisis
  - e. Minimize the long-term adverse impact of a crisis
  - f. Attempt to disassociate from the event, show it as an anomaly, and not indicative of the organization
  
3. The initial 24-hour period is a critical time in the process
  - a. Sets the tone
  - b. Organization management must show leadership
  - c. Establish the primary media contact
  - d. Monitor the news media, social media, blogs, tweets, etc.
  - e. Communicate widely and consistently

4. Crisis communication requires discipline
  - a. Designate one spokesperson to deal with the media
  - b. Speaker must maintain credibility and control the dialogue
  - c. Do not discuss blame or shift responsibility for the situation
  - d. Set guidelines and policies for appropriate employee response
  - e. Response must be proportionate to the crisis
  
5. Message delivery
  - a. Quickly gather and confirm accurate information
  - b. Fact-based – forgetfulness can be forgiven; lies will not
  - c. Acknowledge responsibility if it exists and demonstrate empathy
  - d. Emphasize the organizational measures being taken to protect lives and mitigate damage
  - e. Anticipate questions
  - f. Never say “no comment” or “off-the-record”

6. Restoring a damaged reputation
  - a. Management actions
    - 1) Accept responsibility
    - 2) Help those immediately impacted
    - 3) Take long-term corrective action
    - 4) Address systemic problems
  - b. Other actions
    - 1) Re-establish trust with customers and stakeholders
    - 2) Gather industry support
    - 3) Participate in speaker's bureau
    - 4) Maintain community relations
    - 5) Establish media outreach/leverage media coverage
    - 6) Educate your consumer
    - 7) Develop a new PR/advertising/marketing campaign
    - 8) Implement a government affairs program



# IMPORTANT CONSIDERATIONS FOR MAINTAINING REPUTATION DURING A CRISIS



**Reputation is a key corporate and strategic asset**

**Reputation management requires specific goals**



**The initial 24-hour period is a critical time in the process**

**Crisis communication requires discipline**



**Message delivery**

**Restoring a damaged reputation**



## **Review Of Learning Objectives**

1. Define a crisis, its characteristics, and the potential impact it may have on an organization.
2. Define crisis management and the principles of an effective crisis management program.
3. Identify the goals of crisis management before, during, and after a triggering event.
4. List the key steps of creating a crisis management plan.
5. Explain the four essential steps of the crisis management process.
6. Discuss the important considerations of reputation management during a crisis.



## PRACTICE EXERCISE

A risk manager, for a large hotel resort 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 the plan is finalized. She has requested your participation and has provided the following information:

**Objective:** To assess the organization’s crisis management plan and its readiness to respond to potential critical incidents.

**Method:** A tabletop exercise that simulates a 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:** The 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 upon knowledge of the crisis management process, as well as your personal experience and acquired knowledge.

**Assumptions:** The scenarios will require a number of broad assumptions. During this exercise, assume the following:

- The scenario could actually occur.
- Events occur as they are presented.
- There are no hidden agendas or trick questions.
- All participants receive identical scenario information at the same time.

**Exercise Rules:** There is no single or “correct” solution. Each scenario is different, and each team will respond to the set of facts in a unique manner. 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. Decisions are not precedent setting and may not reflect the organization’s final position on any given issue.

**Suggestions:** Treat the scenarios as real 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, designed to provide an open view of the ocean vistas and the company President's yacht in the marina below. All of 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 of the company's accounting and finance transactions, internal corporate communications, and the reservation records for the various resorts. All of the company employee email service is processed through an email server which is included in the server stack. Even though the IT department's normal 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 the presence of a minor Level 1 storm that is churning in the ocean north of Puerto Rico. The various weather computer models are not clear 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

You are the head of the company's Emergency Response Team (ERT). Given the above information, what are your first steps after you see the weather service announcement on the television?

1st priority?

2nd priority?

3rd priority?

Who will you call?

How will you communicate with them?

What will your instructions be?

**You are the IT Manager** – assuming you are contacted by the head of the Emergency Response Team (ERT)

What will be your first steps?

Who will you call?

How will you communicate with them?

## 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 Bill has grown rapidly into a Level 3 storm and has established a path that will have it moving on shore 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 located within 15 miles of the coast.

## Stage 2 Questions

You are the head of the Emergency Response Team. Given the information above, what will be your first steps?

1st priority?

2nd priority?

3rd priority?

Who will you call?

How will you communicate with them?

What will be your instructions?

### 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 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 land line phone services are out in an area up to 35 miles inland from the Atlantic Coast.

You are the head of the Emergency Response Team. Your home has also sustained substantial damage, as have the homes of many of your co-workers at corporate headquarters.

### Stage 3 Questions

Given the information above, what will be your first steps?

1st priority?

2nd priority?

3rd priority?

Who will you call?

How will you communicate with them?

What will be your instructions?



### Stage 4 Narrative

During the clean-up of the corporate offices, a body was discovered in the building's basement. The identity of the body 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 on a broadcast 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. How do you "get this circus under control NOW"?





# Certified Risk Managers

*a proud member of The National Alliance for Insurance Education & Research*

## Section 4

# Claims Management



### [Key Terms](#)



## Claims Management

### Learning Objectives

1. Define claims management and identify the ways in which it supports the risk control program.
2. List and explain the key steps of the claims management process.
3. Discuss the four types of Alternative Dispute Resolution (ADR) methods.
4. List the considerations when selecting a claims management plan.
5. Compare the three types of claims management plans.
6. Distinguish between bundled and unbundled plans.
7. List the components of a claims audit and describe possible findings.
8. Explain the role of a Third-Party Administrator (TPA) and the major considerations of the selection process.
9. List the considerations when selecting defense counsel for an organization.

### **Learning Objective 1:**

Define claims management and identify the ways in which it supports the risk control program.

---

#### **Definitions:**

1. Loss – a reduction in value
2. Claim – a demand or obligation for payment as a result of a loss
3. 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

#### **Related Terms:**

1. Prompt – the primary goal of claims management is to resolve claims matters promptly and effectively to save money and preserve relationships
2. Resolution – process of bringing claims to their conclusion; may include full or negotiated settlement, denial, litigation/Alternative Dispute Resolution (ADR), subrogation (addressed later in this section)
3. Ethically Responsible – ex gratia payments or compensation without regard to legal fault or responsibility – usually to maintain business relationships/reputation

**The claims management process supports the risk control program by:**

1. Gathering and utilizing claims data to improve business performance
2. Enforcing contractual obligations – insurance policy, hold harmless, additional insured
3. Mitigating damages after a loss event – actions taken to minimize severity
4. Promoting equitable compromise of claims – settling for lowest, reasonable dollar amount
5. Identifying and combatting fraud
6. Loss forecasting – setting accurate reserves, performing trend analyses (inflation and loss development)
7. Advising and consulting with all internal and external stakeholders – underwriting, loss control, named and additional insureds, defense counsel, etc.

## Learning Objective 2:

List and explain the key steps of the claims management process.







- Step 1 - Investigation
  - REPORTING
  - RESPONDING
  - GATHERING INFORMATION
  - DOCUMENTATION

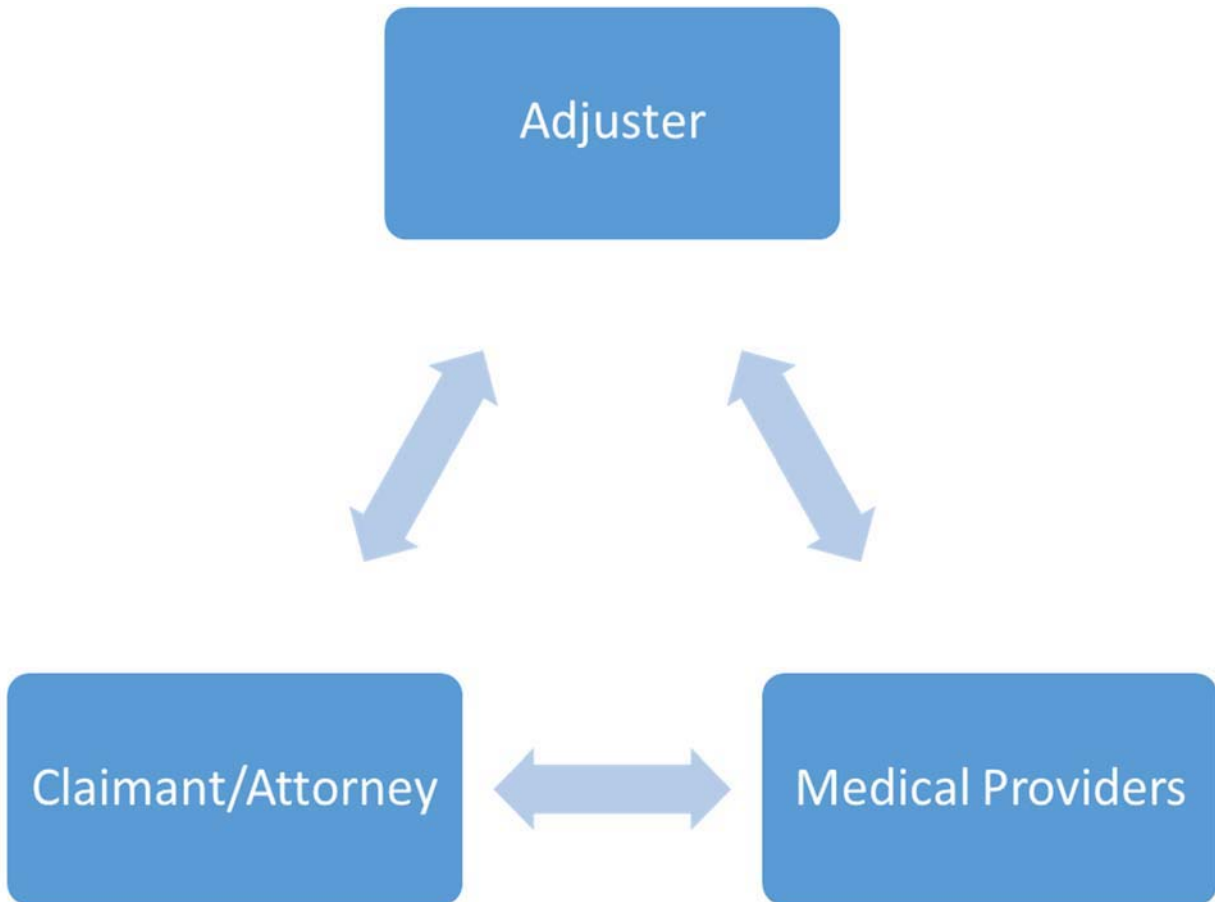
**Reporting** – The claims management process begins with a report of an event, whether an incident, accident, occurrence, claim or a loss

1. Ideally, one person in the organization should be the point of contact for all reports
2. Accidents/claims information must be reported to the adjuster and, if required, to the appropriate regulatory body (e.g. OSHA, WC administration, etc.) as soon as possible
3. If the first notice of an accident/claim is the service of a summons and/or complaint, defense counsel must be notified as soon as possible

## Responding to the incident/accident/claim report

1. Initiate contact within 24 hours and maintain effective contact with the employee/claimant; this is the most influential element of the entire claims management process
2. Recorded statement or claimant questionnaire
3. Initiate medical case management, if appropriate
  - Consent forms – HIPAA compliant (except workers compensation)
4. Once the contact has been established, maintaining the *triangle of communication* is critical
  - a. Set expectations
    - Communication (within 24 hours, by next business day)
    - Case manager assigned immediately on specific cases such as head injuries

# Triangle of Communication



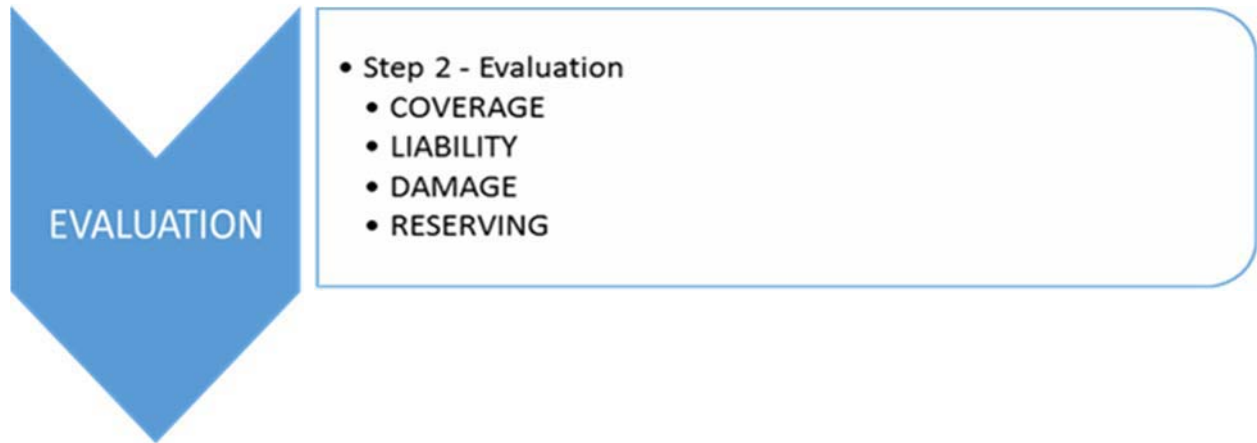
## Gathering information

1. Prompt and thorough investigations are critical
  
2. Who, what, when, where, and how – facts needed will vary based on specific claim
  - a. Unbiased investigation – outcome oriented investigations undermine the goals of insurance/active retention programs
  
  - b. Evidence collection and preservation
  
  - c. Weather, physical conditions, official reports, media
  
  - d. Witness issues – identification, reliability, bias, fading memory, reluctance
  
  - e. Outside support – appraisers, engineers, accountants
  
  - f. Claims history
  
  - g. If there is anticipation of future litigation, consider initial attorney involvement to keep investigation “protected”
  
  - h. File documentation (claim notes) – may be discoverable in litigation and should reflect only facts and professional observations without disparaging or defaming comments

3. Ask “what else could have happened?” to gain clues as to possible defenses or mitigation
  - a. Contributory or comparative negligence
  - b. Contractual provisions – hold harmless, indemnification, exculpatory and limited liability
  - c. Subrogation, recoveries, and waivers
  - d. Fraud

**Documentation** of investigation

1. Phone calls
2. File notes
3. Witness statements
4. Request for relevant documentation



## Determination of Coverage

1. Identify potential insurance coverages and place all potential insurers on notice
2. Insurer will send notification of coverage issues, if applicable.
3. Reservation Of Rights (ROR) letter (unilateral)
  - a. Notifies insured of coverage issues
  - b. Protects the insurer by avoiding waiver and estoppel arguments (*prevents a party from contradicting its previous actions if they have been reasonably relied upon by another party*)
  - c. Identifies all policy provisions that are at issue
  - d. Unilateral – Insured is not required to respond (Several states require the insured to acknowledge receipt of the letter – which is not construed as an acceptance of the terms.)

4. Non-waiver agreement
  - a. Bilateral – Requires both parties to agree to the insurer’s reservation of its rights
  - b. Permits the adjuster to continue processing the claim while preserving the rights of the carrier to deny the claim based on development of facts
  - c. Provides the same protections to the insurer as an ROR, but also protects the insured from waiver, e.g., silence
  - d. Insured must be notified immediately once all coverage issues are resolved
  - e. In most liability situations, even if the insurer issues an ROR or non-waiver letter, they still have a duty to defend as opposed to a duty to indemnify
  
5. Resolving coverage disputes
  - a. Declaratory Judgment Action – requesting the court to decide coverage issues
  - b. Arbitration/mediation – insurers frequently incorporate mandatory arbitration provisions to resolve coverage disputes
  - c. Assignment – policyholder may assign its rights of recovery against an insurer to a 3<sup>rd</sup> party in return for limiting its liability. (if verdict exceeds policy limits or if extra- contractual liability [bad faith] against the insurer may be alleged)
  - d. Concerns
    - Funding costs of resolution
    - Continued relationship – business reasons

## Liability evaluation

1. Early in the investigation, it is important to consider theories of liability that may be used for or against the organization
2. Evaluate the different types of liability (tort, strict, statutory, etc.)
3. Negligence and causation

Negligence – failure to exercise the degree of care which a reasonably prudent person would exercise under the same circumstances

Causation – (proximate cause) – a showing that the injuries or damages were the natural and direct consequence of a party's negligence, without which the injuries or damages would not have occurred

- a. Intervening causation
  - b. Allocation of fault (e.g. contributory/comparative negligence)
4. Negligence per se – conduct that violates standards of care as established by statute or law (reserved for statutes and regulations that are safety statutes or laws designed to improve safety such as building codes and traffic laws)
    - a. Statutory violations
    - b. Criminal violations



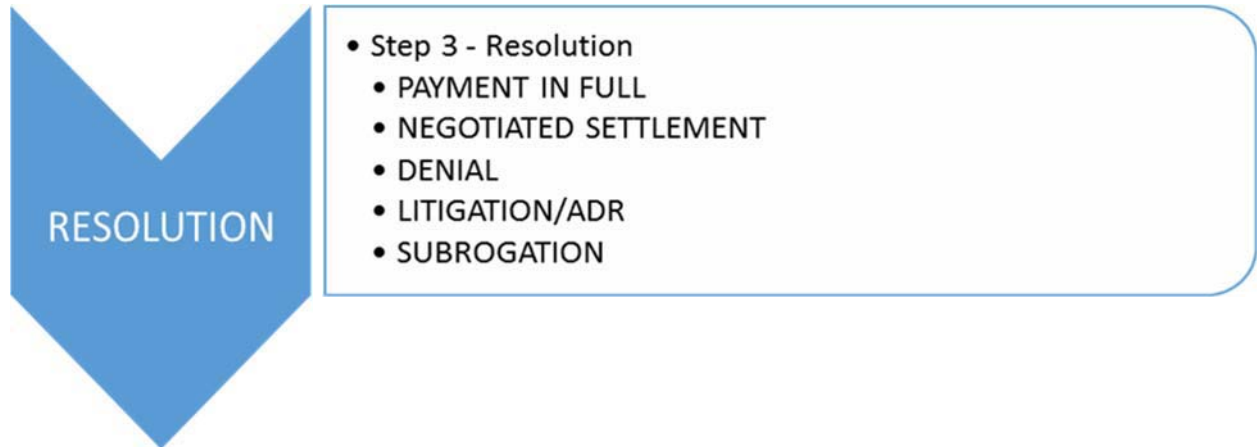
## Damage evaluation

1. Types of damages in tort
  - a. Common law damages
    - Economic – wages, medical, lost earning capacity (past/future)
    - Non-economic – pain and suffering, disfigurement, loss of consortium (past/future)
  - b. Statutory damages – attorney’s fees, fines or penalties under consumer protection or similar statutes
  - c. Punitive or exemplary damages – damages awarded to a plaintiff, in excess of compensatory damages, used to punish the defendant because of the particularly wanton or willful character of the wrongdoing and deter future similar acts
2. Considerations related to damage issues
  - a. Possible sources of recovery (e.g. indemnification, subrogation, etc.)
  - b. Damages should be evaluated regardless of extent of liability
  - c. Liability evaluations can change; damages can impact liability evaluations

## Reserving evaluation

1. Accurate reserving ensures the organization will have sufficient funds to pay both anticipated loss payments and loss adjusting expenses
2. Ongoing and regular review of loss runs is crucial to setting accurate reserves (reserved vs. paid losses, loss trends, late reporting indicators, etc.)
3. Consider two primary types of reserves: Case reserves and Incurred But Not Reported (IBNR) reserves  
(Note: IBNR reserves are not normally reflected on the loss runs available to the insured)
4. Setting reserves too high can result in:
  - a. Understating an organization's assets
  - b. Missed business opportunities, when the organization mistakenly believes it does not have adequate financial resources
  - c. Problems with tax reporting and stockholders
5. Setting reserves too low can result in:
  - a. Overstating an organization's assets
  - b. Insolvency and bankruptcy in the future
  - c. Problems with industry ratings (A.M. Best)
  - d. Problems with regulators
  - e. Understatement of the potential severity of a claim, leading to inadequate claims control measures and management

6. Reserving for IBNR
  - a. IBNR arises from the natural delay between the loss/claim event and the discovery and/or report
    - 1) **Incurred But Not Reported (IBNR)** – 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.
    - 2) **Pure IBNR** – claims that have occurred but have not been reported as of the evaluation date. Since the claim has not been reported, there is no basis for establishing a reserve based upon the specific characteristics of the claim
    - 3) **Broad or bulk IBNR** – includes pure IBNR plus the additional development on known claims
  - b. Casualty exposures have greater IBNR than first-party property exposures
  - c. Methods of estimating IBNR reserves
    - 1) Relationship of previously reported and unreported claims
    - 2) Number of reported claims weighted by average severity
    - 3) Based on organization's revenues
    - 4) Based on a reliable activity indicator
  - d. IBNR reserves are subject to statutory accounting regulations for insurers, captives, or qualified self-insurers
  - e. Accurate IBNR reserves are crucial for an organization's balance sheet



## Five non-mutually exclusive possibilities

1. Payment in full
2. Negotiated settlement
3. Denial
4. Litigation/Alternative Dispute Resolution (ADR)
5. Subrogation/recovery

1. Payment in full
2. Negotiated settlement – steps of the negotiation process
  - a. Preparation
  - b. Exploration
  - c. Exchanges of offers and counteroffers

- d. Settlement agreement
- 1) Reduce the essential elements of the agreement to writing immediately
    - Prepare and execute releases – a release is a legally binding agreement that binds the parties to a resolution
    - Typically, one party agrees to pay the other for specified damages; the other party promises to forgo further claims or litigation
- e. Structured settlements – can provide substantial advantages to both the claimant and responsible party
- 1) For the responsible party/insurer – periodic payment settlements cost less than lump sum payments
  - 2) For the claimant (and family) – periodic payments are not taxable as income unlike the interest from a lump sum payment
  - 3) For both claimant and responsible party – schedule of payments can be “tailored” to the claimant’s personal, medical (and family) needs
  - 4) For claimant’s counsel – meets fiduciary obligation to claimant by forestalling squandering of large awards in early years and by spreading attorney fees over several years to ease tax burden

3. Denial

- a. Unpleasant for both adjuster and claimant
- b. Requires higher standards of investigation/evaluation
- c. Possible litigation

4. Litigation/Alternative Dispute Resolution (ADR)

- a. Litigation management
  - 1) Is the collaboration between risk manager, claims personnel, and legal counsel to accomplish a shared purpose
  - 2) Is the risk manager's responsibility, not the attorney's (the organization's money and corporate reputation are at stake)

---

**Learning Objective 3:**

Discuss the four types of Alternative Dispute Resolution (ADR) methods.

---

The four types of alternative dispute resolution are:

**Mediation**

1. Informal process; no evidence
2. Neutral third-party acts as a facilitator to explore settlement
3. Mediator has no power to impose a decision

**Arbitration**

1. Semi-formal process; summary/documentary evidence only
2. A neutral third party or panel with a neutral umpire's oversight
3. Arbitrator's decision usually final

**Mini-trials**

1. Quasi-judicial format, abbreviated testimony and/or evidence
2. Fact finder will be mini-jury or magistrate
3. Mini-trial results are generally final

**Summary Jury Trials (SJT)**

1. Quasi-judicial format, abbreviated testimony and/or evidence
2. Fact finder will be mini-jury or magistrate
3. SJTs are not binding if not agreed to by parties prior to summary jury trial

5. Subrogation/recovery

- a. Reduces the effect of losses on premiums and retained losses and therefore reduces the total cost of risk
- b. Subrogation – the legal right of one who has paid another’s obligation to collect from the party originally owing the obligation, i.e., the insurer’s right to recover from another the amount that the insurer paid to its insured for a covered loss
  - 1) Whether or not to pursue recovery may be based on these relationships:
    - Legal relationship between subrogee and subrogor
    - Indemnitee/indemnitor relationship under a hold harmless or indemnification agreement
    - Additional insured under an insurance policy



c. Recovery – third-party claims

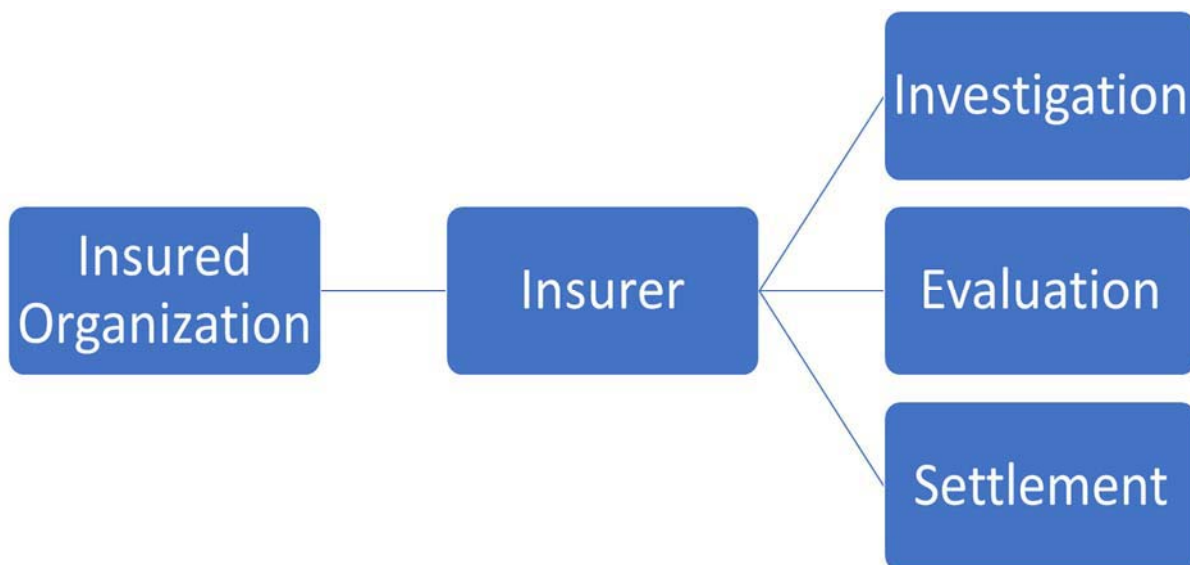
- 1) Obtaining funds from another who bears responsibility or who also has coverage for the claim, before the claim is settled
  
- 2) Examples of recovery sources:
  - Indemnification agreements
  
  - Hold harmless agreements
  
  - Joint venture agreements
  
  - Other insurance

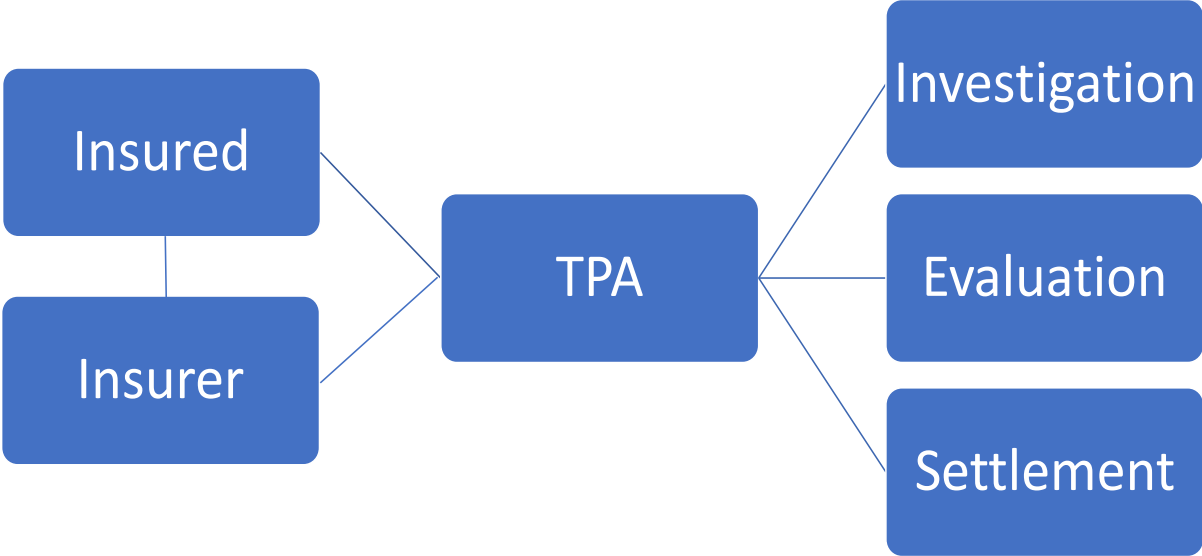
## Types of Claims Management Plans

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.

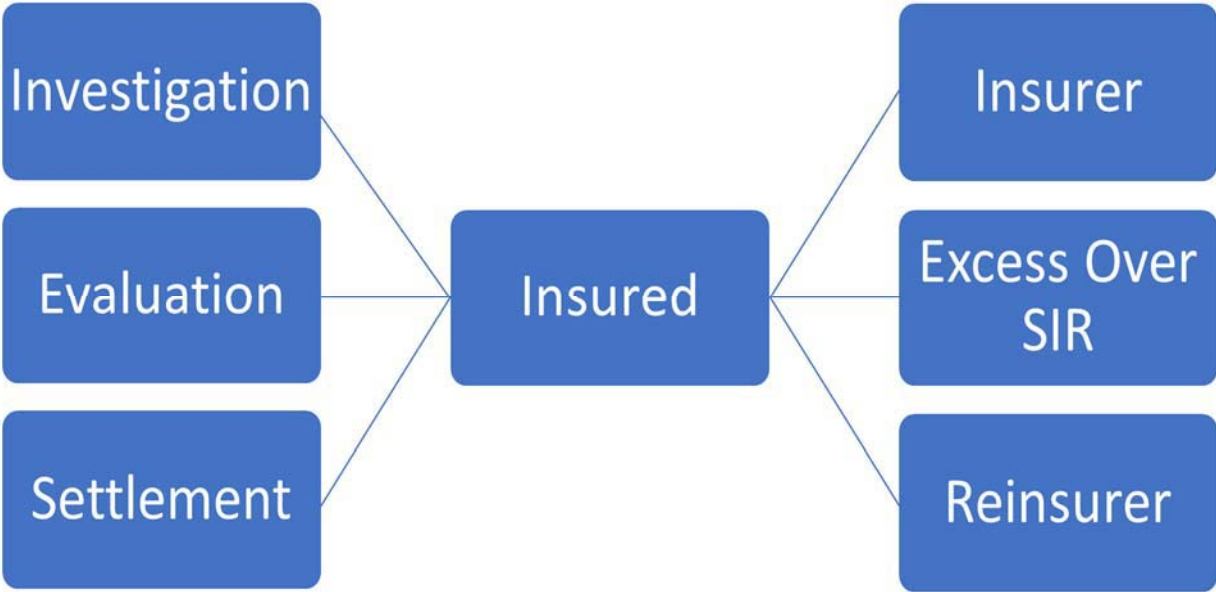
1. Insured plan
2. Third-Party Administered (TPA) plan
3. Self-Administered Plan

### Insured Plan:





**Self-Administered Plan:**



## Learning Objective 4:

List the considerations when selecting a claims management plan.

**THINGS TO CONSIDER WHEN SELECTING A PLAN**

There are many differentiators to consider and decisions to be made when selecting a plan which best suits your business needs.

- 1 LOSS SENSITIVITY** 
- 2 LOSS RUNS** 
- 3 LOSS RESERVES** 
- 4 STAFFING** 
- 5 SETTLEMENT** 
- 6 LITIGATION MANAGEMENT** 
- 7 BUNDLING VS. UNBUNDLING** 
- 8 CLAIMS AUDITS** 

## Things to Consider:

	WHAT IS IT?	WHY DOES IT MATTER?
<b>Loss Sensitivity</b>	The organization's financial ability to tolerate a loss or claim.	To what degree will a loss or claim affect an organization's finances?
<b>Loss Runs</b>	A list of reported claims providing such information as the names of insureds and/or claimants, the date of occurrence, type of claim, amount paid and amount reserved for each as of the report's valuation date.	How easily the data can be accessed and who owns the data based on plan type?
<b>Loss Reserves</b>	Amount of money earmarked for a loss or claim.	How much control do you have over setting loss reserves?
<b>Staffing</b>	Personnel who are handling claims	Quality control issues – level of experience, capabilities, workload, etc.
<b>Settlement</b>	The terms reached to close out a claim.	Who has the decision-making authority?
<b>Litigation Management</b>	An organization's process of managing legal services and costs; or their principles regarding use of outside legal services.	Who selects defense counsel and who determines how aggressively the claim will be fought?
<b>Bundling vs. Unbundling</b>	<p>Bundling – Provides group of services as part of a package.</p> <p>Unbundling – Insurer allows you to select only the services that you need.</p>	Does the insured have the financial ability, the expertise, and the resources to consider unbundled services?
<b>Claims Audits</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?

## Learning Objective 5:

Compare the three types of claims management plans.

CHARACTERISTIC	TYPE OF PLAN		
	INSURED	THIRD PARTY ADMINISTERED	SELF-ADMINISTERED
Loss Sensitivity	<p><b>Usually Low</b></p> <p>Guaranteed cost, dividend, small deductible or SIR and retro plans</p> <p>Deductible – insurer provides all policy services from first dollar and bills insured post-payment</p> <p>SIR – no obligation by insurer until satisfaction of SIR amount by insured</p>	<p><b>Moderate</b></p> <p>Includes larger deductible or larger SIR</p>	<p><b>Extremely High</b></p> <p>Very large SIR or no excess insurance coverage</p>
Loss Runs	<p><b>On-line Access,</b></p> <p><b>Some ad-hoc reporting</b></p>	<p><b>Loss info available in real-time,</b></p> <p><b>Ad-hoc reporting available</b></p>	<p><b>Insured Controls</b></p> <p>Responsible for data, use of RMIS, ability to customize reports for specific problems or loss exposures</p>

<i>(continued)</i>	TYPE OF PLAN		
CHARACTERISTIC	INSURED	THIRD PARTY ADMINISTERED	SELF-ADMINISTERED
Reserving	<b>Insurer Controls</b> Insured has little input regarding philosophy or case reserves	<b>TPA Controls</b> Reflects TPA's reserving philosophy, Notification to insured when reserve is exceeding a set amount, RM resources required to monitor and audit	<b>Insured Controls</b> Tendency for reserves to be set too low, monitoring is part of the auditing process, credibility with reinsurers must be maintained
Staffing	<b>No Control</b>	<b>Some Control</b> Most TPAs are responsive to staffing requests and preferences of the insured	<b>Ultimate Control</b> Must adhere to regulatory requirements (licensing, CE issues)
Settlement	<b>Insurer has Control</b>	<b>Greater Control – within SIR</b> Approval/authorization of insurer typically required prior to payment on larger cases	<b>Ultimate Control</b> Settlement authority often obtained from senior management, cash flow/cash management issues require proactive attention
Claims Audits	<b>Insurer seldom shares results</b>	<b>Internal audits, rarely shared</b>	<b>Internal Audits are critical; full feedback</b>
Litigation Management	<b>Insured has little or no influence over insurer</b>	<b>More responsive to Insured's philosophy</b>	<b>High Control</b> Generally, more willing to litigate
Bundling vs. Unbundling	<b>Bundled</b>	<b>Some unbundling available</b>	<b>Unbundled</b>

In a bundled plan, the insurance provider may include additional services as part of a package while an unbundled plan allows the insured to select only the services needed.

---

**Learning Objective 6:**  
Distinguish between bundled and unbundled plans.

---

**Bundling:**

1. The following services are “bundled” into the traditional/standard package:
  - a. Loss control
  - b. Claims services
  - c. Policy issuance
  - d. State filings – (e.g., W/C, DOI, etc.)
  - e. Statistical filings – (e.g., NCCI, etc.)
  
2. The insurer retains control of claims services and loss control as part of the insurance package



## Unbundling

1. Removes loss control and/or claims administration services from the package, leaving only the risk financing function of the insurance contract
2. Annual premium (per line of coverage) must be large enough to justify the insurer's willingness to unbundle services
3. Requires the willingness and ability of insured to assume a larger portion of the risk, compared to traditional "bundled" insurance programs
4. Insured's financial ability must support the anticipated cost of risk, including increased service costs
5. Unbundling with a large SIR is a viable substitute for self-insurance

## Introduction to the Claims Audit

**Ensures proper handling, reserving, compliance with regulatory requirements and internal policies, combat fraud, etc.**

### **Includes closed files**

- Reviewed for trends, reserve surplus or reserve inadequacy at the time of closing

### **Requires regular and ongoing verification of the status of all outstanding claims (open files)**

1. May vary by product line
2. Minimum annually; quarterly/monthly may be best

**Conducted by an audit team – needs claim handling experience and cannot be auditing own files or cases**

**Audit process may vary due to types of claims management plan (insured, TPA, self-insured)**

### **Possible audit findings**

### Learning Objective 7:

List the components of a claims audit and describe possible findings.

Claims Audit	Possible Findings
<b>Claims Payment Issues</b>	<ul style="list-style-type: none"> <li>• Duplicate Payments</li> <li>• Overpayments</li> <li>• Frivolous Payments</li> </ul>
<b>Claims Handling and Reserving Practices</b>	<ul style="list-style-type: none"> <li>• Poor reserving (i.e. stair-stepping or creeping)</li> <li>• Failure to pursue subrogation</li> <li>• Failure to seek contribution from excess and reinsurance carriers</li> <li>• Failure to watch aggregates</li> </ul>
<b>Procedural Issues</b>	<ul style="list-style-type: none"> <li>• Evidence that telephone calls, emails, etc. are not being promptly returned</li> <li>• Failure to obtain releases</li> <li>• Improper application of statutes, e.g., incorrect temporary total disability TTD rate</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>

### **Learning Objective 8:**

Explain the role of a Third-Party Administrator (TPA) and the major considerations of the selection process.

---

Usually retained by the individual organization – carrier approval may be required; there may be an approved list

With given authority, investigates, adjusts, and resolves claims within the organization's SIR (unbundled services may be available)

Reports to excess carrier on high value claims that are expected to exceed retention (when incurred losses reach 50% of retention or "red flags")

Will request reimbursement from carrier of funds spent in excess of the retention on reimbursement policies

TPA represents and reports to the organization

TPA should advise the organization when a claim is not covered and seek direction on handling; however, TPAs do not typically involve themselves in coverage issues or disputes between the insured and the carrier

TPA should advise organization when claims should be paid or denied; e.g.: acceptance of non-covered claims in excess of SIR will not be reimbursed

1. Accessibility
2. Systems compatibility
3. Flexibility in account handling
4. Staffing
5. Best practices and quality control
6. Industry experience and reputation
7. Additional services
8. Pricing and contract

### **Accessibility**

1. Availability for physical inspections, meetings, etc.
2. Assigned account manager and claims team
3. Inside or outside adjusters; portion of investigation that will be outsourced
4. Ease of claims reporting, communication, and access to claims management system
5. Frequency of file reviews and reports

## Systems Compatibility

1. Are the Risk Management Information System (RMIS) and the Claims Management System (CMS) compatible? – to support meaningful risk management analysis
  - a. Revenue codes
  - b. Divisions, departments, and locations
  - c. Special client-specific coding
  - d. Supports statutory reporting – captures needed fields, e.g. NCCI<sup>1</sup> codes, NAICS<sup>2</sup> codes, OSHA<sup>3</sup>
2. Ability to import existing claims data into Claims Management System
3. Ease of extracting data and internet access
  - a. Customizable reports readily available
  - b. Claim notes and financials
  - c. Operating system compatibility
  - d. System security – internal and external
  - e. Monthly report package – online or email
  - f. Monthly upload to excess carriers

---

<sup>1</sup> National Council on Compensation Insurance, Inc.

<sup>2</sup> North American Industry Classification System

<sup>3</sup> Occupational Safety and Health Administration

**Flexibility in Account Handling** – claims handling instructions, particularly for claims within SIR or deductible

1. Ability to design a program to match the organization's needs and objectives
2. Ability to customize reporting schedule for large losses
3. Reserve and payment authority limitations
4. Preferred vendors (yours)

### **Staffing**

1. Bios of all expected claims team members
  - a. Years of experience in the industry
  - b. Experience handling lines of coverage similar to the organization's business for past and present accounts
2. Turnover rates for company and branch
3. Licensing, professional development, internal training
4. Level of professionalism
5. Number of employees adequate for workload?
6. Determine ownership involvement in day-to-day operations

## Best Practices and Quality Control

1. Is there a written policy for claim standards?
  - a. Does it reflect industry standards?
  - b. Can it be modified to fit organization's needs?
  - c. Will the TPA incorporate the claim standards into the service contract as a material element of performance?
  
2. Audits to measure performance/quality control
  - a. Is there an internal audit process? Who audits?
    - Frequency?
    - Will the TPA provide the audit results?
  - b. Independent/outside audits
    - What is the TPA's position on independent audit?
    - Establish expectations that you or your representative will audit
  - c. Resulting action plans required?



## Industry Experience and Reputation

1. Obtain TPA recommendations from broker, trade organizations, insurance carrier, etc.
2. Research websites and promotional materials. Check multiple sources, not just company published material. Look for:
  - a. Information about lost clients and cancelled contracts
  - b. Pending litigation/settled court cases
3. Contact client and carrier references with specific questions in mind
4. Review financial solvency based on an independent audit, longevity, and E&O coverage limits

## Additional Services

1. Does the TPA allow you to select only the services you want/need?
2. Will the TPA work with your existing service providers?
3. Can the TPA provide services beyond your current program, e.g., loss control, medical case management, PPOs<sup>4</sup>, MCOs<sup>5</sup>?
4. Identify subcontractors who may be doing work for the TPA – obtain certificate of insurance and additional insured endorsement naming the TPA and the organization
5. Will the TPA disclose any ownership interests in recommended services, e.g., Is the bill-review company a subsidiary?
6. Will services be billed in a way that your insurers/reinsurers will accept?
7. Will the TPA develop additional risk management services, such as; training, internal forms, light duty programs?
8. Does the account manager provide analysis of claims, loss causes, frequency and severity, and consult with you towards improvement?

---

<sup>4</sup> Preferred Provider Organizations

<sup>5</sup> A Managed Care Organization is an entity that specializes in provider network development, provider credentialing, provider contracting, ongoing network management, claims pre-processing (to ensure the contracted rate is applied) and utilization management programs.

## Pricing and Contract

1. Compare services and selection criteria, remembering the lowest price is not always the best price
2. Pricing structured to budgetary needs
  - a. Annual flat fee for all claims
  - b. Per claim fee
    - Does the fee cover the life of the claim?
    - Sunset clause – states time period after which the billing structure will change (e.g., 2 years, 3 years)
  - c. Reconciliation with billing (charged hourly, etc.)
  - d. Management fees
3. Review the allocated expense categories and confirm understanding of what is not included in the basic file handling arrangement
4. Contractual considerations
  - a. Does the service agreement require the TPA to indemnify you for its negligence? Are there other indemnification issues in the service agreement requiring review/negotiation?
  - b. Who “owns” the data and claim files?
  - c. Provisions for terminating the relationship – notice of termination requirements? Who pays what?

# 8

## MAJOR CONSIDERATIONS WHEN SELECTING A TPA

- 1 Accessibility
- 2 Systems Compatibility
- 3 Flexibility in account handling
- 4 Staffing
- 5 Best practices and quality control
- 6 Industry experience and reputation
- 7 Additional Services
- 8 Pricing and contract

### Learning Objective 9:

List the considerations when selecting defense counsel for an organization.

4



## **Firm's management profile**

**Attorney Workloads** – How many files or cases and what types are they working on simultaneously?

**Size of firm** – Is it large enough and does it have the depth of qualified attorneys to handle your claims?

**Attorney's or firm's current client base** – Who do they work for, what types of industries – potential conflicts of interest?

**Experience level, education, and training** of the individuals related to the industry of the organization – Do they require ongoing training in relevant fields?

**Attorney's reputation in the insurance/business community** – Are they known for litigating or settling cases? Goals per claim may influence decision.

## Fee structure

1. Types of billing agreements
  - a. Hourly rate
  - b. Negotiated discount rate
  - c. Negotiated hourly limit
  - d. Flat fee per claim
  - e. Flat fee for all claims (virtual in-house counsel)
  - f. Contingent fee
  
2. Other litigation costs
  - a. Reporter fees
  - b. Photocopying
  - c. Overnight mailing and couriers
  - d. Research – LexisNexis
  
3. Potential billing problems/issues
  - a. Differentiated rates for varying levels of employees; including senior partners, investigators, paralegals, administrative assistants
  - b. At what level are activities assigned?
  - c. Activity reviews – match billings to activity reports
  - d. Incremental charges – meals, mileage, etc.

## Review Of Learning Objectives

1. Define claims management and identify the ways in which it supports the risk control program.
2. List and explain the key steps of the claims management process.
3. Discuss the four types of Alternative Dispute Resolution (ADR) methods.
4. List the considerations when selecting a claims management plan.
5. Compare the three types of claims management plans.
6. Distinguish between bundled and unbundled plans.
7. List the components of a claims audit and describe possible findings.
8. Explain the role of a Third-Party Administrator (TPA) and the major considerations of the selection process.
9. List the considerations when selecting defense counsel for an organization.



Thank  
You!

