



# **CERTIFIED RISK MANAGERS**

## **Practice of Risk Management**

The National Alliance  
2024



**CERTIFIED RISK MANAGERS**  
**Practice of Risk Management**  
**Table of Contents**

**1 — THE RISK MANAGER**

---

**2 — THE RISK MANAGEMENT NETWORK**

---

**3 — INFORMATION TECHNOLOGY FOR RISK MANAGERS**

---

**4 — TOTAL COST OF RISK**

---

**5 — DUE DILIGENCE**

---

**6 — MANAGING THE RISK OF INTANGIBLE ASSETS**

---

**7 — EXECUTIVE RISK**

---

**8 — INTERNATIONAL & MULTINATIONAL RISKS**

---





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





# Certified Risk Managers

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

## Section 1

# The Risk Manager





## Key Terms



# The Risk Manager

## Section Goal

To provide participants with a solid understanding of the risk manager's role as they build skill sets that add value to the organization and create long-term success:

## Learning Objectives

1. By using knowledge of the **typical responsibilities** and the technical, soft, leadership and managerial **skill sets** of an effective risk manager, participants will explain the **value of** an effective risk manager.
2. By using knowledge of the **Management Model**, participants will argue the value of implementing it.
3. By using knowledge of the **requirements for long term program success**, participants will understand how to effectively **implement and monitor** a risk management program.



## **Learning Objective 1:**

Using knowledge of the **typical responsibilities** and the **technical, soft, leadership, and managerial skill sets** of an effective risk manager, participants will explain the **value of** an effective risk manager.

---

## The Risk Manager

... is mindful that the practice of risk management is constantly evolving, growing and maturing and is always committed to treating current and emerging risks using the methods most beneficial, economical, feasible and sensible on behalf of management, boards of directors, shareholders, employees and the general public.

... understands that the risk management department is uniquely positioned to be a repository of vast amounts of information which may need to be analyzed and communicated to many different stakeholders.

... is committed to ensuring that risk management is understood throughout the organization. Its success rests entirely with those who have the ability to execute risk management strategy, regardless of the individual's role in the organization.

## Who Is a Risk Manager?

1. The size of the organization and the available resources will determine the approach to risk management. There could be:
  - a. A single dedicated risk manager
  - b. A risk management department
  - c. Other employees – depending on job functions and specialties (CEO, HR, etc.)
  - d. Outside providers, such as an insurance agent or a consultant

2. Potential reporting structures

The risk management professional should interface with and report directly to the highest level of management which varies with each firm. A risk manager may report to the:

- a. Chief financial officer
- b. President or chief operating officer
- c. Human resources director
- d. Legal counsel
- e. Head of administration/operations
- f. Risk management committee

## **The Reporting Structure May Affect:**

1. Risk appetite – legal would be more risk averse, whereas marketing would be more risk tolerant
  
2. The areas of focus for the risk manager – legal would be more focused on compliance and insurance, while human resources would be more people-oriented, focusing on safety and workers compensation



## PRACTICE EXERCISE

To whom do you report? Human resources, accounting, operations, legal or the president?

Which of these would have the greater risk appetite?

What is the best fit?

What other things can the reporting structure impact?

Which structure would allow you to be most effective?

## What Does a Risk Manager Do?

The role of the risk manager is to implement and manage an organization's risk management program through risk identification, analysis, control, financing and administration techniques, ensuring that the organization's assets and financial statements are protected.

### Typical responsibilities include:



1. Developing risk management policies and procedures
2. Claims and litigation management
3. Risk financing through transfer and retention
4. Contract and lease reviews
5. Management of the risk management team
6. Cost of risk allocations
7. Overseeing safety training and loss control programs
8. Accident investigation
9. Risk Management Information System (RMIS)
10. Crisis management and business continuity programs
11. Regulatory compliance

**Types of risk managers:**

1. Strategic risk managers
2. Risk and insurance managers
3. Credit risk managers
4. Financial risk managers
5. Technology risk managers

## Skills of an Effective Risk Manager

Risk managers will be challenged by others about the concepts that they are introducing to the organization. Without the proper skills, the risk manager is ill-equipped for the job and could potentially damage relationships and harm the risk management program.

**Technical Skills** – the risk manager needs to have expertise in:



1. Efficiently identifying risks
2. Analyzing losses and exposures
3. Selecting and implementing appropriate safety and loss control programs
4. Managing claims and investigations
5. Managing the organization's insurance program
  - a. Matching identified risks to available coverages
  - b. Selecting best provider option – agent/broker/insurer
  - c. Performing cost benefit analyses for retention vs. transfer options
6. Reviewing contracts for risk-related implications
7. Accounting and finance
8. Ensuring compliance with regulations
9. Managing relationship between the industry and the organization



## Soft Skills



1. Emotional intelligence – the art of dealing with people in a sensitive and effective way
  - a. The capability of individuals to recognize and understand their own and other’s emotions; to manage and/or adjust behaviors to navigate social complexities and to make informed decisions
  - b. Enhances communication and interactions on a daily basis
2. Diplomacy
  - a. The art of negotiation and conflict management
  - b. Tactfulness
3. Facilitation
  - a. Promote an open exchange of information
  - b. Encourage cooperation
  - c. Encourage efficiency and effectiveness of processes through communication
  - d. Support and encourage risk management efforts
4. Communication
  - a. Adapt message to the audience
  - b. Practice active listening

## Leadership Skills



1. Ability to stay level-headed/objective in a crisis
2. Proactive
3. Accepts responsibility
4. Solution-minded
5. Innovative and inquisitive
6. Motivational
7. Trustworthy
8. Awareness that leadership does not necessarily equate to management or authority

## Managerial Skills

1. Experience with policy and strategy development and implementation
2. Experience with general management and project management

**They are knowledgeable.**



**They have access to tools and expertise.**

**They have been empowered to make decisions.**



## Value of an Effective Risk Manager

Some of the value added by the risk manager can be quantified, while other value may simply be qualitative in nature.

**Some of the ways a risk manager adds value to the organization include:**



1. Elevating the importance of risk management by:
  - a. Establishing senior management's proactive support of risk management objectives and policies
  - b. Creating understanding and acceptance of risk management policies and procedures across the organization
  - c. Illustrating the value risk management discipline brings to the organization
  - d. Reinforcing a positive organizational risk culture (a set of understandings, habits, beliefs, values and knowledge) *towards risk*
2. Supporting measured risk-taking to:
  - a. Achieve business objectives
  - b. Improve planning and budgeting
  - c. Reduce frequency and severity of incidents, accidents, losses and claims

- d. Increase awareness of indirect losses and the connections between risks
- e. Prioritize resources for proactive preparation vs. reactive response
- f. Improve morale and productivity among the workforce
- g. Improve processes and technology
- h. Protect the organization's reputation and brand
- i. Impact financial results
  - 1) Reduces claims management and legal costs
  - 2) Optimizes total cost of risk
  - 3) Protects cash flow, assets and financial statements
  - 4) Increases stock prices due to investor confidence
  - 5) Improves competitive position within the market and industry



### **Learning Objective 2:**

Using knowledge of the **Management Model**, participants will argue the value of implementing it.

---

## **Planning, Organizing, Leading, and Evaluating (POLE)**

Traditional management involves Planning, Organizing, Leading, and Evaluating (POLE) the resources of people, funds, materials and time to protect the organization's assets and positively affect the organization's performance.

**Planning** – determining a course of action

1. Identify goals
2. Establish a roadmap – necessary steps to meet the goal
3. Consider economic and resource variables



**Organizing** – the allocation of resources and responsibilities

1. Bring together necessary resources to meet objectives – physical, human, financial
2. Assign responsibilities or delegate authority
3. Coordinates activities of external and internal team members

**Leading** – motivating people to take action

1. Provide clear direction and goals
2. Use sound judgment to make effective decisions
3. Work within formal and informal networks to foster open communications – builds relationships at all levels of the organization
4. Promote teamwork and cooperation
5. Remove obstacles to employee performance
6. Reward, inspire and help develop potential
7. Be a positive role model

**Evaluating** – measuring achievement against established goals

1. Establish benchmarks and performance standards
2. Compare actual performance to the standards
3. Take corrective action where necessary
4. Submit reports and communicate results to senior management



## PRACTICE EXERCISE

**Goal: To Reduce Claim Costs**

Planning

Organizing

Leading

Evaluating





### Learning Objective 3:

Using knowledge of the requirements for **long term program success**, participants will understand how to effectively **implement and monitor** a risk management program.

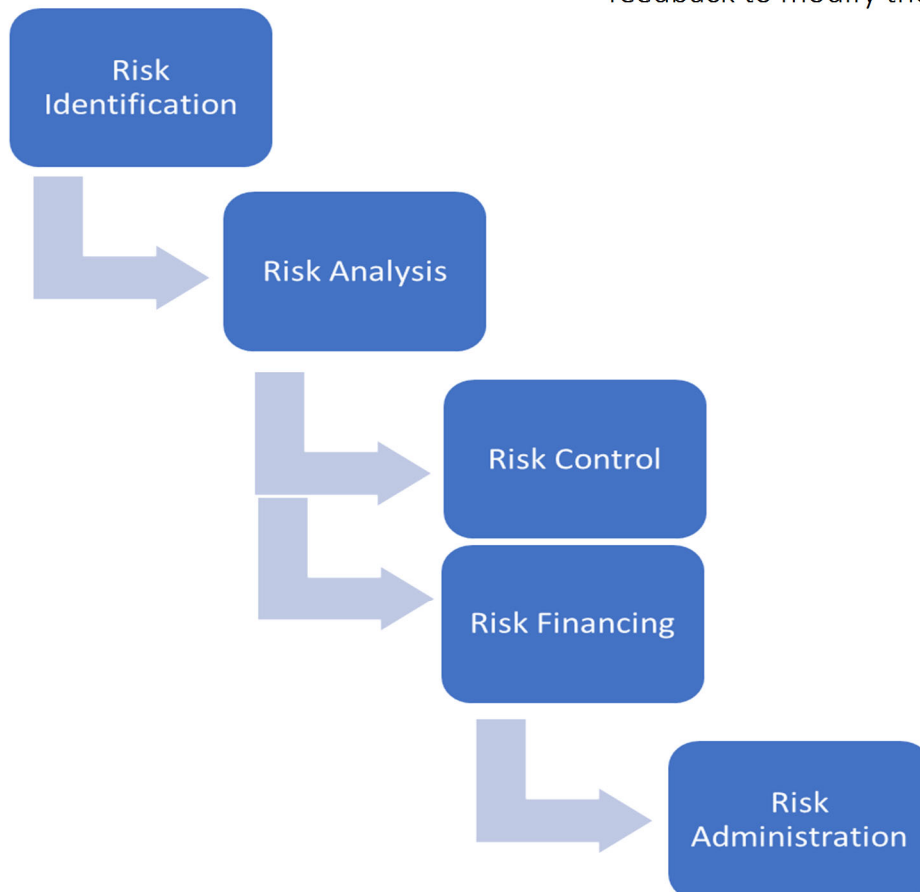
## Implementation and Monitoring of a Risk Management Program

### Implementation

The part of administration where the desired actions and plans of the risk management department are initiated.

### Monitoring

The part of administration where risk management examines and evaluates the results of the actions and plans and then uses that feedback to modify the process.



## Implementation



1. Present the risk management policy and procedure manual to the organization and other applicable service providers
2. Communicate risk management goals and objectives throughout the organization
3. Demonstrate the organization's commitment to risk management principles
4. Create an organizational chart or flowchart showing risk management's interaction with other departments
5. Establish and communicate individual responsibilities and accountabilities for the success of the risk management program

6. Partner with various levels of the organization
  - a. Executive management
    - 1) Actively involved in the rollout of the program
    - 2) Thank them for providing resources to achieve program objectives
  - b. Middle management/supervisors
    - 1) Provide necessary support to achieve risk management goals and objectives
    - 2) Active engagement of this group is required for executing loss control programs, claims gathering information, observations, ideas and feedback.
  - c. All other employees
    - 1) Daily activities are affected by risk and loss control measures, therefore their cooperation, input and insight are needed
    - 2) Engagement determines the effectiveness of the risk management policies and loss control procedures

## Monitoring



1. Evaluate the effectiveness of the program
  - a. Significant incidents/accidents
  - b. Open/closed claims
  - c. Litigated claims, large loss claim reports
  - d. Risk financing options with an analysis of the deductible/SIR (self-insured retention) levels and limits
  - e. Total cost of risk and allocation
  - f. Loss trend analysis
  - g. Contractual issues

2. Periodically review risk management policies and procedures
  - a. Changes in operations/acquisitions/divestiture
  - b. New products and services
  - c. New laws and regulations
  - d. Annual quality control
3. Report on results, opportunities, threats, successes and recommendations. Frequency of reports can be:
  - a. Time driven
  - b. Event driven
  - c. Issue driven
4. Reviews and adjustments – feedback, process experience, changes in needs and management, document reviews



### **The Risk Manager Must:**

- 1) Have objectives that align with the needs of the organization
- 2) Be an active participant on the organization's leadership team
- 3) Find advocates or influencers who reinforce commitment and encourage resource allocation
- 4) Create adaptable processes and approaches – evolving over time to fit new needs, best practices and emerging risks
- 5) Never change for the sake of change – utilize existing processes that have effective risk management elements and continue utilizing those processes instead of creating duplicate/alternate work
- 6) Select appropriate technology that supports the risk management process – don't let software dictate your process
- 7) Seek continued professional development through education and training – job specific, trends, best practices



## The Risk Manager

Apex Products has always relied on its insurance agent for risk management expertise but is frustrated by its increasing insurance program costs. Apex's president is considering formalizing the risk management process within the company. She is not sure if she should hire a full-time risk manager, contract with an independent consultant or see if her agent can structure the services on a fee basis. Currently, the CFO handles the insurance program and gets regular loss runs from the carriers through the agent.

1. If Apex decides to hire a full-time risk manager, what effect should he or she have on the company? What added value can a risk manager bring to the company?
2. Apex does not have any formal risk management program since the agent has been the "acting" risk manager. What qualities or skills should Apex look for when hiring a risk manager?
3. Assuming Apex decides to hire either a full-time risk manager or a risk management consultant, what would his or her standard responsibilities be?
4. Depending on what reporting structure Apex designs for its risk management department, what potential conflicts may arise with the current structure?
5. If Apex wants its risk manager to be successful, Apex will have to support risk management initiatives. What other things will the risk manager need to do to have long-term success?

## Review of Learning Objectives

1. Using knowledge of the typical responsibilities and the technical, soft, leadership and managerial skill set of an effective risk manager, participants will explain the value of an effective risk manager.
2. Using knowledge of the Management Model, participants will argue the value of implementing it.
3. Using knowledge of the requirements for long term program success, participants will understand how to effectively implement and monitor a risk management program.





# Certified Risk Managers

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

## Section 2

# The Risk Management Network



## Key Terms



## The Risk Management Network

### Section Goal

To provide necessary skills to:

- Gather expertise through the structuring of the risk management network
- Facilitate effective communication through the appropriate communication channels
- Utilize the risk management network
- Write an effective stewardship report

### Learning Objectives

1. By using an understanding of **risk management's involvement** throughout an organization, participants will be able to collaborate with a **network of members** to build the expertise necessary to run an effective risk management program.
2. By using knowledge of the **four-step communication process**, participants will be able to facilitate productive communication through the appropriate **channels**, fostering teamwork and cooperation.
3. By determining what is **mission critical and business critical** to the organization, participants will be able to build a **network of risk-aware individuals** across departments who will help to implement and maintain a risk management program.
4. By using an understanding of the **audience and stakeholders**, participants will be able to write a stewardship report which includes **risk management program information, key performance indicators and key risk indicators** to communicate the integration of risk management and build a risk-aware culture.



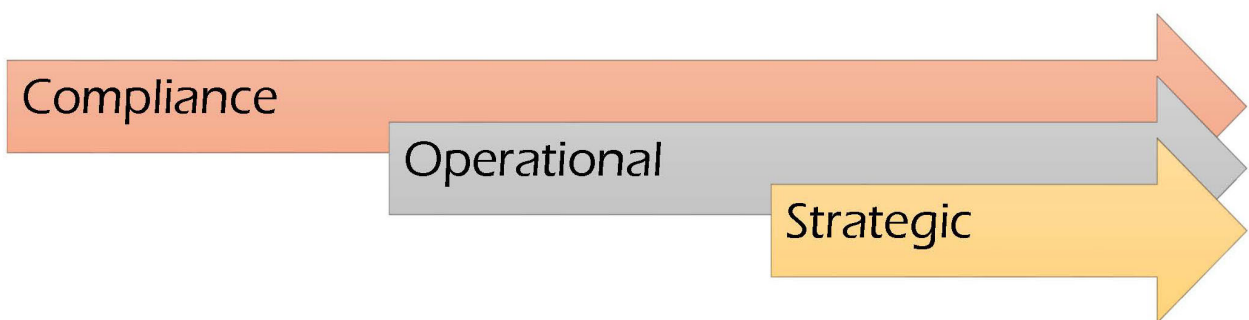
### Learning Objective 1:

Using an understanding of **risk management's involvement** throughout an organization, participants will be able to collaborate with a **network of members** to build the expertise necessary to run an effective risk management program.

The risk management team's interactions within the organization are heavily dependent on the organization, industry, culture and size.

Risk management must have a strong foundation of legal compliance to stay in business. To ensure long-term stability, a more functional (operational) approach is necessary. For an organization to experience sustainable growth, the risk management function must also be involved at a strategic level.

### Risk Management Involvement



	Compliance	Operational	Strategic
<b>Goal</b>	Legal Operations	Safety and stability	Capitalize on opportunity and mitigate threats
<b>Examples</b>	Legal Regulatory Audit Contracts	Health and Safety Environmental Insurance Business Continuity	Expansion Plans Product Development Due Diligence Corporate Goal Achievement Reputation Management Growth

Effective risk management is never a one-person job. Resources outside the risk management department are required to be effective. A successful risk manager builds a network of support and expertise.

## The Risk Management Network

Risk managers need a network of connections and people because they need access to information and expertise they don't have. A risk manager should use services of others, both internal and external, to achieve the risk management objectives. Selecting outside service providers requires knowledge of who, what, when and how to work with them.

**Additional resources** may be required when:

1. An outside or objective viewpoint is required
2. Time is of the essence
3. An outside expert is more cost effective
4. Upper management requests it
5. A limited term activity or special project arises



## Members of the network

1. Formal groups vs. informal connections (internal, external, etc.)
2. Expertise including, but not limited to:
  - a. Risk management
  - b. Health, safety and environmental
  - c. Human resources
  - d. Functional areas of the organization
  - e. Legal
  - f. Agents, brokers, carriers, captive managers
  - g. RMIS providers
  - h. Actuaries

## How to identify the best fit for network members

1. Background
2. Roles and responsibilities
3. Soft skills, including working effectively with others
4. Time availability

The risk manager/risk management team are in a unique position in that they have knowledge of and visibility in all areas of the organization. As a result, they have the opportunity to build risk awareness by facilitating communication across the organization.

**Good communication is essential to:**

1. Foster cooperation and active participation
2. Identify any changes or influences that impact organizational performance

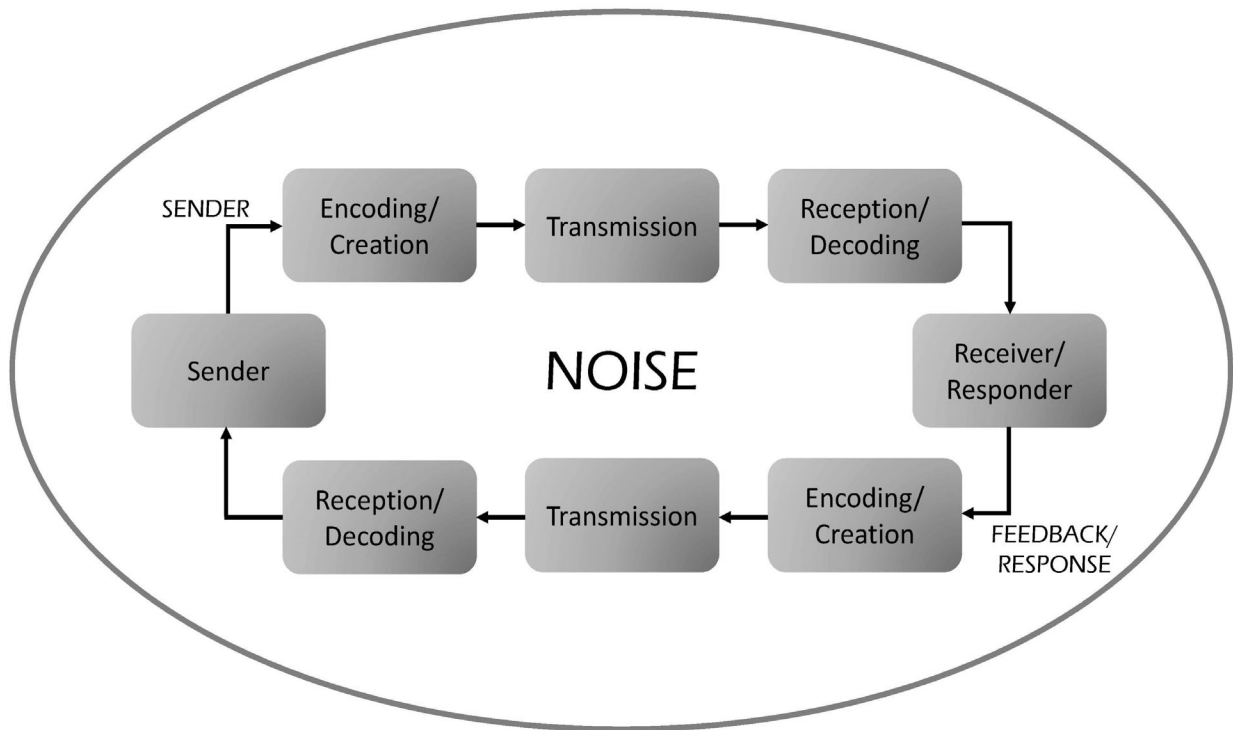




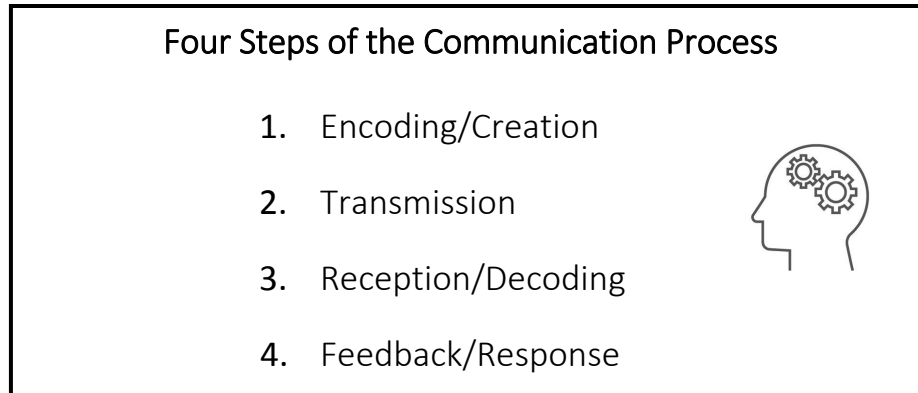
**Learning Objective 2:**

Using knowledge of the **four-step communication process**, participants will be able to facilitate productive communication through the appropriate **channels**, fostering teamwork and cooperation.

Basic Communication Process



Effective communication uses appropriate context and includes scope, goals, outcomes (expected or actual) and resources (available and required).



### **Step 1: Encoding/Creation**

1. Is this a message that needs to be delivered?
2. Content of the message:
  - What information should be provided and at what point in time?
  - How much detail is needed?
  - Does the receiver have enough context to understand the message? Or do you need to provide information such as background, setting or framework for additional understanding?

## Step 2: Transmission

1. Is there a time frame for transmitting the message?
2. What is the appropriate medium to convey the information?
3. Face-to-face, phone call, email, formal written document, etc.
4. Written communication creates a more permanent means of sharing information that allows the writer to more carefully consider content and tone.

Note: Email is discoverable in litigation and, because of its rapidity of use and dissemination, duplicative ability, informal language and potential lack of proofreading, can easily create problems for an organization.

## Step 3: Reception/Decoding

1. The receiver will interpret the message for understanding and expectations.
2. The receiver's response will be determined by his or her understanding. Were you clear in your communication to influence the understanding you wanted?
3. The expectation is that the message was communicated efficiently and effectively.

## Step 4: Feedback/Response

1. Message back to sender
2. Action taken
3. Question or request for clarification

## Communication “noise”

Anything that distorts a message by interfering with the communication process is considered “noise”; it can affect the process at any stage, take many forms and may not always be recognizable.

1. How will you know if “noise” interfered?
  - Was the communication ineffective? Did it produce the desired result?
  - Was there interference in the process that influenced the response?
  
2. What causes “noise”?
  - Ambiguous, incomplete or incorrect wording
  - Internal or external distractions experienced by sender and/or receiver
  - Misinterpreted nonverbal cues
  - Misunderstanding due to diversity of experience or cultural differences



**Linear channels** – one-way communication where there is no feedback expected from the receiver; typically used for mass communication, harder to gauge effectiveness

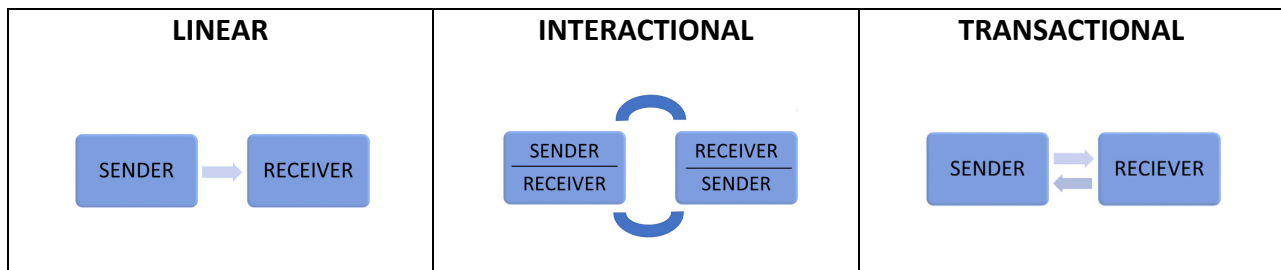
- Examples: directions to subordinates, policy and procedure manuals, organizational notifications, advertisements, signage

**Interactional channels** – this model has two linear models stacked on top of one another, where communication includes feedback; typically found in modern communication methods such as email, instant messaging or texting

- Examples: discussion boards, social media sites, interactive marketing

**Transactional channels** – communication where the roles between sender and receiver are interchangeable; typically used for interpersonal communication like a phone call, face-to-face interaction or video chat

- Examples: advice, problem-solving discussions or activity coordination



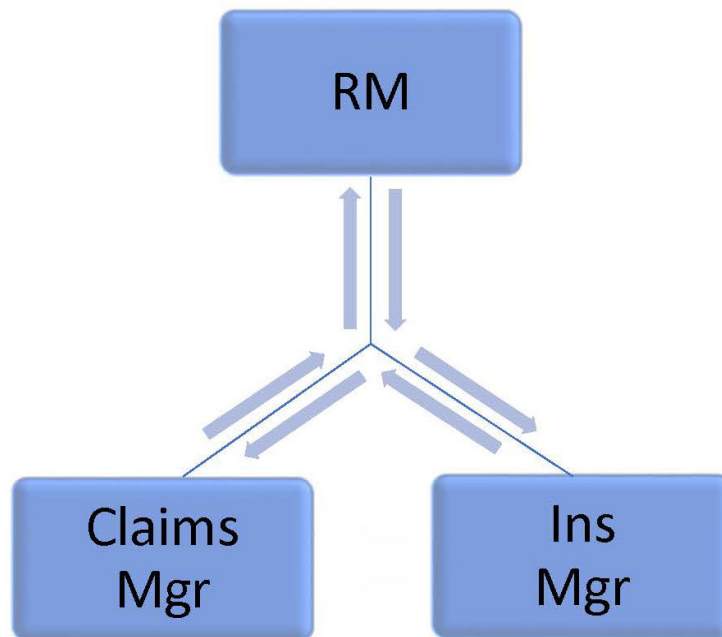
## Communication Networks

Communication networks differ according to the structure of the organization and depict the directional pattern of communication flow within the organization.

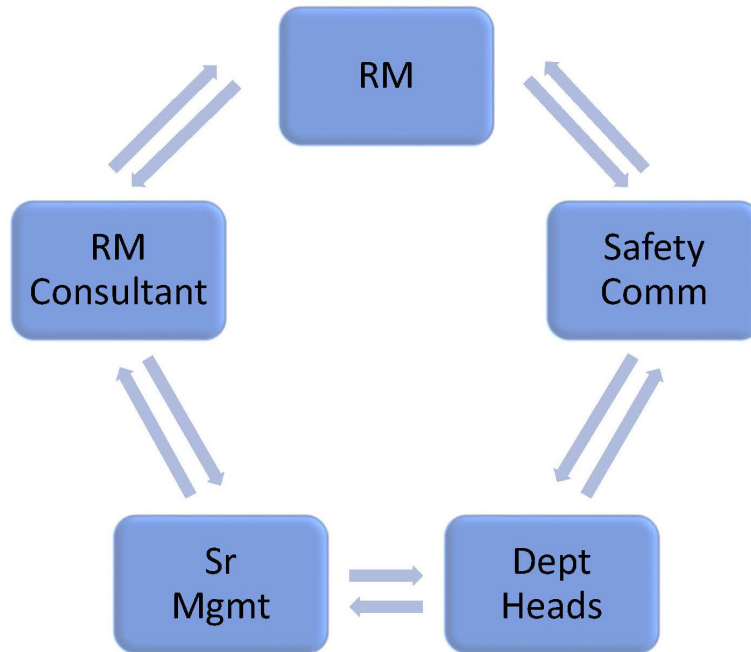
**Chain network** – individuals linked through common activity or purpose



**'Y' network** – individuals linked through a hierarchy or span of control



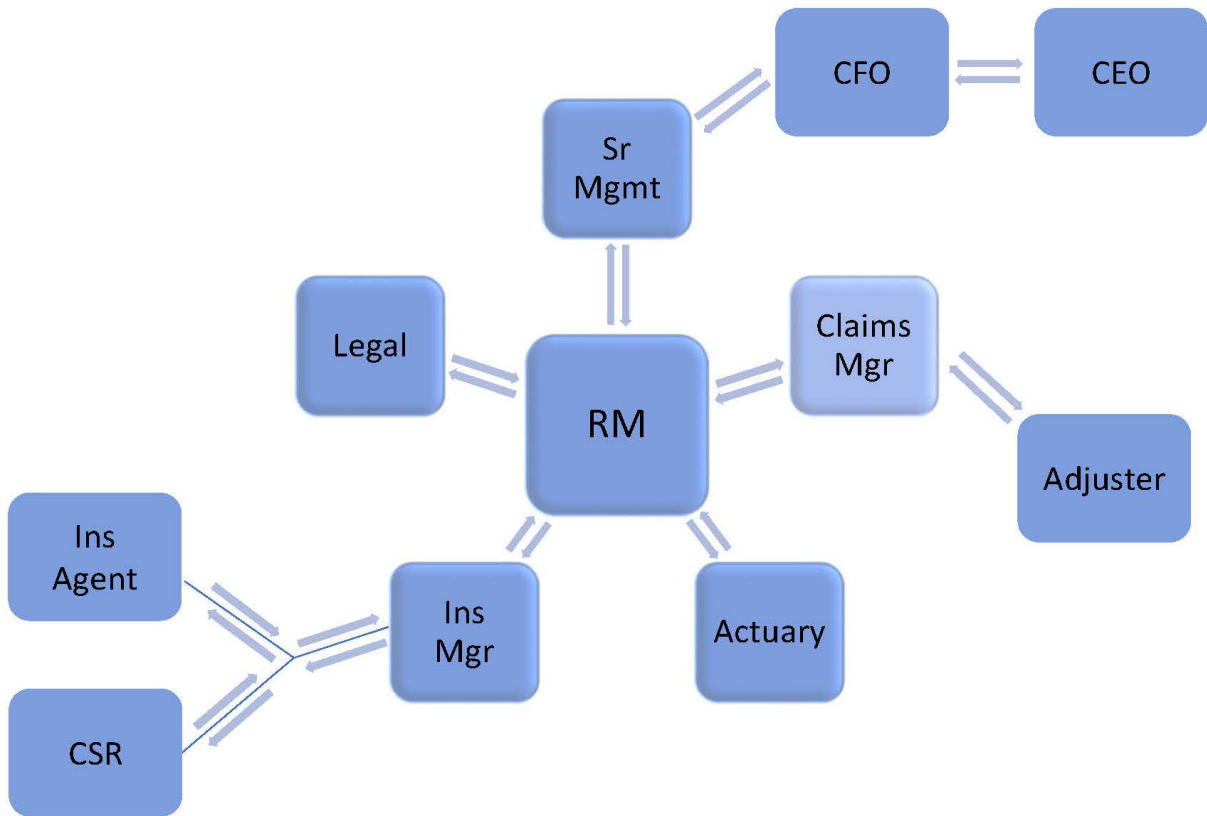
**Circle network** – peer communication



**Wheel network** – one individual who receives and disseminates information to others, such as in a crisis communication network with one spokesperson



**All-channel network** – network of linked networks







### Learning Objective 3:

By determining what is **mission critical** and **business critical** to the organization, participants will be able to build a **network of risk-aware individuals** across departments who will help to implement and maintain a risk management program.

Understanding communication methods and pathways is critical to the risk manager as he or she acts as a liaison between all of the varying functional departments of an organization. The risk manager needs to have the skills to coordinate and facilitate cooperation among those groups. Additionally, the risk manager needs to be able to organize and lead the network of individuals who directly support and assist the risk management function.

### Using your network to implement and maintain your risk management program

The risk manager has the opportunity to break down silos to create a plan for growth and success. By identifying and addressing the weaknesses and threats that inhibit sustainability, the risk management team can better support growth.

### What type of critical business or critical processes does the organization have?



1. Mission critical – factors such as equipment, processes, personnel, utilities that are essential to the survival of business operations; failure of one of these can seriously damage business operations

Examples: online banking, electricity, computer systems

2. Business critical – factors that make operating difficult or inconvenient and could create serious financial or legal consequences

Examples: email systems, automation processes, computer programs

What may be considered a mission critical or business critical situation varies based upon type of organization or business function.

### **Determining what is most important**

1. What is mission critical to the organization?
2. What is business critical to the organization?
3. What is mission/business critical to each functional department?
4. What are the interdependencies between functional departments?
5. What is the risk tolerance for each critical element?
6. What are the impacts of critical exposures on individual departments as well as the organization as a whole?

### **Fostering teamwork**

Building a network of risk-aware individuals across departments helps break down silos to create the cross-functional approach to risk management.



By tying risk management programs and communication to business-critical exposures, the risk manager can better articulate the value of risk management.



### Learning Objective 4:

Using an understanding of the **audience and stakeholders**, participants will be able to write a stewardship report which includes **risk management program information, key performance indicators and key risk indicators** to communicate the integration of risk management and build a risk-aware culture.

While communication between the risk management department, its network and the rest of the organization is an ongoing process, the most comprehensive communication regarding the state and efficacy of the risk management program is the stewardship report. A steward is a person responsible for overseeing and protecting something worth caring for and preserving.

The risk management department is a steward of the organization's assets: property, human resources, liability and net income. A key aspect of championing a risk-aware culture is to communicate how the risk management program is integral to protecting these assets while being aligned with the organizations mission, strategic objectives and risk tolerance philosophy.

**Definition:** A formal summary of the objectives, accomplishments and challenges of the risk management efforts that is shared with appropriate management, the board of directors and stakeholders.

**Purpose:** The purpose of a stewardship report is to provide an overview of risk management programs which will identify successes, challenges and opportunities for improvements that are aligned with an organization's mission and operational and strategic goals. The needs and focus of each stakeholder will drive the content, presentation, delivery method and frequency (annual or as needed). An effective stewardship report uses metrics to illustrate the risk management story and includes critical information of interest to each stakeholder.

### **Audience/Stakeholders**



Communication coming from risk management will have a broad audience with varied interests.

Possible stakeholders:

- Employees
- Managers
- C-suite
- Board of directors
- Investors and stock exchange entities
- Clients/consumers
- Agents/brokers, underwriters and other key vendors such as third-party administrators (TPAs) and RMIS
- Regulatory and other authorities

A risk manager is responsible for setting standards, practices and procedures and embedding them in business processes, as well as aggregating information needed to report to various stakeholders. The content will include information (graphs, charts and text) that can be easily segmented for presenting key data to match each stakeholder’s needs. Data should be compiled, reviewed and analyzed prior to publishing and distributing.

The following is common content, not an exhaustive list:

### **Risk Management Program Information**



- Mission statements and core values for both the organization and risk management department, including risk tolerance philosophy
- Loss control and claims management updates
- Insurance trends and projections projects and initiatives
- Summaries from external support team (TPA, RMIS and agency services such as loss control, engineering etc.)

## Key Performance Indicators (KPI)



- Liquidity ratios
- Profitability measures
- General and administrative costs
- Return on investment

## Key Risk Indicators

- Benchmarks, both internal and external
- Total Cost of Risk
- Employee turnover (churn rate)
- DART (days away restricted or transferred) rate
- Workers compensation experience modifier

### **Presentation and Delivery Methods**

The type of presentation and mode of delivery will depend on your audience and what will create the best impact and awareness. Today there are many methods to distribute information, such as social networks, electronic reports, email, printed material.

Consider the following when determining the type of presentation and mode of delivery:

- Confirm management’s expectations
- Mode of delivery (in person, online webinar, etc.)
- Determine who will present the report (risk manager, broker or both as a team)

### **Stewardship Reports in Action**

The board might be interested in an executive “State of Risk Management” report, showing the risk management issues that may affect (negatively and/or positively) the accomplishment of strategic objectives and forecasting its impact on financial performance and brand reputation.

Management would have more detailed reports showing impact on operational objectives and performance goals.

Other internal stakeholders might need a KPI on performance outcomes and impact of key loss control programs.

External reporting can be used for marketing at renewal to communicate progress and improvements. It also serves as a method for communicating your operational and strategic objectives when having the annual stewardship meeting with your key external risk management support team (broker, TPA and RMIS vendor)

## Review of Learning Objectives

1. Using an understanding of risk management's involvement throughout an organization, participants will be able to collaborate with a network of members to build the expertise necessary to run an effective risk management program
2. Using knowledge of the four-step communication process, participants will be able to facilitate productive communication through the appropriate channels, fostering teamwork and cooperation.
3. By determining what is mission critical and business critical to the organization, participants will be able to build a network of risk-aware individuals across departments who will help to implement and maintain a risk management program.
4. Using an understanding of the audience and stakeholders, participants will be able to write a stewardship report which includes the risk management program information, key performance indicators and key risk indicators to communicate the integration of risk management and build a risk-aware culture.





## Certified Risk Managers

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

### Section 3

# Information Technology for Risk Managers



### Key Terms



# Information Technology for Risk Managers

## Section Goals

To provide participants with the core competencies to:

- Secure, organize and utilize data in alignment with legal compliance and best practices
- Assist with a data risk assessment
- Select and utilize a Risk Management Information System (RMIS)
- Conduct a benchmark study to properly analyze an organization's risk management performance

## Learning Objectives

1. By using an understanding of the **acts and rules** that apply to data security and the **four parts of Data Risk Assessment**, participants will provide a foundational argument for using data in the risk management process.
2. By using knowledge of the **functions and purchasing considerations** of a Risk Management Information System (RMIS), participants will be able to evaluate the **characteristics of a RMIS** to assess whether it would meet the organization's needs.
3. By using knowledge of the **methods of, appropriate times for, and advantages and disadvantages** of benchmarking, participants will be able to navigate through the **steps of the benchmarking process**.





### Learning Objective 1:

Using an understanding of the **acts and rules** that apply to data security and the **four parts of Data Risk Assessment**, participants will provide a foundational argument for using data in the risk management process.

### Introduction

Almost all organizations use technology to conduct business. The risks associated with data security continue to evolve and emerge as one of the top risks for business entities. The ever-increasing number of cyberattacks and breaches threaten to have an adverse impact on the financial assets and reputations of these organizations and emphasizes the need to control these exposures.

Risk managers need to be highly aware of their organization's functions related to data storage and security. They need to work with all departments and teams that have access to or collect data. They also need to serve as an intermediary between the various departments and senior management to ensure that the organization has identified all of its data-related exposures and has taken proactive steps to manage them. Although the risk manager may not have the control over or expertise regarding each department's decisions related to data storage and security, they need to be aware of all the laws, regulations and ramifications of those decisions.



Legislation enacted at various levels – state, federal, etc. – may affect the organization depending on the type of business transactions they perform and the types of data they collect, process and store. Additional legislation is introduced as risks continue to evolve.



### **Gramm-Leach-Bliley Act of 1999**

1. Applies to financial institutions – banks, brokerages and insurance companies
2. Must securely store personal information
3. Must disclose policies regarding information sharing and allow customers the opportunity to opt out

### **Data Security and Breach Notification Act of 2015**

1. Requires business entities to:
  - a. Employ security measures that protect data from unauthorized access
  - b. Restore data systems, data integrity and confidentiality after a security breach
  - c. Determine whether a breach will result in economic loss, identity theft or financial fraud
2. In event of a breach, requires business entities to notify:
  - a. Affected U.S. residents
  - b. The FTC and U.S. Secret Service or FBI
  - c. Consumer reporting agencies if more than 10,000 individuals are affected

## Fair and Accurate Credit Transactions Act of 2003 (FACT Act or FACTA)



1. Allows consumers to request and obtain a free credit report once every twelve months
2. Contains provisions to help reduce identity theft, such as the ability to place alerts on credit histories if identity theft is suspected, and requires secure disposal of consumer information
3. Also requires reporting agencies to block reporting of any information in a consumer's file that has originated from an alleged identity theft

3

**Cybersecurity Information Sharing Act of 2015 (CISA)** – makes it easier for companies to share personal information with the government, especially in cases of cybersecurity threats

1. Creates a system for federal agencies to receive threat information from private companies
2. Includes provisions to prevent sharing data known to be both personally identifiable and irrelevant to cybersecurity

**Red Flags Rule** – created by the FTC to help prevent identity theft; applies to financial institutions and creditors

1. **Financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a consumer
2. **Creditor** applies to any entity that regularly extends or renews credit – or arranges for others to do so – and includes all entities that regularly permit deferred payments for goods or services

A creditor:

- a. Obtains or uses consumer credit reports and provides information to consumer reporting agencies, or
- b. Advances funds which must be repaid in the future (or against collateral)

## Additional Legislation Includes:



# COMPLIANCE

### **Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended**

- Any healthcare provider that electronically stores, processes or transmits medical data must comply with HIPAA regulations
- Sets standards for documentation, handling and privacy of medical records
- HIPAA Security Rule – defines what administrative, physical and technical safeguards must be in place and defines who may have access to the data
- Provides a set of standardized codes for medical data – diagnoses, procedures and drugs

### **Federal Information Management Security Act Of 2002 (FISMA)**

- Applies to federal agencies
- Has brought attention within the federal government to cybersecurity and explicitly emphasizes a “risk-based policy for cost-effective security”
- Requires agency program officials, chief information officers and inspectors general (IG) to conduct annual reviews of the agency’s information security program and report the results to the Office of Management and Budget



**Fair Credit Reporting Act (FCRA)** was enacted to promote the accuracy, fairness and privacy of information gathered in the files of consumer reporting agencies

- Intended to protect consumers from inaccurate information in their credit reports; the FCRA regulates the collection, dissemination and use of consumer information
- The FCRA forms the foundation of consumer rights law in the United States; originally passed in 1970, it is enforced by the FTC, the Consumer Financial Protection Bureau and private litigants

#### **Data Quality Act (DQA) or Information Quality Act (IQA)**

- Applies to the sharing by federal agencies of, and access to, information disseminated by federal agencies, and
- Requires that each federal agency to which the guidelines apply:
  - Issue guidelines ensuring and maximizing the quality, objectivity, utility and integrity of information (including statistical information) disseminated by the agency by not later than one year after the date of issuance of the guidelines
  - Establish procedures allowing affected persons to seek and obtain a correction of information maintained and disseminated by the agency that does not comply with the guidelines
  - Report periodically to the director of the Office of Management and Budget:
    - The number and nature of complaints received by the agency regarding inaccuracy of information disseminated, and
    - How such complaints were handled by the agency



## PRACTICE EXERCISE

In your organization, what types of data do you collect, process or store?

What compliance issues do you face?

What other responsibilities come with handling data? Consider social, contractual, etc.



# DATA RISK ASSESSMENT

**Data Inventory**

What data do you have?  
What type?  
How many records?  
Sensitive data?



**Data Risk Analysis**

Why is data risky?  
Does type and quantity of make you a target?  
Potential repercussions of a release?



**Data Mapping**

What is the flow of data?  
Multiple databases?  
Who is data shared with?



**Data Protection**

What has been done to protect the data?  
Firewalls?  
Security measures and policies?  
Training of employees?  
Are policies monitored and enforced?



**Data Risk Assessed**

**Data Inventory – What data do you have?**

1. What types of information are collected and stored?
2. How many records are kept?
3. Are the files sensitive in nature and are they subject to compliance?
  - a. Personally Identifiable Information (PII)
  - b. Personal Health Information (PHI)
  - c. Personally Identifiable Financial Information (PIFI)
  - d. Claims data
  - e. Intellectual property
  - f. Data of others (subject to confidentiality agreements)

# WHAT DATA DO YOU HAVE?



## PERSONALLY IDENTIFIABLE INFORMATION

Full Name, Social Security Number, Date Of Birth, Drivers License Number, Passport Number, Phone Number, Email Address, Birthplace, Home Address.

## PERSONAL HEALTH INFORMATION

Medical History, Demographic Information, Test Results, insurance information., Health Care Payments



## PERSONALLY IDENTIFIABLE FINANCIAL INFORMATION

Account Balances, Payment History, Credit or Debit Card Purchase Information, Credit Report Information

## CLAIMS DATA

Will most likely include PII, PHI, and PIFI, as well as injury Details, Procedure Codes, Settlement Amounts, and Provider Information



## INTELLECTUAL PROPERTY

Patent, Copyright, Trademark, Trade Secret, License, Franchise, Designs, and Manuscripts

## DATA OF OTHERS

What information do you have that doesn't belong to you? It may be subject to contractual liability or a confidentiality agreement.



### **Data Risk Analysis – Why is retention of data risky?**

1. Records have value
2. The type and quantity of data stored may make the organization a target for hacking, identity theft, cyberterrorism, extortion, corporate espionage, etc.
3. The greater the volume, the greater the risk release creates
4. What are the potential repercussions associated with the release of the information?
  - a. Direct – data restoration, client notification, credit monitoring, investigation, loss of service, regulatory penalties, lawsuits, etc.
  - b. Indirect – reputation, loss of goodwill, etc.

### **Data Mapping – Tracking of the data cycle, from point of input through storage to output, to identify the organization’s systems that are involved and that expose the organization to risk**

1. Multiple databases
  - a. HR – employee records, performance appraisals, benefits
  - b. Accounting – accounts payable, accounts receivable, fixed assets, payroll
  - c. Procurement – vendor data, insurance information, product pricing
  - d. Proprietary information – scientific, market information, R&D, trade secrets
  - e. Claims management system
2. Information exchange – who is data shared with?
  - a. Between departments
  - b. With outside parties

**Data Protection and Exposure Reduction** – What steps have been taken by the organization to protect the data and reduce the exposure?

- 1. Testing for firewalls, vulnerability, password strength, etc.
  
- 2. Implementing new security measures and policies

Biometrics	Mandatory password change	Email limitations
Attachment limitations	Antivirus software	Run updates on schedule
Secure laptops	Encryption	Secure smartphones
Remote wiping	Regularly scheduled backups	Restricted downloads

- 3. Training and educating employees
  
- 4. Monitoring and enforcing policies



---

---

# DATA RISK ASSESSMENT CHECKLIST

---

## DATA INVENTORY

---

---

- Determine the types of data collected and stored
- How many records does the company store?
- Does the company collect, process or store any sensitive data? (Check all that apply below)
  - Personally Identifiable Information
  - Personal Health Information
  - Personally Identifiable Financial Information
  - Claims Data
  - Intellectual Property
  - Data of Others (subject to confidentiality agreement)

## DATA RISK ANALYSIS

---

---

- All companies are at risk of a data breach. Do any of the following apply to make the company a target?
  - Type of industry
  - Type of data stored
  - Quantity of data
- What are the potential repercussions of a data release?



## DATA MAPPING

---

- What is the data cycle? Consider the following:
  - Input
  - Processing
  - Storage
  - Output
- Multiple databases?
- Is the information shared?

## DATA PROTECTION

---

- Which of the following safeguards are in place to protect data?
  - Firewalls
  - Password strength requirements
  - Penetration testing
- Which of the following security measures and policies are in place?
  - Biometrics
  - Mandatory password changes
  - Email limitations (number of recipients, specific recipients and senders)
  - Email attachment limitations
  - Antivirus software
  - Regular software updates
  - Laptop security
  - Encryption
  - Smartphone security
  - Remote wiping
  - Regularly scheduled backups
  - Restricted downloads
- What employee education and training is in place?
- Is there consistent monitoring and enforcement of the policies?



### Learning Objective 2:

Using knowledge of the **functions** and **purchasing considerations** of a Risk Management Information System (RMIS), participants will be able to evaluate the **characteristics of a RMIS** to assess whether it would meet the organization's needs.

### Characteristics and Functions of an RMIS

As the organization should have selected and designed systems that work for and protect the organization's various functions, the risk manager also needs to select and design a system that works to support the risk management function and to protect the information that a risk manager obtains.

### Characteristics of an RMIS



**Definition of RMIS:** an information system that helps the user to identify, measure and manage risks in the organization or other organizations

RMIS can be a combination of the following:

1. Simple spreadsheet
2. Database using commercial computer applications
3. Highly customized software program tailored to the organization
4. Commercially developed RMIS software offering basic risk services and specialized components running on a variety of platforms

## Functions of the RMIS



1. Supports the user in the key steps of the risk management process: identification, analysis, financing, control and administration
2. Integration with other internal and/or external information systems including real-time event monitors
3. Reports and dashboards
  - a. Trends
  - b. Ad hoc queries
  - c. Heat maps
  - d. Loss forecasting
  - e. OSHA reporting
  - f. Total cost of risk reports and allocations
4. Facilitates the consolidation of the following into one system:
  - a. Insurance policy information, e.g., policy dates and numbers, deductibles or retentions, coverage specifics, certificates of insurance
  - b. Claims information, e.g., date of claim, type of claim, claimant, cause of claim, reserves
  - c. Property schedules, e.g., real, personal, intellectual, intangible and legal interest
  - d. Exposure information, e.g., revenues, vehicles, miles driven, units produced, payroll, number of employees
  - e. Exposure identification information, e.g., checklists, flowcharts, contractual reviews
  - f. Document storage, e.g., safety audits, actuarial studies

## Considerations When Purchasing an RMIS



<b>Costs</b>	<p>Purchase price, setup costs, custom programming</p> <p>Cost benefit analysis (short-term and long-term)</p> <p>Licensing options and costs</p> <p>Service contract pricing/technical support</p> <p>Data storage</p>
<b>Security</b>	<p>Login requirements</p> <p>Security certifications</p> <p>Vulnerability scans</p> <p>Penetration tests</p> <p>Encryption</p> <p>Compliance related to SOC 1, HIPAA, ISO 27001, etc.</p>
<b>Technology</b>	<p>App/mobile compatibility</p> <p>Compatibility with other programs – ability to import and export data into/from various formats</p>
<b>Customer Service/Tech Support</b>	<p>Expertise level</p> <p>Availability</p> <p>International or multilingual staff</p>
<b>Customization</b>	<p>Open architecture or proprietary programming</p> <p>Can it be tailored to client’s industry, special reports?</p> <p>Foreign conversion</p> <p>Availability of related models</p>
<b>Usability/Ease of Use</b>	<p>Dashboards/analytics</p> <p>Speed for data loads, reporting, etc.</p> <p>Does it have all the features/functions needed to meet certain objectives, e.g., can it track TCOR?</p>
<b>Users</b>	<p>RM department</p> <p>Other departments – Finance, HR, Operations</p> <p>Insurance – Agents, Brokers, TPAs</p>
<b>Other Features</b>	<p>Claims management, policy management, reporting, dashboard &amp; analytics and health &amp; safety</p>

# RMIS FEATURES



## CLAIMS MANAGEMENT

- TPA interface
- Carrier interface
- Predictive modeling
- Claims audits



## POLICY MANAGEMENT

- Coverage gaps and overlaps
- Certificate tracking
- Policy and endorsement listing
- Policy modelling
- Deductible tracking



## REPORTING

- Scheduled reporting
- Automatic distribution
- Loss triangulation
- Customized reports



## DASHBOARD & ANALYTICS

- Custom data views
- Communication and collaboration
- Comprehensive RM resource



## HEALTH & SAFETY

- Incident reporting
- DART rates
- Accident/illness investigation
- Root cause analysis



### Learning Objective 3:

Using knowledge of the **methods** of, **appropriate times for**, and **advantages and disadvantages** of benchmarking, participants will be able to navigate through the **steps of the benchmarking process**.

Once a Risk Management Information System has been purchased and put into use, one of the most important functions it will perform for the risk management department is its ability to benchmark performance. The RMIS can track data and compare it over periods of time to show whether the risk management department is operating efficiently and effectively. The RMIS also provides data that can be compared to other organizations and to industry standards.



## Methods of Benchmarking



1. Internal benchmarking – comparing the organization’s own performance from one-time period to another or between departments, locations, divisions, etc.
2. External benchmarking – comparing an organization’s performance against “best in industry” (competitors) or “best in class” (those recognized for certain functions) to determine if improvements are needed

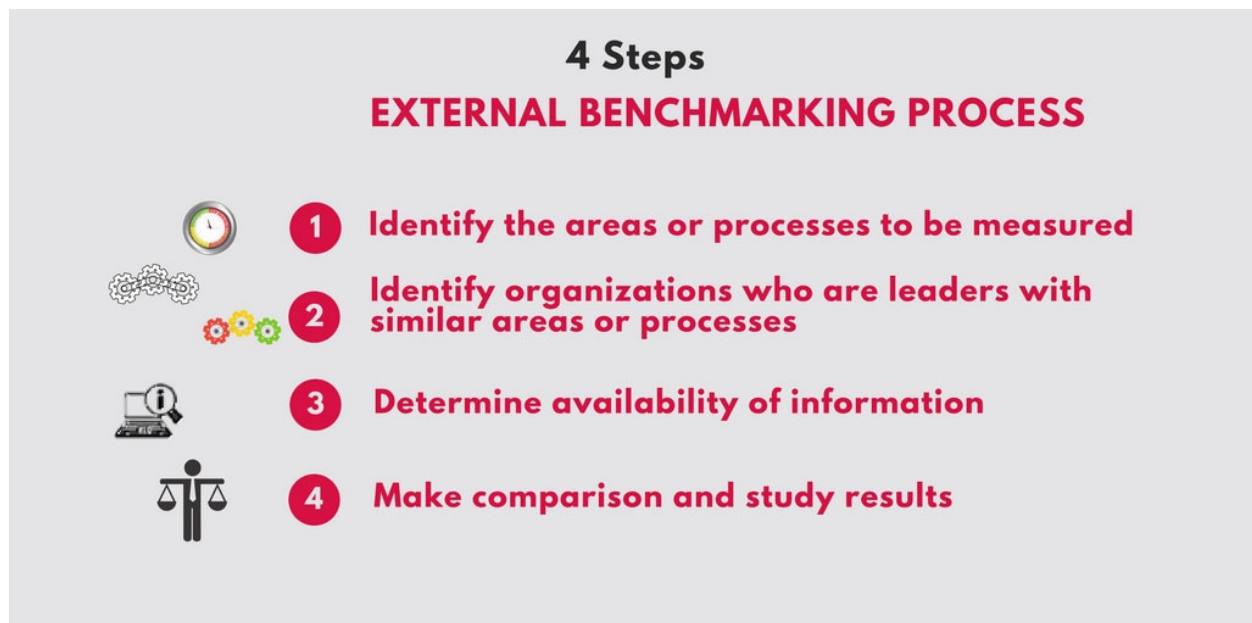
## Appropriate Times for Benchmarking

1. A baseline is needed
2. Improvement in existing activities is desired
3. Internal trending and comparisons are needed

## Steps in the External Benchmarking Process



1. Identify the area or process to be measured
2. Identify organizations who are leaders with similar areas or processes
3. Determine availability of the information
  - a. Regulatory agencies, e.g., OSHA, DOL, MSHA (Mine Safety and Health Administration)
  - b. Industry organizations
  - c. Trade groups
  - d. Online resources, e.g., annual reports and data aggregation services
  - e. Carriers
4. Make the comparison and study the results





## Advantages of Benchmarking



1. Encourages continuous improvement
2. Helps prioritize areas in need of improvement
3. Enhances creativity and “out of the box” thinking

## Disadvantages of Benchmarking

1. Results
  - a. The data must be interpreted and cannot be taken at face value
  - b. Bias by the party conducting the benchmark may affect the outcome
  - c. Findings may not accurately reflect the root cause of an issue
2. Data can be easily misinterpreted or manipulated
3. Data comparison issues
  - a. Insufficient volume of data
  - b. Unverified data
  - c. Inconsistent comparison data
  - d. Inadequate comparison groups

## **Applications of Benchmarking in Risk Management**

1. To make risk management decisions
2. To study “best practice” organizations to identify leading edge practices
3. To implement new and improved processes reflecting those best practices

## Review of Learning Objectives

1. Using an understanding of the acts and rules that apply to data security and the four parts of Data Risk Assessment, participants will provide a foundational argument for using data in the risk management process.
2. Using knowledge of the functions and purchasing considerations of a Risk Management Information System (RMIS), participants will be able to evaluate the characteristics of a RMIS to assess whether it would meet the organization's needs.
3. Using knowledge of the methods of, appropriate times for, and advantages and disadvantages of benchmarking, participants will be able to navigate through the steps of the benchmarking process.





# Certified Risk Managers

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

## Section 4

# **Total Cost of Risk**



### Key Terms



# Total Cost of Risk

## Section Goal

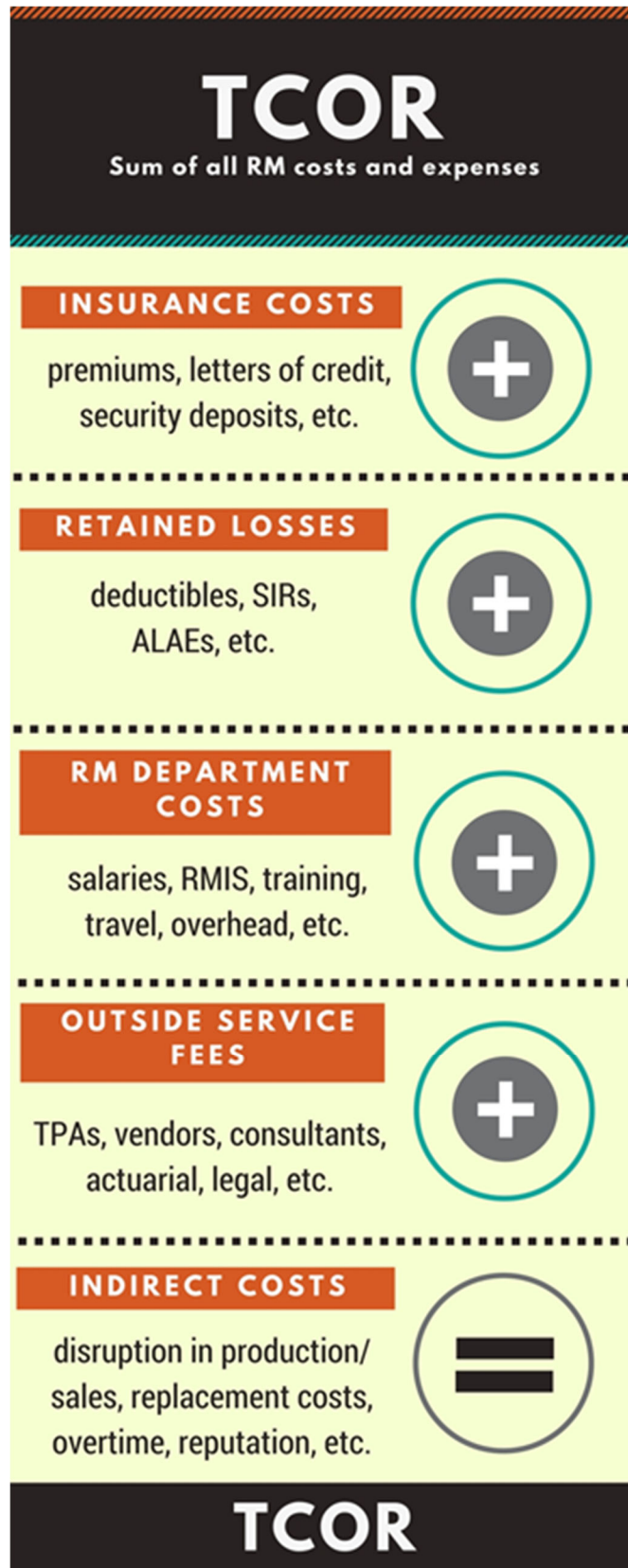
To provide participants with the core knowledge and tools necessary to properly analyze and allocate the Total Cost of Risk (TCOR), creating greater risk management awareness and accountability across an organization

## Learning Objectives

1. By understanding the **benefits and possible negative implications related to TCOR allocation**, participants will be able to engage others within their organization in the risk management process.
2. Using the **steps of the TCOR process**, participants will develop a TCOR allocation model.
3. By understanding the **different allocation models**, participants will be able to create a TCOR model appropriate for their organization.







## Foundation Information

**Definition:** Total Cost of Risk (TCOR) is the sum of all quantified costs and expenses associated with the risk management function of an organization

**Purpose:** TCOR is a risk management tool that is used to

1. Make effective risk management decisions by measuring progress
2. Establish accountability in the workplace
3. Effectively manage financial budgets and product pricing
4. Promote and focus on safety and loss control by demonstrating the financial impact of the TCOR

### Allocation Systems

Allocation systems are used to assign risk-related costs and expenses to different areas of an organization. Allocating costs can lead to greater risk management awareness and accountability across the organization. The ultimate goal is to reduce the expenses that contribute to the TCOR.

### Allocating TCOR

**Definition:** A process that identifies and assigns the TCOR among the various operating or accounting units within an organization

**Rationale:** To remain competitive, an organization must be able to track and properly account for all types of organizational costs, including the TCOR

#### Must-Haves for Success:

1. Senior management's input, approval and support
2. Consistent and equitable allocation of costs across the organization
3. A process for communicating the information in a way that is understood by all departments



### **Learning Objective 1:**

By understanding the **benefits and possible negative implications related to TCOR allocation**, participants will be able to engage others within their organization in the risk management process.

---

### **Benefits of Allocating TCOR Include:**



1. Identifying factors contributing to the TCOR – where do the costs originate?
2. Creating accountability
  - a. Each department, cost center, division, store, etc., is responsible for its cost of risk
  - b. Bonuses, salary increases, and performance evaluations can be tied to the results of the allocation
  - c. Employees become aware of the costs associated with losses, exposures and other components of the TCOR
  - d. Identifies areas that need risk management attention (locations, departments, managers, employees, etc.)
3. Enhancing loss control
  - a. Motivates employees to focus on reducing frequency and severity of losses, thereby reducing the TCOR
  - b. Builds risk control into projects, products and business decisions
  - c. Provides managers with specific loss and exposure information
  - d. Demonstrates the cost-effectiveness of investments in safety, loss prevention, and risk control equipment
4. Supporting the competitive advantage
  - a. Tracks and accounts for all types of costs
  - b. Holds fluctuating costs to a minimum
  - c. Limits manipulation of data and results
5. Altering behaviors

# Benefits of Allocating TCOR



## Possible Negative Implications Due to TCOR Allocation



1. Middle management pushback
2. Circumventing accident reporting procedures
3. Late reporting/non-reporting
4. Poor morale
5. Distorted goals & objectives
6. Disparate financial consequences
7. Can damage team approach to risk management

## Methods for Creating Active Participation in Others

1. Inform all employees about the allocating methodology and rationale
2. Provide frequent TCOR updates (monthly or quarterly) to keep employees engaged in the risk management process
3. Provide opportunity for input
4. Actively involve members from all levels of the organization to identify opportunities to lower TCOR



### Learning Objective 2:

Using the **steps of the TCOR process**, participants will develop a TCOR allocation model.

### Steps in the TCOR Allocation Process

Step 1 – Define Desired Result  
Step 2 – Define the Costs  
Step 3 – Select the Allocation Variables  
Step 4 – Create the Allocation Model



#### Step 1 – Define Desired Result

1. Goals and objectives
  - a. What is to be accomplished by allocating costs?
  - b. How will progress be measured?

#### Example:

If a goal of allocation is to alter behavior, how will the risk manager measure changes?  
Are there fewer accidents?

2. Impact
  - a. Company culture and politics
  - b. Motivation and incentive opportunities
  - c. Loss control programs
  - d. International operations

3. Compatibility
  - a. Accounting system – new codes may be needed, budgets revised, etc.
  - b. Claims management system
  - c. Human resources database, payroll system, etc.
  - d. RMIS
  - e. Any other proprietary systems
  
4. Consistency and equality
  - How to maintain consistency and equality across the organization
  
5. Communication
  - Which communication channels will be utilized to communicate the allocation system to all personnel?
  
6. Additional considerations
  - a. Tax implications – income tax, foreign taxes, franchise taxes, etc.
  - b. International operations
    - 1) Law, tribunals
    - 2) Currencies, exchange rates
    - 3) Insurance product availability



## Step 2 – Define the Costs

1. Insurance costs – premiums, premium taxes, letters of credit, deposits, collateral, etc.
2. Retained losses
  - a. Deductibles or SIRs
  - b. Self-funding costs, e.g., accruals, bonds, surety costs
  - c. Funded reserves for catastrophes or unexpected events
  - d. Costs associated with handling retained losses or claims, e.g., legal expenses, medical case management fees, TPA fees
3. Risk management departmental costs
  - a. Payroll and related costs
  - b. RMIS costs
  - c. Administration, e.g., travel, education, training, conferences
4. Outside service expenses
  - a. Fee-for-service agents/brokers
  - b. Actuaries
  - c. Legal fees
  - d. TPAs not included in retained losses
  - e. Other outside services such as loss control, environmental services, etc.

5. Quantified portion of indirect expenses
  - a. Training for new employees
  - b. Loss of productivity
    - 1) New hires
    - 2) Downtime because of accident
  - c. Overtime costs
  - d. Lost opportunity costs
  - e. Social costs (reputation, public image), e.g., public relations consultant fees
  - f. Management costs (time spent on loss-related activities)

**Note:**

When an organization decides against allocating a specific cost to the TCOR, those costs could be charged to the organization as part of overhead operating expenses. Certain components of the TCOR may be assigned to home office only, such as insurance premiums and retained losses for executive risk exposures, e.g., D&O, fiduciary liability.

6. Sources of cost data and information
  - a. Insurance company/carrier
  - b. Risk management department
  - c. Accounting department
  - d. Legal department
  - e. Human resources department
  - f. Safety and quality control
  - g. Management

7. Decide when to allocate costs
  - a. Before they are incurred (based on your loss pick)
  - b. As they are actually incurred
  - c. At the end of the year/established period
  - d. Allocated in advance and adjusted at end of year

### **Step 3 – Select the Allocation Variables**

1. Structure and ownership
  - a. Privately owned
  - b. Publicly traded
  - c. Governmental – including government-regulated tax structure organizations, e.g., cities, school districts, hospital districts, airports, joint powers or authorities
2. Geographic
  - a. Number of locations
  - b. Permanent or variable locations, operations, activities, management
  - c. Domestic or international locations, operations, activities
  - d. State differentials (benefit levels, statutes, etc.)
3. Economic factors such as business cycles, strikes and natural disasters
4. Political climate
5. Tax structure

## Step 4 – Create the Allocation Model

1. Common approaches to allocating the cost of risk are:
  - a. Exposure method – costs are allocated based on exposure units
  - b. Experience method – costs are allocated on an experience basis
  - c. Combination method – a mix of allocating portions of costs to operating units based on exposures and experience that can take many forms
2. Determine what level of costs will be allocated
  - a. Minimum costs
  - b. Maximum costs or caps
  - c. Aggregate limits
3. Determine if the allocation will be prospective or retrospective
  - a. Prospective allocations are “one and done” – allocated at the beginning of the time period and generally not adjusted at the end; a solid loss pick is required to be able to do this
  - b. Retrospective allocations begin with a “deposit” allocation at the beginning of the time period and adjusted at the end of the time period, usually upon experience
4. Test the allocation model
5. Because of organizational diversity, there is no one “best model”

Once the allocation process has been implemented, the risk manager will need to analyze and track the success of the system. Are the costs being allocated appropriately and fairly? Are the selected variables the right ones? Are all costs being accounted for properly? Are behaviors changing due to the allocation system? Are new control measures being put into place? Are costs coming down? Are incident rates dropping?

# STEPS IN THE TCOR ALLOCATION PROCESS

## STEP 1 - DEFINE THE DESIRED RESULT

- Goals and objectives
- Allocation methodology affects other parts of the organization
- Compatibility between systems
- Consistency and equity across organization
- Communication to personnel
- Additional considerations such as taxes and international operations
- Insurance product availability



## STEP 2 - DEFINE THE COSTS TO BE ALLOCATED



- Insurance costs
- Retained losses
- Risk management departmental costs
- Outside services
- Quantified indirect costs

## STEP 3 - SELECT THE ALLOCATION VARIABLES

- Structure and ownership
- Geographic
- Economic factors
- Political climate
- Tax structure



## STEP 4 - CREATE THE ALLOCATION MODEL



- Consider common allocation methods
- Determine what level of costs will be allocated
- Decide on retrospective or prospective allocation
- Test the allocation model



### **Learning Objective 3:**

By understanding the **different allocation models**, participants will be able to create a TCOR model appropriate for their organization.

### Exposure-Based Method



**Definition:** Each unit is assigned costs on an equitable basis, based on the exposures each unit presents

#### **Examples of exposure units:**

1. Number of employees or number of Full-Time Equivalent (FTE) employees
2. Payroll
3. Sales, receipts, revenue
4. Units produced
5. Square footage
6. Value of assets
7. Miles driven

#### **Two variables involved in this method:**

1. Change in exposure values, e.g., appreciation of an asset, such as a building
2. Change in number of exposure units, e.g., increase or decrease in number of vehicles or employees

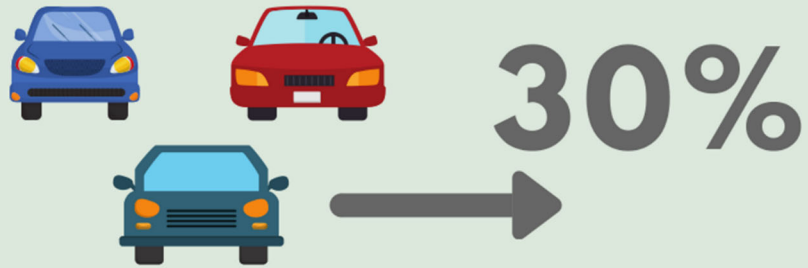
#### **Characteristics:**

1. Easy to administer and adjust if exposures change
2. Simple to understand
3. Supports period-to-period consistency
4. Not linked to loss experience
5. No incentive to reduce losses because of allocation

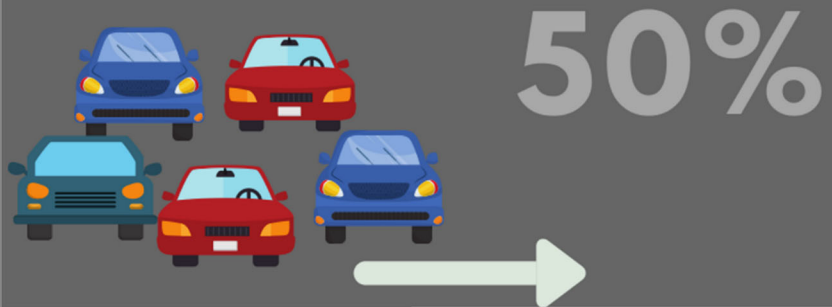
# EXPOSURE - BASED METHOD

Costs are allocated based on exposure units.

## LOCATION 1



## LOCATION 2



## LOCATION 3



Each unit is assigned costs on an equitable basis, based on the exposures each unit presents. In this example, the exposure units are vehicles.

## Experience-Based Method



**Definition:** Each unit is assigned costs on an equitable basis, based on the loss experience each unit presents.

Each unit's own loss experience is the only variable involved in this method.

### **Experience-based allocations:**

1. Number of losses
2. Cost of losses

### **Characteristics:**

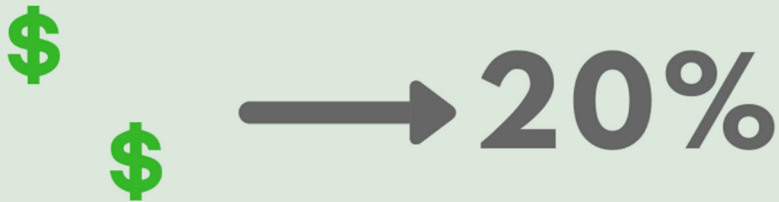
1. Encourages loss control
2. Supports accountability
3. Doesn't allow for strategic or discretionary allocation
4. May be more difficult to administer due to the volume of data



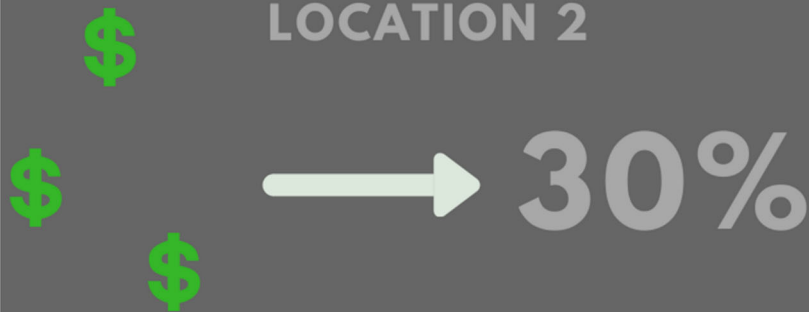
# EXPERIENCE - BASED METHOD

Costs are allocated based on loss experience.

## LOCATION 1



## LOCATION 2



## LOCATION 3



Each unit is assigned costs on an equitable basis, based on the loss experience each unit presents.

The number of vehicles at each location is irrelevant in this calculation.

## Combination Method



**Definition:** Each unit is assigned costs in a model that balances a mix of exposure-based and experience-based allocations based on relative percentages of exposures or experience

**Percentage of total method:** TCOR is allocated according to the percentage that the amount of exposures or experience of each allocation division bears to the total of the exposures or experience

**Per unit method:** TCOR is allocated based upon a per unit TCOR (the TCOR for each unit of exposure or each unit of experience) times the number of exposure or experience units for each allocation division

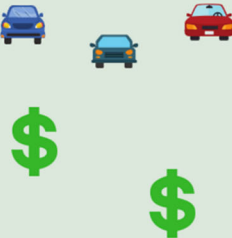
### Examples:

1. Insurance costs (all or a portion) are allocated on an exposure base that varies with the type of insurance
2. Risk management department costs are fully allocated using an appropriate exposure base, e.g., number of employees
3. Outside service costs are allocated to those allocation divisions that use them
4. Portions of insurance premiums not allocated on an exposure base are allocated according to historic losses for that type of exposure
5. Retained losses are generally charged to the allocation division that had the loss, but may be limited to mitigate the impact of catastrophic losses; the portion not allocated may be assigned to the general overhead

# COMBINATION METHOD

Each unit is assigned costs in a model that balances a mix of exposure-based and experience-based allocations based on relative percentages of exposures or experience.

**LOCATION 1**

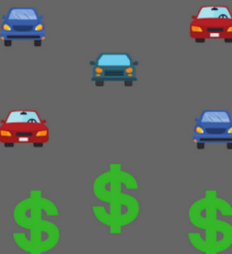


3 CARS/ 10 TOTAL CARS X .5 = 15%

20% OF LOSSES X .5 = 10%

15% + 10% = 25%

**LOCATION 2**

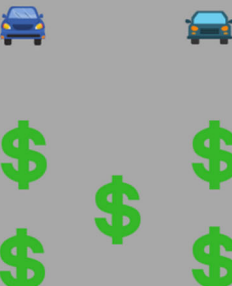


5 CARS/ 10 TOTAL CARS X .5 = 25%

30% OF LOSSES X .5 = 15%

25% + 15% = 40%

**LOCATION 3**



2 CARS/ 10 TOTAL CARS X .5 = 10%

50% OF LOSSES X .5 = 25%

10% + 25% = 35%

In this example, half of the costs are allocated based on the number of vehicles (exposure-based), and half of the costs are allocated based on the cost of losses (experience-based).



## PRACTICE EXERCISE

You are the risk manager for a growing chain of restaurants. Currently the organization consists of a home office and three restaurants. There are plans to add at least one location per quarter for the next five years. As the organization plans for future expansion, it has become clear that there needs to be a more organized approach to risk management. As the newly hired risk manager, you have been studying the loss data and the cost of risk; however, you have found that those outside the home office have very little knowledge about what costs are associated with the Total Cost of Risk.

Before you can even begin the allocation process, you must first educate those in the home office about the components of TCOR.

Component					
Examples of included costs					

Now that everyone has a better understanding of what is included in the TCOR, you are ready to begin the TCOR allocation process.

## Step 1 – Define Desired Result

What is to be accomplished by allocating costs?

How will progress be measured?

What are the potential benefits of TCOR allocation for your organization?

What additional questions do you need to have answered to design an appropriate model?

4

## Step 2 – Define the Costs

Insurance Costs	_____
Retained Losses	_____
RM Departmental Costs	_____
Outside Service Fees	_____
Indirect Costs	_____

Consider which of these costs should be allocated across the organization and when the costs should be allocated.

### Remember:

When an organization decides against allocating specific costs to the TCOR, those costs could be charged to the organization as part of overhead operating expenses. Certain components of the TCOR may be assigned to home office only, such as insurance premiums and retained losses for executive risk exposures, e.g., D&O, fiduciary liability.

What additional information would you need to design an appropriate cost allocation model?
1.
2.
3.
4.
5.

**Step 3 – Select the Allocation Variables**

What if you had the following additional information?  
What information would influence your decision in choosing an allocation model?  
What data might unfairly skew the results?

By Location	Home Office	Store 1	Store 2	Store 3
# of Employees				
Payroll				
Square Footage				
Sales				
Retained losses				
Outside Services				

**Step 4 – Create the Allocation Model**

Based on the information provided, which method seems most appropriate?

## Review of Learning Objectives

1. By understanding the benefits of the TCOR model, participants will be able to engage others within their organization in the risk management process.
2. Using the steps of the TCOR process, participants will develop a TCOR allocation model.
3. By understanding the different allocation models, participants will be able to create a TCOR model appropriate for their organization.







# Certified Risk Managers

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

## Section 5

# Due Diligence



### Key Terms



### Business “Scientific” Method



## Due Diligence

### Section Goal

To provide participants with practical knowledge needed to properly analyze a potential business decision, merger or acquisition by performing SWOT analyses and working through the due diligence process.

5

### Learning Objectives

1. By applying the **definition** and understanding the **purpose** of due diligence, participants will be able to recommend **when due diligence is necessary**.
2. Based on the understanding of the **SWOT analysis**, participants will be able to define the **components of SWOT** and to explain what each indicates to an organization.
3. By understanding the **reasons an organization must change** in order to grow and expand, participants will be able to assess the options of partnering with another organization through a **buy-sell agreement** such as a **merger or acquisition** to facilitate the needed change.
4. By working through the **four steps of the due diligence process**, participants will be able to make recommendations to management on important business decisions.

## Introduction

To remain competitive, an organization must continue to change and evolve. Due diligence is essential because there is inherent risk involved with any business decision or organizational change.



### Learning Objective 1:

By applying the **definition** and understanding the **purpose** of due diligence, participants will be able to recommend **when due diligence is necessary**.

**Definition** – Due diligence is a detailed and thorough examination and analysis conducted by an organization prior to making a business decision and commonly applies to voluntary investigations. However, in certain circumstances, the term relates to a legal obligation.



### Purpose:

1. To bring together legal and other professionals with specialized expertise whose collective responsibility is to:
  - a. Perform an investigation of a business, situation, activity or person to assist with effective decision-making
  - b. Assess the health and viability of a business or entity

**When to Use** – Examples of when due diligence would be critical:

1. Merger and/or acquisition
2. Purchase of new assets, particularly real property
3. Development or modification of a product, service or process
4. Undertaking of a joint venture or contract
5. Establishing or altering relationships, e.g., hiring and firing personnel, choosing a new supplier or service provider

**How does an organization decide what changes to make?**

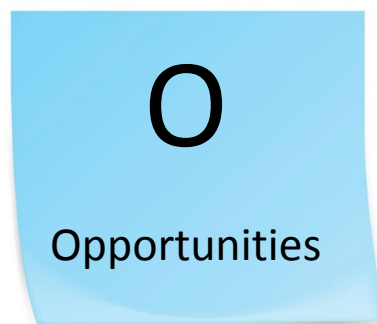
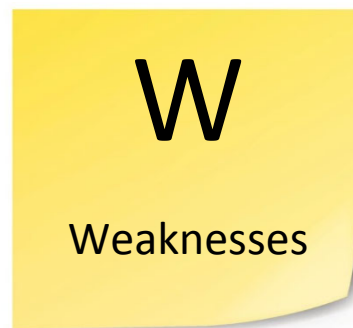
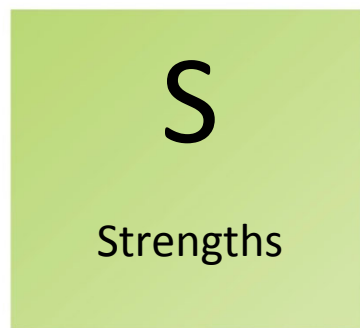
One of the ways an organization might assess its current status and future needs is through performing a SWOT Analysis (Strengths, Weaknesses, Opportunities, and Threats). A SWOT analysis can pinpoint areas that need change, so that an organization can set priorities and determine action items. These action items will often require due diligence.



### Learning Objective 2:

Based on the understanding of the **SWOT analysis**, participants will be able to define the **components of SWOT** and to explain what each indicates to an organization.

**SWOT Defined** – A SWOT analysis is a common method of analyzing where the organization has its strengths and weaknesses as well as analyzing what threats and opportunities exist to determine internal and external opportunities available to an organization





## PRACTICE EXERCISE

Once an organization has performed a SWOT analysis, it needs to utilize the results to determine how to build upon its strengths, correct its weaknesses, capitalize on its opportunities, and to minimize its threats. Using the examples below, create additional potential action items that the organization should explore for each.

	<b>Strengths</b>	<b>Weaknesses</b>	<b>Opportunities</b>	<b>Threats</b>
<b>Examples:</b>	Internal resources Intellectual property Well-performing products Competitive advantage Expertise Reputation	Talent gap Loss of market share Underperforming products Speed to market Low brand recognition Costs	Emerging markets New product lines Public relations Increase efficiencies Reduce costs Increase customer base New locations New territory	Limited supply chain Emerging risks and changing regulations Competition Changing customer demands or attitudes Increased supply cost Production disruption
<b>Potential Actions:</b>	Create complimentary products	Outsource specific projects or tasks if personnel is lacking	Promote service projects to create social media presence	Reciprocal agreements

Once an organization has determined its needs, what are some of the motivations that prompt action?

**Motivations:**

To eliminate competition	To adopt new technologies
To fill in talent gaps	To expand market share
To gain cost efficiency	To become more competitive
To strengthen customer relationships	

Some of these motivations will prompt small changes, like a new hire or a new software program. Others need larger solutions and might prompt larger scale organizational change, such as a merger or acquisition.

## Mergers & Acquisitions

When an organization has identified a need to change, it may look to outside/existing companies to fill that need. Instead of simply purchasing new technologies, hiring new staff or expanding product lines, an organization may consider a merger with or acquisition of another entity.



### Learning Objective 3:

By understanding the **reasons an organization must change** in order to grow and expand, participants will be able to assess the options of partnering with another organization through a **buy-sell agreement**, such as a **merger or acquisition**, to facilitate the needed change.

What might you look for in another organization?



<b>Market Share</b> Product lines Geographic reach Customer base Public image/company credibility	<b>Infrastructure</b> Locations Supply chains Distribution channels Systems/network
<b>Processes</b> Technology Quality control Manufacturing Sales & marketing	<b>Expertise</b> Experience Research & development Customer service Knowledge



**What types of buy-sell agreements might be considered?**



**Merger** – two or more organizations agree to move forward as one new entity and issue the appropriate ownership interests (common stock, memberships, partnerships, etc.)

**Acquisition** – one organization takes over all or part of another organization and is established as the new owner with ownership interests continuing unchanged

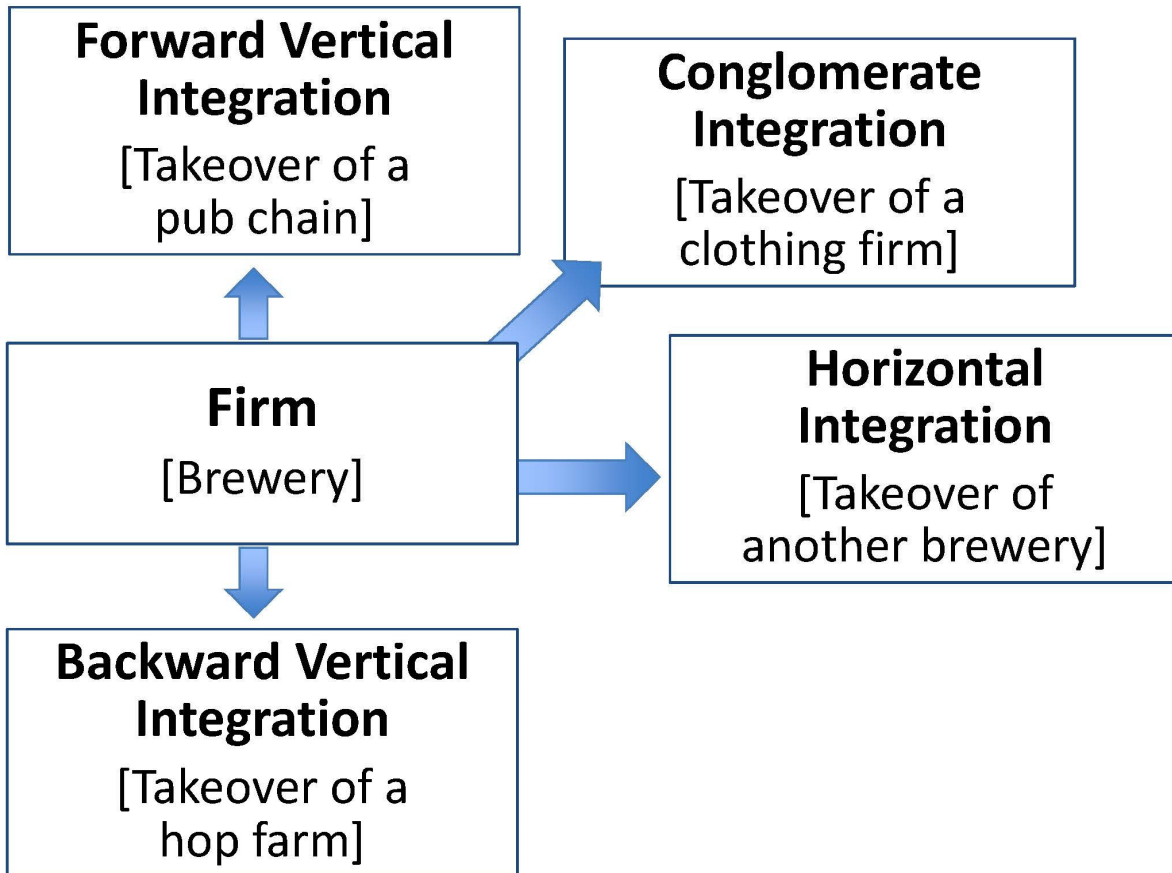
**Divestiture** – when an organization decides to sell off investments or business interests in a subsidiary

**What structure might they take?**

## TYPES OF MERGERS AND ACQUISITIONS

Type of Merger	Definition	Objective
Horizontal 	Combine firms in same industry	<ul style="list-style-type: none"> <li>• Increase size</li> <li>• Increase market power</li> <li>• Gain efficiency</li> </ul>
Vertical 	Combine companies with buyer-seller relationship	<ul style="list-style-type: none"> <li>• Provide tighter integration and increase control</li> </ul>
Conglomerate 	Combination of unrelated companies	<ul style="list-style-type: none"> <li>• Increase company's diversity</li> </ul>

# Types of Mergers





## PRACTICE EXERCISE

Examples & Exercise:

Disney & Pixar	Chase & Bank One	Cigna & Express Scripts	T-Mobile & Sprint
Merger 2006	Acquired 2004	Proposed	Proposed
Disney needed the modern technology that Pixar had, and Pixar needed the market reach and brand recognition that Disney already had	Chase wanted to expand further across the U.S. and Bank One was well-established in regions where Chase was not	Why?	Why?

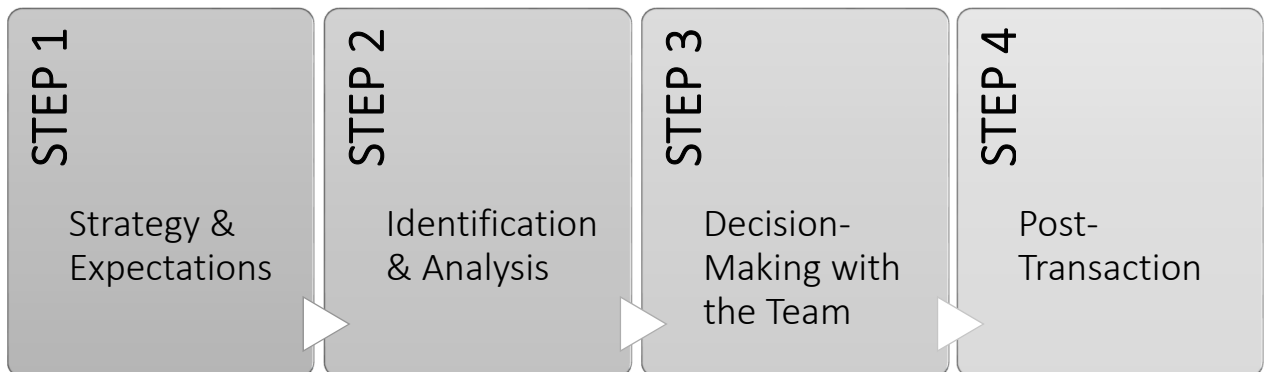
## The Due Diligence Process

While an organization will certainly perform due diligence during mergers and acquisitions, it is also an important process to follow for most business decisions and organizational changes.



### Learning Objective 4:

By working through the **four steps of the due diligence process**, participants will be able to make recommendations to management on important business decisions.



## Step 1: Strategy & Expectations



5

- What are your needs and how do you plan to address them?
- What is the task or target? What are we changing?
- Requirements: What is the desired result? Is there a hurdle rate? Are there make-or-break scenarios?
- Set a timeline
- Define roles and responsibilities – to avoid overlap or duplication of efforts and eliminate power struggles

## The Due Diligence Team

**When forming a due diligence team, members need to be selected strategically to ensure that the team:**

- Represents each functional business area of the organization
- Has knowledge of cross-departmental risks and understands how changing one variable can affect another
- Has a vested interest in and knowledge of the organization as a whole

**The team will include:**

- The risk manager
- Senior leaders or representatives from each key functional business area
- Legal representation

**Key responsibilities**

- Explain the purpose, nature and structure of the deal
- Explain the expected scope of the due diligence team's efforts
- Explain any issues related to the process

## Step 2: Identification & Analysis



Ensure all information is complete and accurate:

- Background information – conduct interviews, check references
- Company information – discontinued products, services or operations; successor liabilities from previous acquisitions or consolidations
- Financial information – review financial documents, cash flow funding mechanisms
- Key exposure areas (depending on type of business), e.g., products/general liability; environmental; workers compensation; contractual and professional liability; business interruption and extra expense; regulatory agency citations; fines; and improvements required by OSHA, EPA, EEOC, ADA, etc.
- Risk management program:

Program activities and functions

Risk financing arrangements – retrospectively rated plans, pools, captives, retentions and TCOR

Loss history and insurance information including policies, claims-made policies, tail coverage, premiums, claims records, workers compensation experience modifier and litigation records

# Look for and Analyze

**Loss  
history**

**Open  
claims**

**Retained  
losses**

**Actuarial  
review**

**Evaluation  
of IBNR**

**Loss  
development &  
trending**

**Loss  
portfolio  
transfers &  
financial  
reinsurance**

**Adverse  
development**



## **\* Insurance coverage review \***

### **SCOPE OF COVERAGE**

- Schedule of insurance
- Occurrence vs. claims-made policies
- Exclusions/gaps in coverage
- Concurrency between primary and excess coverage
- Ownership of policies

### **INSURER CONTRACTS & AGREEMENTS**

- Collateral trusts, letters of credit, escrow accounts
- Retrospectively-rated plan agreements
- Self-insured retention financial requirements
- Deductibles/retentions, per occurrence & aggregate
- Information on pool participation & captive insurance companies

### Step 3: Decision-Making with the Team



1. Report back findings from Step 2 – summary of the exposures uncovered, appraisals and estimates, expert and professional reports
2. Perceived value from the transaction
3. Liability that will be assumed through the transaction
4. Identify any critical transition issues
5. Integration issues, facility closures, new construction, retrofitting, etc.
6. Determine impact on other functions within the organization
7. Identify the worst-case scenario in any given situation with an estimate of what is most likely to happen
8. Review key assumptions and make recommendations to management
9. Tax implications and structure of the sale (entity, asset, liability)

## Step 4: Post-Transaction



1. Identify and address new exposures
2. On-site inspection of locations, particularly if subject to closing
3. Organizational structure, culture, leadership, policies and procedures
4. Consolidate or separate programs
  - a. Human resources
  - b. Risk management departments (consolidation or separation)
  - c. Safety
  - d. Other departments (legal, accounting, etc.)
  - e. Insurance
    - Outstanding claims and aggregate loss levels
    - Experience rating changes
    - Tail coverage exposures
    - Workers compensation administration
  - f. Claims management

Business “Scientific” Method



## Review of Learning Objectives

1. By applying the definition and understanding the purpose of due diligence, participants will be able to recommend when due diligence is necessary.
2. Based on the understanding of the SWOT analysis, participants will be able to define the components of SWOT and to explain what each indicates to an organization.
3. By understanding the reasons an organization must change in order to grow and expand, participants will be able to assess the options of partnering with another organization through a buy-sell agreement, such as a merger or acquisition, to facilitate the needed change.
4. By working through the four steps of the due diligence process, participants will be able to make recommendations to management on important business decisions.



## Certified Risk Managers

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

### Section 6

# Managing the Risk of Intangible Assets



### Key Terms



# Managing the Risk of Intangible Assets

## Section Goal

To provide participants with the core knowledge and tools necessary to formulate communications and utilize risk control mechanisms to protect the organization's integrity through reputation and brand management

## Learning Objectives

1. Using an understanding of the **common types of intellectual property** and **control options for intellectual property**, participants will create a plan for protecting the various types of intellectual property in his/her institution.
2. Using knowledge of **reputation, logo and brand, factors that influence them, and control mechanisms** used to manage them, as well as understanding **communication**, participants will design a communication plan for protecting an organization's reputation and brand.



### **Learning Objective 1:**

Using understanding of the **common types of intellectual property** and **control options for intellectual property**, participants will create a plan for protecting the various types of intellectual property in his/her institution.

Intangible assets are not physical in nature and include intellectual property (patent, copyright, trademark, designs, and trade secrets), as well as customer goodwill, reputation and brand. These assets represent legal rights and competitive advantages to an organization. Their continued growth in volume and value in the market place elevates their importance to risk management. Managing these exposures requires collaboration between all areas of management; specifically, legal, risk management, quality assurance, marketing and public relations. Many of these departments are highly cognizant of protecting intangible assets and have their own protocols for addressing these risks. These should be aligned with the organization's overall objectives and goals for protecting and managing the risk associated with them.

**Definition:** Intellectual Property (IP) has a value and lacks a physical existence, examples are industrial property such as inventions, patents, designs, trademarks, and copyrights for literary and artistic works.





## Common Types of Intellectual Property



1. **Patent** – used for an invention; the grant of a property right to the inventor, issued by the U.S. Patent and Trademark Office
2. **Copyright** – a form of protection provided to the authors of “original works of authorship” including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished (e.g., music)
3. **Trademark** – unregistered mark (a symbol, word, or words) used to represent a company or product; trademark is used to represent goods (e.g., Slap Chop)
4. **Service mark** – a legally registered name or designation used in the manner of a trademark to distinguish an organization's services from those of its competitors (e.g., NBC for both the peacock logo and the tri-tone sound)
5. **Registered mark** – The **registered trademark** symbol (®) is a symbol that provides notice that the preceding word or symbol is a **trademark** or service mark that has been **registered** with a national **trademark** office (e.g., Coca Cola)

Often, the registered mark will be used in combination with a TM or SM symbol, (e.g., Microsoft Windows)

The **TM** and **SM** symbols are used with unregistered marks: **TM** for trademarks, or marks that represent goods, and **SM** for service marks, or marks that represent services. The federal registration symbol, or ®, is reserved for marks registered in the U.S. Patent and Trademark Office

6. Trade secret – any confidential business information which provides a competitive edge. Trade secrets include manufacturing or industrial secrets and commercial secrets (e.g., KFC's original recipe)
  
7. License – process of leasing a legally protected (trademarked or copyrighted) entity – a name, likeness, logo, trademark, graphic design, slogan, signature, character, etc. The entity, known as the property or intellectual property, is then used in conjunction with a product (e.g., Nike licensed to use sports logos on their product)
  
8. Franchise – the right or license granted to an individual or group to have access to a business' proprietary knowledge, processes and trademarks in order to market a company's good or services in a particular area; (e.g., McDonald's; selling your product in my store)
  
9. Concession – a right or privilege to operate commercially within the limits of a larger concern (e.g., Clinique, department store; selling my product in your store)

# INTELLECTUAL PROPERTY



Patent



Copyright

# TM

Trademark

# SM

Service Mark



Registered Mark



Trade Secret



License



Franchise



Concession

The risk manager should work closely with the organization's legal department, product development function, research and development function, and marketing department to coordinate risk management activities and to arrange financing of intellectual property risks.

### Risk Control



1. Protecting the organization's assets (our stuff)
  - a. Identify infringements
    - Conduct surveys (can be outsourced) to determine if other organizations are using your intellectual property
    - Rely on observant employees or concerned third parties voluntarily reporting infringements
  - b. Obtain necessary protections
    - Normally within the purview of the legal department
    - Protections such as trademarks, copyrights, patents

2. Not violating anyone else's assets (their stuff)
  - a. Usually the responsibility of research and development, product development, marketing or advertising departments
  - b. Must ascertain that products and services are not previously protected by other parties
  - c. Involves careful research, including trademark and patent searches, as well as proofreading (for use of brand names, etc.) to make sure there are no infringements upon the IP of others
    - Legal department is normally the first to respond to allegations that the organization has infringed upon the IP of others and will initiate actions to mitigate potential losses

As it can be difficult to assign costs and values to intangible assets, it is often necessary to use qualitative and quantitative analysis.

## **Risk Financing**

1. Cyber insurance policies for both first party and third party intellectual property may be available for purchase
2. Generally, insurance mechanisms for intellectual property can be manuscript policies or an endorsement to an existing policy, which are flexible, but must be individually read and reviewed as they vary greatly
3. Alternative financing methods such as a captive, funded or unfunded segregated accounts



### **Learning Objective 2:**

Using knowledge of **reputation, logo and brand, factors that influence them, and control mechanisms** used to manage them, as well as understanding **communication**, participants will design a communication plan for protecting an organization's reputation and brand.

---

### **Difference between Logo, Brand and Reputation**

**Logo** – a symbol or design that identifies a brand. Many organizations think their logo is their brand; however, the values and associations that customers and others have when thinking about the company are the most important elements of the brand.

**Brand** – a set of perceptions or expectations that represent a company, product or service and differentiate it from its competitors (e.g., Samsung Galaxy, NFL, Rolex, American Airlines).

Consumers live and breathe brand information daily. One negative can often overpower a hundred positives and business and opportunities can be immediately lost and difficult to recover.

**Reputation** – collective assessments of a corporation's past actions and the ability of the company to deliver improving business results over time. Think of consumer perception of trust, corporate responsibility and citizenship (e.g., TOMS shoes).

Reputation and brand are connected. An organization cannot have the reputation it desires if promises are made that cannot be kept.

Reputation is far more than corporate social responsibility or doing good things. It means that expectations must be shaped appropriately through the organization's branding activities. Once this is done, the organization can meet or exceed those expectations through communications and actions (e.g., Disney, Walmart, Volkswagen).



### Corporate behavior

1. Corporate behavior is a business's general philosophy and corporate responsibility, as determined in the board room and managers' offices; it permeates throughout the business to the point that it cannot be attributed to any one individual or group
2. Marketing and communications
  - a. Marketing should be cognizant of IP infringement issues
  - b. Marketing and communications must be real and truthful to avoid liability caused by misrepresentation and violation of warranties or other promises

### Individual behavior

1. Abuse of authority
2. Careless or negligent acts of employees
  - a. Can give rise to catastrophic equipment failure or allow faulty products and services to enter the market and/or stream of commerce
  - b. Disclosure of confidential information
  - c. Improper use of social media – individuals posting negative or rude comments or inappropriate photos
3. Criminal acts – the acts themselves may not damage reputation and brand unless the organization's response is ill-perceived or if the organization fails to mitigate further perpetration of criminal acts





## Importance of Protecting Reputation and Brand

1. Critical assets of an organization
2. Susceptible to any type of disaster but are most affected by human actions, accidental or deliberate
3. Can be damaged through no fault of the organization, its employees or its representatives
4. Losses can single-handedly cause the organization to fail



## PRACTICE EXERCISES

Consider the facts from the two following crises and how reputation and brand were affected:

1. Johnson & Johnson vs. Bon Vivant Soup

<b>Company:</b>	<b>Johnson &amp; Johnson</b>	<b>Bon Vivant Soup</b>
<b>Crisis:</b>	3 <sup>rd</sup> party product tampering	Botulism in product
<b>Impact:</b>	7 dead	1 dead, 1 sick
<b>Immediate action:</b>	Recalled 31 million products including products not affected by the tampering	Recalled 6,444 cans
<b>Communication:</b>	Restated the company credo Acknowledged the problem Reassured consumers	Remained silent
<b>Current status:</b>	Strong brand, trusted product	Out of business, including the successor company that used a new name

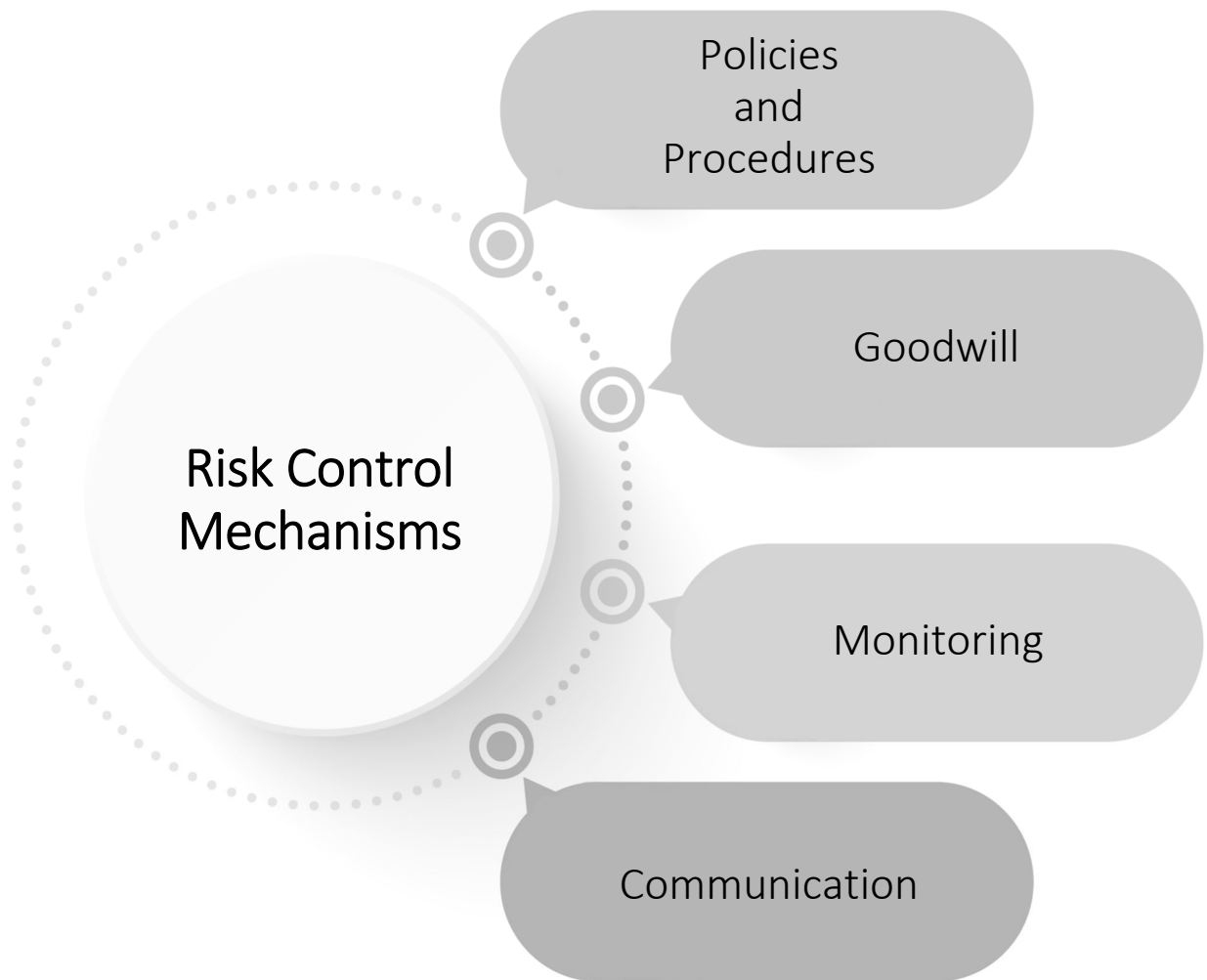
Why did one company survive and one fail?

## 2. Ayds vs. AIDS

In 1937, an appetite suppressant candy was sold under the brand Ayds. In the mid-1980s, public recognition of the seriousness of acquired immune deficiency syndrome, commonly referred to as AIDS, caused sales of the diet candy to drop 50% by 1988. The company changed the name to Diet Ayds (Aydslim in Britain), but the association with the illness had fatally damaged the product name. Through no fault of its own, the company was forced to withdraw the product from the market.

What are other situations that could cause damage to reputation and brand?

Are there other examples you know of?



## Policies and procedures

1. Establish and enforce codes of ethics and conduct
2. Implement a social media and blogging policy to include the following:
  - a. Clearly defined company philosophy
  - b. Definition of “social networking” and which specific sites the policy addresses
  - c. Identification of the person as an employee
  - d. Recommendations or referrals
  - e. References to any clients, customers or partners
  - f. Confidential or proprietary information
  - g. Terms of service
  - h. Copyright and other legal issues
  - i. Guidelines for time spent on social networking in the workplace
  - j. Consequences for violations

## **Goodwill**

1. Customer relations
2. Community outreach programs
3. Charitable donations
4. Environmentally friendly

## **Monitoring**

1. Website gatekeeper for comments made by outsiders
2. Maintenance of quality assurance programs
3. Training employees in procedures and policies

## **Communication** – (this area will be explored in the next section in greater detail)

- Rumor control
- Risk finance – adverse reputation coverage: protection against adverse reputation arising out of product failure, product recall, extortion, business operations contrary to organizational image, misrepresentation of products and employees' criminal acts or offenses against public taste or decency



The risk manager plays a very important role in the creation of message content. Bringing together members of the organization to create consistent communication helps to mitigate the financial impact of a crisis. The content of the message is scrutinized by the risk manager to make sure the organization isn't opening itself up to any liability, such as a privacy breach, an admission of liability or a misrepresentation.



### **Critical communication events**

1. New hire in a major position
2. New product line
3. Merger, acquisition or divestiture
4. Community initiative
5. Major organizational change
6. Crisis

### **Recipients**

Who receives the communication?

1. Employees (on-site and off-site)
2. Visitors, customers or service providers
3. Media outlets
4. Regulatory agencies
5. Law enforcement
6. Local government officials
7. Family members of affected persons
8. Neighbors or property owners
9. Partnering companies
10. Industry sector contacts (including competitors)



**Delivery channels** – What is the appropriate (and available) method to get the message out given a certain situation?

1. Text alerts
2. Email
3. Social media
4. Website
5. Press release
6. Press conference or other public appearance

**Content** – What key components should be communicated? (not an exhaustive list and applicability dependent on situation)

1. What happened?

Prompt, concise and accurate description with:

- a. Relevant information necessary for an accurate depiction of the event and current status; avoid jargon and technical terminology
- b. Extent of damages and injuries, if known
- c. Only provide verified, factual information; acknowledge uncertainty; avoid over-reassurance – be willing to state that not every possible contingency is known, and actions are being taken based on the most accurate information available; NEVER speculate or offer opinion, especially in the early stages
- d. Acknowledge tension and emotions as legitimate and avoid humor or an appearance of making light of the situation
- e. Acknowledge obvious mistakes in certain circumstances; an expression of regret and empathy should be considered and an apology may be appropriate in limited cases (check state laws on apologies and admissions of liability)

2. What information is critical to the recipient?
  - a. Available assistance
  - b. Evacuation and safety instructions
  - c. Expected duration of the crisis
  
3. What is being done to manage the event?
  - a. Immediate actions taken and by whom
  - b. Actions taken to mitigate further loss or damage
  - c. Description of preparations made in advance for the crisis and how they are being implemented
  - d. Ongoing current intelligence on the situation and rumor control, including when operations are expected to return to normal
  - e. Designation of official spokesperson and how future information will be distributed (type and frequency)
  - f. Project authority, confidence and a sense that a plan is in place

4. Addressing questions and control rumors
  - a. Never say, “No comment”
  - b. “I don’t know,” “We do not have all the details at this time,” and “We will continue to work with the proper authorities throughout the process” are acceptable answers to many questions
  - c. Deflection should be used judiciously, as it generally provides an answer that satisfies most members of the media; it should not be used when questions persist
  - d. Prepare the spokesperson to answer questions including those not relevant to the event
  - e. Perception becomes reality and misinformation spreads quickly
  - f. Allowing misinformation to spread can have serious consequences
  - g. Be aware that amplified demand for information and impaired judgment in stressful situations can contribute to the spread of rumors



## PRACTICE EXERCISE

The press conference: What does it do?

In a September 11, 2001 press conference, New York City Mayor Rudy Giuliani did not cry or exhibit other traditional motions of grieving. He simply gave the news, showing simple, moving restraint. When he met with worried and grieving families, he comforted them without creating a sense of false hope. At the following Sunday's memorial, he included a Muslim imam and appealed to the citizens to recognize Arab-Americans were innocent of the crime, but he also added additional police protection to prevent retaliation.

In June 2009, Mark Sanford, governor of South Carolina, left the office for a hike on the Appalachian Trail. He was out of contact from his family and his assigned police protection squad for four days. After he was spotted by a reporter while leaving an aircraft recently arrived from Argentina, not the Appalachian Trail, he held a press conference in which he stated that he had been unfaithful to his wife, that he had met his soul mate, that he had had affairs with a handful of other women and that he had "crossed the lines I shouldn't have crossed as a married man, but never crossed the ultimate line."

Both press conferences were filled with truthful and factual statements, but which press conference was more effective in restoring confidence?

Why?

## Review of Learning Objectives

1. Using an understanding of the common types of intellectual property and control options for intellectual property, participants will create a plan for protecting the various types of intellectual property in his/her institution.
2. Using knowledge of the factors that influence reputation and brand and the risk control mechanisms used to manage an organization's reputation and brand as well as knowledge of key components that make up the content of communication, participants will design a communication plan for protecting his/her organization's reputation and brand.





# Certified Risk Managers

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

## Section 7

# Executive Risk





### Key Terms



## Executive Risk

### Section Goal

To provide participants with the transformative and practical knowledge to identify and manage the exposure created by management activities and to properly address liability derived from executive risks by implementing risk controls

### Learning Objectives

1. Using knowledge of the **types of laws** that create the potential for executive liability, participants will create a plan for managing Executive Risk.
2. Using knowledge of the **common law duties** of directors and officers, directors and officers liability, **control methods** commonly used to manage directors and officers exposures, and the **Business Judgment Rule**, participants will create a plan to manage exposures caused by officers and directors.
3. Using understanding of the **duties and responsibilities of fiduciaries**, participants will assign **risk control methods** specific to fiduciary exposures.



Running a business inherently comes with risk. Executive risk, which is liability that arises from management activities, needs to be identified and controlled. The risk manager needs to implement control techniques to reduce the frequency and severity of potential management liability claims. They may also transfer some of the risk through insurance options, such as:

*Employment Practices Liability (EPL)*

*Directors & Officers Liability (D&O)*

*Fiduciary Liability*

Even if insurance coverage is purchased, the risk manager still needs to manage the exposures from inside the organization.

Statistics show that lawsuits can come from shareholders as well as current and former employees, competitors, customers, vendors and governmental and regulatory agencies. Liability arises out of violations of common law, statutory law, and regulatory provisions in addition to breaches of duty, fraud, unfair business practices, infringement of trade secrets, and other wrongful acts.

The risk manager needs to understand the basis and sources of potential liability facing the organization to properly manage executive risk.






### Learning Objective 1:

Using knowledge of the **types of laws** that create the potential for executive liability, participants will create a plan for managing Executive Risk.

**Common law** – refers to precedents and/or prior rulings by judges and juries



**Civil law** – while the interests of society are protected by criminal law, the interests of individuals are protected by civil law



# Civil Law

---

Torts  
Contracts  
Statutes

**Civil law includes the following:**



1. **Torts** – a tort is a private or civil wrong, other than a breach of contract, for which the courts will allow an action (lawsuit) for damages
  - a. Unintentional – an unintended accident that leads to injury, property damage or financial loss. In the event of an unintentional tort, the person who caused the accident did so inadvertently and typically because he or she was not being careful. The person who caused the accident is considered *negligent*.

**Negligence** is the failure to exercise that degree of care which a reasonably prudent person would exercise under the same circumstances.

**The elements of negligence are:**

- 1) **A duty owed** (by the defendant to the plaintiff)
- 2) **A breach of that duty**
- 3) **Causation** – the breach of duty must be the proximate cause of the injury, in an unbroken chain of events
- 4) **Damages** resulting from the injury

*All four elements must be proven to establish negligence.*

- b. Intentional – when an individual commits an act with the intention of causing injury, damages or a violation of another person’s rights

Examples of intentional acts:

- Libel/slander
- Assault/battery
- Wrongful detention/false imprisonment
- Discrimination

- c. Strict liability – liability directed by law (statute or common law) without regard to the intention of the offender’s actions. Strict liability shifts the burden of proof; it creates a rebuttable presumption that the defendant must overcome.

Examples of strict liability:

- Keeping wild animals – zoos are strictly liable for injuries caused by their animals; private individuals may also be held strictly liable for injuries caused by wild animals in their care
- Selling alcohol to minors – a person can be convicted even if they believed the minors were old enough to buy alcohol – strict liability imposed by statute
- Ultra-hazardous/inherently dangerous activities (construction, blasting, excavation) – strict liability imposed by common law

- d. Remedies for tort actions awarded by the court

1) Damages – financial

a) Compensatory – to make the plaintiff whole

- Economic – medical, lost wages
- Non-economic – pain and suffering

b) Punitive – to punish or make an example of the defendant

c) Fines/penalties

2) Injunction – a requirement to refrain from doing an act, an enforcement of performance, or an obligation stated in a contract

a) Temporary restraining order

b) Peace bond

c) Cease and desist order

2. **Contracts** – the law of contracts governs the performance of a promise between parties

a. Four requirements for an enforceable contract:

- 1) Competent parties
- 2) Agreement or assent
- 3) Legal consideration (exchange of values)
- 4) Legal purpose

b. Remedies for breach of contract or failure to perform:

- 1) Damages – compensatory, punitive or liquidated
- 2) Reformation – change the contract to better reflect the intentions of the parties
- 3) Injunction – a requirement to refrain from doing an act, an enforcement of performance or an obligation stated in contract
- 4) Performance – enforced compliance with contractual promises

3. **Statutes** – enactments of legislative and administrative bodies (state and federal) that impose responsibility for certain actions or omissions
- a. Examples of statutes relevant to directors and officers
- Infringement of patent, copyright and trademark
  - False Claims Act: fraud in connection with government contracts
  - Tax withholding
  - Business incorporation acts
  - States that have codified the Business Judgment Rule, e.g., Delaware
  - Mirroring laws, e.g., COBRA
- b. Examples of exposures
- Fines
  - Penalties
  - Injunction



## Regulatory liability exposures

1. Mandatory compliance – examples
  - Licensing
  - OSHA
  - EPA
  
2. Voluntary regulations – rules created by professional, trade and other organizations to internally govern their members
  - a. Codes of conduct
  - b. Professional standards

## Private law

Organizational charters and bylaws – corporate rules that define what the executives can and cannot do and that carry the force of law. Violations of these laws are *ultra vires* acts, or “acts beyond the powers of the organization.”

In most cases financial liability cannot be accurately measured in advance of a loss. The amount of the loss depends upon the following:

1. Circumstances of the event
  
2. Nature and severity of the damage or injury
  
3. Degree of fault by one or more parties
  
4. Applicable law
  
5. Judge’s or jury’s decision



### **Learning Objective 2:**

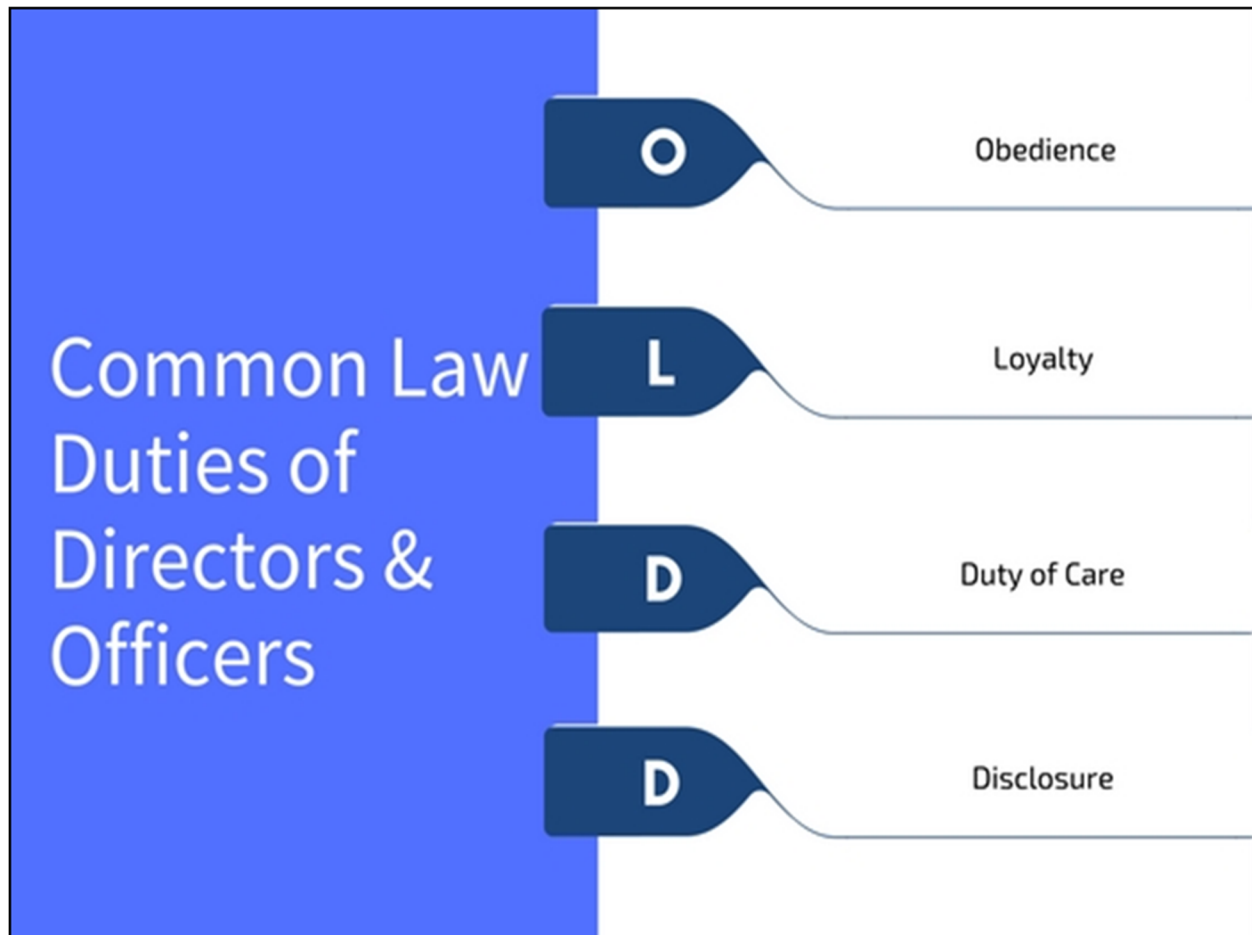
Using knowledge of the **common law duties** of directors and officers, directors and officers liability, **control methods** commonly used to manage directors and officers exposures, and the **Business Judgment Rule**, participants will create a plan to manage exposures caused by officers and directors.

The terms “director” and “officer” are not restricted to the senior management of a corporation, but can also include others, such as members of a limited liability company and senior managers of nonprofit organizations, regardless of their title. Additionally, under the law, a corporation is a person and therefore included as a director or officer.

Directors and officers liability results from a director or officer of an organization committing a negligent act or omission, misstatement or misleading statement.

Duties and responsibilities of a director or officer are to act as a reasonably prudent person in representing the interests of the organization's owners and other organizational constituencies while directing the business and affairs of the organization within the law.

1. What is a reasonably prudent person?
  - Frequently used in criminal and tort law as well as in the law of negligence, this term describes an ideal, hypothetical person who behaves in society under a standard of average care, skill and judgment and who serves as a standard for comparison when determining liability. Liability arises if one fails to exercise a similar level of care in similar circumstances.
  
2. Who are the organization's owners?
  - For profit vs. not-for-profit
  
3. What are the other constituencies?
  - Employees, customers, competitors, suppliers, contractors, government, etc.
  
4. What does within the law mean?
  - Ignorance of the law is no excuse



**Obedience** – actions conform to legal standards and requirements



**Loyalty** – undivided and unselfish loyalty with no conflict between organizational duty and self-interest

**Duty of care** – competent oversight of the organization in a deliberate and knowledgeable manner using the standard of care of a reasonably prudent person in a similar position in similar circumstances

**Disclosure** – disclosure of any interest in any transaction where the director or officer could be a beneficiary



### Board composition

1. Who is appointed to the board?

Board members should represent the nature of the business and the decisions that will be made in the board room and could include representatives from management, the community, shareholders and other stakeholders.

2. Should independent members be appointed to the board?

In an effort to diversify opinion and assure that the board does not become insular in its decision-making, independent board members may be appointed.

3. What is the preferred size of a board?

While there is no perfect size for a board, it should be large enough to provide diversity of thought, functional expertise and independent representation. However, it shouldn't be so large that it cannot be effective and efficient in decision-making unless executive committees are used; typically, an odd number is preferred to ensure a majority vote.

4. Who evaluates the board and board members?

- a. The board must analyze its own performance
- b. The board must analyze performance of its individual members

5. Should your board members have term limits?

Terms should be limited and staggered appointments are preferred to reduce brain drain and provide continuity.

6. What is the role of standard education for board members?

Completion of education programs should be documented annually to show that each board member has an understanding of the organization, applicable laws governing the organization and expectations and responsibilities of a board member.

## Procedural actions

1. Preparing for the meeting
  - a. Scheduling – how often are the meetings and are they scheduled at times that maximize attendance?
  - b. Notification – the timing and content of notice of meeting is dictated by corporate bylaws
  - c. Duration of meeting – no standard meeting time; long enough to adequately analyze and discuss matters, but not a marathon
  - d. Board books – evidence of due care; advance distribution of agenda and related documents, including executive summaries and supporting documentation
  
2. During the meeting
  - a. Formality – *Robert's Rules of Order* or a derivation of those rules
  - b. Presentation of information – appropriate use of PowerPoint with detail in the board book
  - c. Conduct
    - 1) Safe environment for open discussion where all members have equal opportunity for input
    - 2) Directors should engage in active questioning and challenging of issues; chair should try to receive input and feedback from every board member and to articulate an opinion last (still only has the weight of one individual vote)
    - 3) Dissent must be an affirmative vote against; abstention is tacit approval
    - 4) Recusal – excusing oneself due to a conflict of interest or potential lack of impartiality
  - d. Guest attendance – key management, outside advisors, employees, shareholders, etc.

3. Documentation
  - a. Accurate and complete minutes – precisely record matters considered, discussed and voted upon
  - b. Identification of documents incorporated by reference or attached to minutes
  - c. Precise record of results of any vote taken including identification of dissenting and abstaining directors
  - d. Avoid imprecise wording, inflammatory comments or ambiguous language
  - e. Pre-finalization review of minutes by directors and legal counsel or by risk manager
  
4. Opportunity for absent directors to review meeting actions taken and to record their support or dissent

## Delegation and the reliance defense

1. When to delegate – issues that are complex, require extensive analysis or research, or require specific expertise beyond the board’s capability
2. Types of delegation
  - a. Management – delegation of authority to management for issues and questions that come up to the level of the board but require more extensive input and are solely under the purview of management

### Examples:

- Bonus plans
- Work rules
- Dress codes

- b. Committee – facilitates an in-depth study of issues and brings special talents, expertise and experience to bear on problems

### Examples:

- Regulatory compliance
- Information privacy and security
- Collective bargaining



3. The defense of reliance on professional advice – the burden of proof is on the defendant to establish an affirmative defense and that defense is available to directors and officers under the following conditions:
  - a. Director sought out in good faith the advice of a professional who is considered competent in their area of expertise
  - b. Nature of advice sought must be within the scope of delegate's expertise
  - c. The advice was sought out and considered before taking any action
  - d. A complete and accurate account was given to the professional, including all pertinent facts (full disclosure)
  - e. Director acted in strict accordance with the advice given by the professional and with the knowledge that the advice was not unreasonable or repugnant

## Management of conflicts of interest

1. Avoiding conflicts of interest is central to the common law duty of loyalty and the Business Judgment Rule elements (discussed later) of disinterestedness and good faith
2. Conflicts of interest include actual conflicts, potential conflicts or the appearance of conflicts of interest
3. Conflicts of interest should be avoided as much as possible, but whenever they cannot be avoided, they must be managed
  - a. Unavoidable conflicts can be managed by:
    - Disclosure to directors
    - Abstention from discussion
    - Abstention from voting
  - b. Frequent disclosure, inquiries and reminders to maintain sensitivity to identification and handling of conflict issues
  - c. Formulation of organizational response to conflicts of interest that arise includes abstaining from, or participating in, an official action or remedial actions, such as looking at other alternatives
4. Recusal (abstention) is used when a board member has a disqualifying conflict of interest that might compromise that member's impartiality or create an appearance of impropriety

## Risk financing

Despite best efforts to manage exposures, the organization will still have claims. Therefore, an insurance policy needs to be purchased and/or corporate assets need to be reserved for funding.



# CONTROL METHODS TO MANAGE D&O EXPOSURES

## BOARD COMPOSITION

1. Who is on the board?
2. Should independent members be appointed?
3. What is the size of the board?
4. Who evaluates board members?
5. Do members have term limits?
6. What education is provided for board members?

## MEETING PROCEDURAL ACTIONS

1. Preparing - scheduling, notifications, length of meetings, board books
2. During - formality, presentations, conduct, attendance
3. Documentation - complete minutes, include reference documents, review of minutes by legal or RM, record of voting, clear language
4. Review actions with absent directors

## DELEGATION AND THE RELIANCE DEFENSE

1. When to delegate?
2. Types of delegation - management or committee
3. Defense of reliance on professional advice

## MANAGEMENT OF CONFLICTS OF INTEREST

1. Avoid them
2. Even the appearance of a conflict of interest is bad
3. When you can't avoid them, manage them
4. Use recusal when necessary

## RISK FINANCING

1. The organization is bound to have claims
2. Purchase an insurance policy OR
3. Set aside assets for funding

“Business decisions that are made in a disinterested manner with due care and good faith and no abuse of discretion shall be upheld.”



### Importance

Single most powerful defense available to a director or officer that insulates them from liability and recognizes that not all decisions will benefit the organization or its stakeholders or may even be unintentionally detrimental to the organization.

### Key elements

An “all or nothing” rule – each of the following five elements must be satisfied. Failure of even just one of these key elements will result in the defense not being available to the directors and officers.

1. **Business decision** – action must be taken in making business decisions, not personal decisions (i.e., not family disputes, personal gain, vendetta, anticompetitive); not taking action is protected if it was a conscious decision not to act
2. **Disinterestedness** – decisions are made in a deliberately objective manner and weigh heavily toward the needs of the organization and its constituents rather than toward individual personal gain of directors and officers
3. **Due care** – following a defensible procedure to fully deliberate on actions taken which include reviewing expert reports, documents, spreadsheets, financials, actuarial reports, etc.
4. **Good faith** – refers to the use of honesty and best efforts in dealing with others
5. **No abuse of discretion** – even with a defensible procedure, a failure to take into proper analytical consideration the facts and law to a particular matter



### Learning Objective 3:

Using understanding of the **duties and responsibilities of fiduciaries**, participants will assign **risk control methods** specific to fiduciary exposures.

**Definition:** The term “fiduciary” is not restricted to persons named as a fiduciary or “trustee” under ERISA; it can be extended to include anyone who has discretionary authority or control over plan assets, including the more mundane or clerical aspects of managing a plan, such as writing benefit checks.

**Fundamental responsibility** of a fiduciary – to act as a reasonably prudent person in representing the interests of the benefit plan, its participants and beneficiaries, and the sponsoring organization while directing the business affairs of the benefit plan within the law.

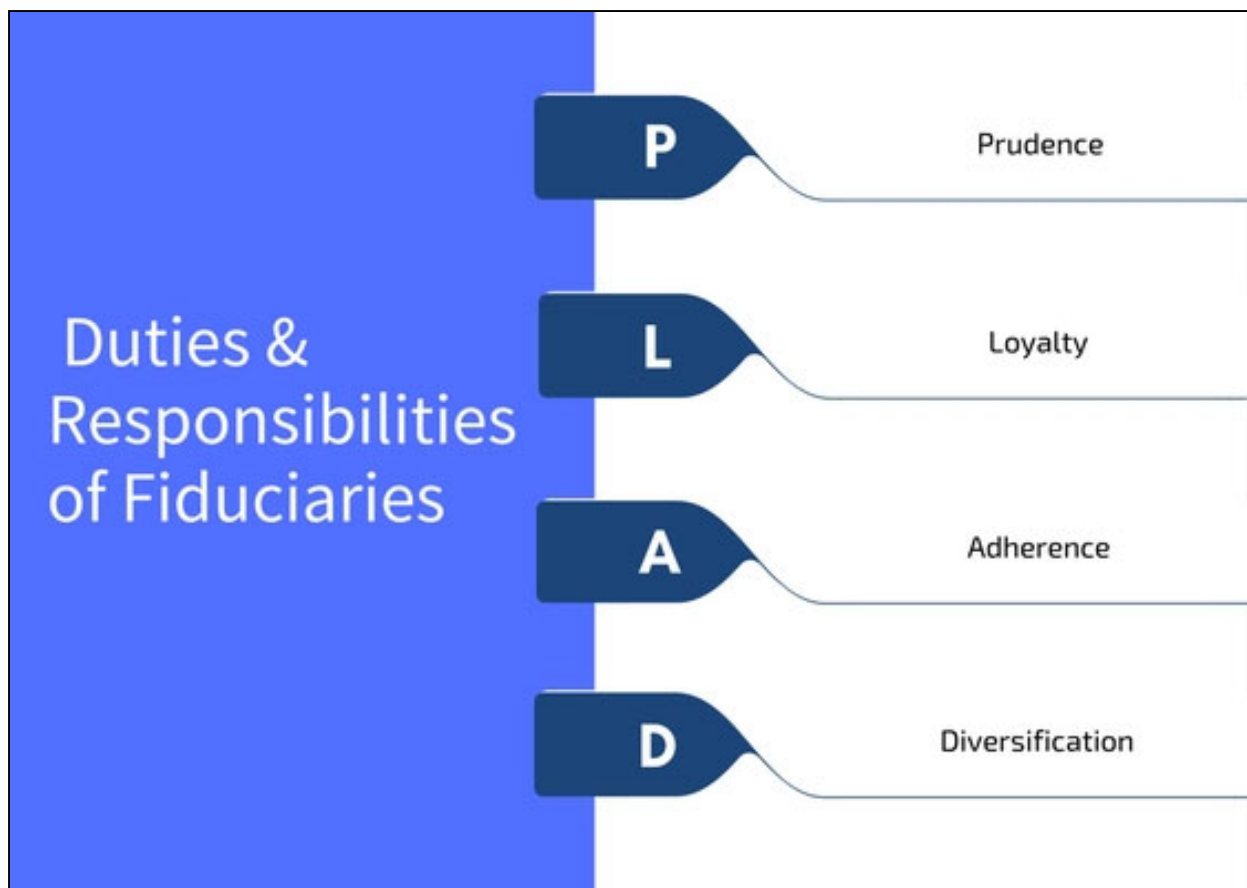
### Fiduciary liability arises from:

1. **Common law:** liability imposed upon a party who stands in a special relationship of trust with another party for a breach of that trust; federal and state courts have concluded that employers, employee and plan participants have a special relationship of trust
2. **Statutory law:** Employment Retirement Income Security Act of 1974 (ERISA) – liability imposed upon any person who exercises any discretionary authority or control with respect to the management or administration of an employee benefit plan or its assets

## Duties and responsibilities of fiduciaries



1. **Prudence** – like D&Os, fiduciaries must act as reasonably prudent persons in similar circumstances using the same level of care, skill and diligence
2. **Loyalty** – actions on behalf of the plan must be solely for the benefit of the plan participants
3. **Adherence** – must adhere to ERISA standards and the plan documents
4. **Diversification** – plan investments must be sufficiently diversified to minimize risk



**Fiduciary exposures** – exist with the management of any plan, fund or program established or maintained for the purpose of providing employee benefits to its participants or beneficiaries (ERISA)

1. Generally, there are two types of benefit programs:
  - a. Employee retirement benefit plan – any plan that provides retirement benefits to employees or defers income for employees to periods after termination of employment
  - b. Employee welfare benefit plan – any plan that provides medical care or benefits for sickness, accident, disability, death, unemployment, vacation, training, day care, scholarships, prepaid legal services or any other plan as described in the Labor Management Relations Act

## Prohibited transactions specific to fiduciaries under ERISA

1. Self-dealing transactions – any that use plan assets for personal gain, use plan assets on behalf of persons whose interests are adverse to the plan or personal gain in connection with any transactions

Examples:

- A fiduciary grants a loan to his family at a preferred interest rate
- A fiduciary grants herself a benefit that is not available to other participants
- A fiduciary authorizes \$25,000 monthly compensation for his advisory services

2. Party-in-interest transactions – include the following individuals:

- a. Any person who provides services to the plan
- b. Fiduciaries and employees to the plan
- c. An employer whose employees are covered by the plan
- d. A person who owns 50% or more of such an employer or employee association
- e. Relatives of any of the aforementioned individuals

3. Other “transactions” include:

- a. A sale, exchange or lease of property
- b. A loan or extension of credit
- c. The furnishing of goods, services or facilities
- d. A transfer of plan assets
- e. An acquisition of employer securities or real property above the ERISA limit

Examples:

- A fiduciary selects a plan provider who employs a close relative
- A fiduciary selects a plan provider in which the fiduciary has a financial interest



## Other sources of liability

1. Administrative or clerical actions
  - a. Benefits denials or changes
  - b. Incorrect benefit calculations
  - c. Wrongful termination of an individual's benefits
  - d. Misrepresentation of benefits or features
  - e. Administrative errors
  - f. Incorrect or inappropriate advice
  
2. Managerial actions
  - a. Allowing excessive fees to be charged by co-fiduciaries, such as TPAs and investment advisors
  - b. Inadequate funding of plan
  - c. Imprudent investment decisions
  - d. Wrongful termination of an entire benefit plan
  - e. Civil rights denial or discrimination
  - f. Conflicts of interest

The same five key elements of the Business Judgment Rule that apply to directors and officers also apply to fiduciaries. In this section, we will discuss the additional control mechanisms that are specific to the fiduciary exposure.



# 5

## METHODS TO MANAGING FIDUCIARY EXPOSURES

- 1 BOARD COMPOSITION
- 2 PROCEDURAL ACTIONS
- 3 DELEGATION
- 4 MANAGEMENT OF CONFLICTS OF INTEREST
- 5 RISK FINANCING

## Fiduciary/trustee board composition



In addition to the board composition discussion for directors & officers, fiduciaries cannot have been convicted of certain criminal offenses. Under a Taft-Hartley (union) plan, there must be an equal number of management and employee representative trustees.

1. Evaluation of fiduciaries more specifically includes:
  - a. Performance assessments of co-fiduciaries and outside consultants
  - b. System for identifying and investigating complaints
  - c. Administrative time and cost efficiencies
  - d. Investment performance

7

**Procedural actions** – in addition to the procedural actions in the D&O section, for fiduciaries there are sponsor oversight responsibilities to establish:

1. Operating procedures
2. Procedures for evaluation of reports, compensation records, outside benefit records, participant entry and exit
3. Procedures for secure data transmission and storage (under HIPAA and other statutes)

**Delegation** – in addition to the delegation guidelines for D&O, the following points are applicable to fiduciaries:

1. Delegation defense not available unless the plan documents specifically authorize delegation
2. Delegate must meet ERISA requirements and be adequately capable of fulfilling delegated duties
3. Delegation must be to a registered investment advisor, bank or qualified insurance company with acknowledgement of fiduciary status; delegation transfers fiduciary liability, but fiduciaries are still responsible for negligent selection and supervision
4. Fiduciaries must be willing to revoke the delegation of responsibility

**Management of conflicts of interest** – in addition to the points regarding managing conflicts of interest for directors and officers, the following points are applicable to fiduciaries:

1. Fiduciary employed by plan sponsor
  - a. Inherent conflicts of interest include conflicting duty of loyalty to employer, fiduciary duty to plan and self-interest in plan benefits
  - b. Requires exercise of extraordinary care in making decisions that are fair to participants and the plan
  - c. Requires documentation of provable fairness
  - d. Special problem areas
    - 1) Sponsor fails to contribute to plan
    - 2) Stripping of assets or termination of an overfunded plan

**Risk financing** – administrative or clerical actions can be insured with an employee benefit errors and omissions endorsement, but managerial actions can only be insured on a fiduciary liability policy. Endorsement also exists for fines and penalties imposed by ERISA.

## Review of Learning Objectives

1. Using knowledge of laws that create the potential for executive liability, participants will create a plan for managing Executive Risk.
2. Using knowledge of the common law duties of officers and directors, officers and directors liability, control methods commonly used to manage directors and officers exposures, and the Business Judgment Rule, participants will create a plan to manage exposures caused by officers and directors.
3. Using understanding of the duties and responsibilities of fiduciaries, participants will assign risk control methods specific to fiduciary exposures.





## Certified Risk Managers

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

### Section 8

# International & Multinational Risks





### Key Terms



### Unctad.org



### USNews 13 Superstitions Article



## International and Multinational Risks

### Section Goal

To provide participants with relevant knowledge to be able to properly adjust the risk management program to meet the unique needs of international exposures

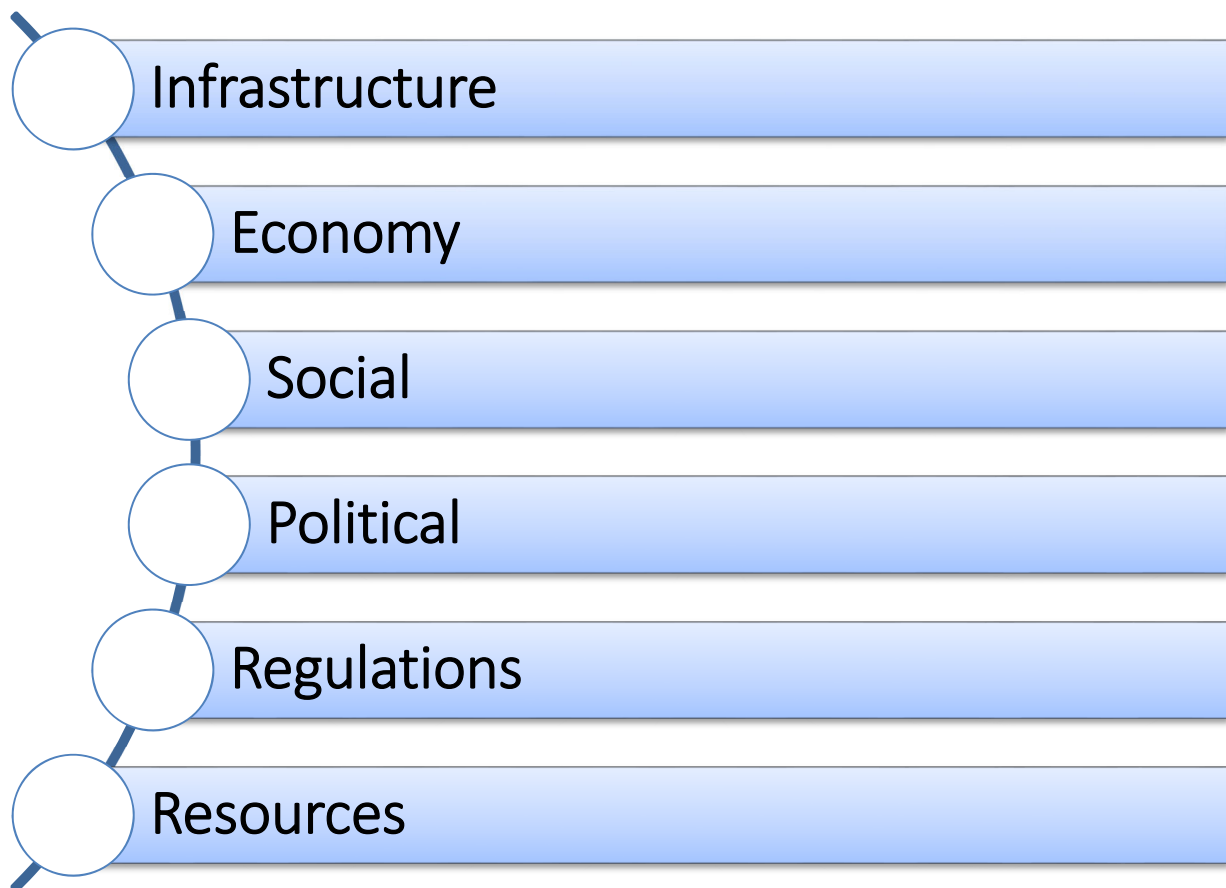
### Learning Objectives

1. By understanding the various **business arrangements** and **types of operations**, participants will be able to adjust the risk management program to address international exposures.
2. With an understanding of the various **exposures related to international travel** and the **cultural sensitivities** that exist, participants will be able to advise and prepare others for international travel and interactions.
3. With a knowledge of available insurance programs, **policy mechanics and costs**, participants will be able to positively influence decisions regarding the **insurance needs and legal requirements** for international operations.

## Introduction

When an organization is considering expanding beyond its home country, whether international travel or opening a location in another country, there are a vast number of risks that must be thoroughly considered in advance to ensure the organization is protected.

Entering into the foreign market exposes a company to political, legal, financial and social risks. Some of the basic considerations might be:



**Infrastructure** – How easily can you get around or get in and out of the country? Is it easy to ship to and from? Do they have a solid communication network? Will there be access to health care or emergency services?

**Economy** – What is their current economic status? What is their unemployment rate? Do they have a skilled labor force? Is their currency strong and stable? Is their monetary policy influx?

**Social** – What is the culture? Are they struggling with terrorism or civil unrest? What is their anti-foreign sentiment? Is there crime, corruption or fraudulent practices?

**Political** – Is the government stable? How are their diplomatic relations with other countries? Which countries? Is there any anticipation of or struggle for a change in power?

**Regulations** – What are their foreign trade policies? How do their environmental policies differ? What is their source of law? (Most of the world operates on European civil law, not the U.S.'s English common law.) Is their legal system strong or poor? What are their laws concerning banking, intellectual property, tariffs and taxes?

**Resources** – Consult with the CDC (Centers for Disease Control and Prevention) on any health or safety concerns. Check the International Trade Association (ITA) within the U.S. Dept of Commerce for support. Be compliant with the FCPA (Foreign Corrupt Practices Act).

Any organization with international operations should keep a watchful eye on local conditions to ensure that risks are being effectively managed. To secure the financial interests of a parent company, preparation and attention are paramount to protect an organization from threats to international business. With a constantly changing global market, a good risk management strategy will depend on regular research and updates to the international risk management policy.



### **Learning Objective 1:**

By understanding the various **business arrangements** and **types of operations**, participants will be able to adjust the risk management program to address international exposures.

---



### **Exclusive Distribution Arrangements**

- Parent company partners with another company in a different country that will distribute their product in a new market
- Allows the parent company the opportunity to enter a new market quickly, but at the risk of losing control of product or service to the distributing company

### **Joint Ventures**

- Some countries do not allow U.S. companies to have ownership of property in their country
- Other laws may be highly restrictive or prohibitive on Americans or other foreigners wanting to do business within the country
- Joint ventures are formed between a foreign party and a company of the home country
- Allows entry into a foreign market without expense of another branch or subsidiary
- Due diligence is required by the Foreign Corrupt Practices Act to establish relationships with foreign parties

**Global Company** – centralized production and cost sharing, including certain shared services for certain functions, such as accounting, treasury and real estate

- Investment in other countries
- Consistent brand and image with products and markets controlled by a home office

**International Company** – is an extension of the parent company

- Operate from a home country only
- Import and export goods to and from other countries

**Multinational Company**

- Investment in other countries
- Products and services focused on local market

**Transnational Enterprises**

- A commercial enterprise that operates substantial facilities
- Does business in one or more countries
- Does not consider any particular country its national home



## Operations



Just as there are many types of organizational structures that may have international exposures, there are also many types of operations that could be exposed to risk internationally. These include:

1. Organizations with assets, operations and employees outside their home country which may include:

Manufacturing	Home offices	Corporate apartments
Retail locations	Land ownership	Satellite offices

2. Products or services which are exported to other countries outside the organization's home country. Although most General Liability programs provide "worldwide territory" coverage, a suit may need to be brought in the organization's home country.

3. Organizations that engage with foreign suppliers or service providers:

Client technical support	Call centers	Outsourcing product assembly
Raw materials	Components	

4. Employees who travel outside their home country for business purposes. Auto accidents, medical issues and personal security are some of the risks for this exposure. Services such as repatriation, travel security information and medical assistance are normally provided by the company.

Regardless of the type of operation, considerations should be made to facilitate collaboration across time zones. Whether working with another location or supplier or planning for travel, it is important to be mindful of date and time differences as these can impact communications and even recordkeeping.



## Learning Objective 2:

With an understanding of the various **exposures related to international travel** and the **cultural sensitivities** that exist, participants will be able to advise and prepare others for international travel and interactions.

With locations or operations overseas, a need to manage risks related to travel may arise. International travel requires planning beyond what you normally do for domestic travel.



### Legal documents

- Current passport (including backup copies stored separately) that is valid at least six months beyond trip duration
- Travel visas if required
- Registered traveler programs – Global Entry, Clear, TSA PreCheck, etc.

### Credit cards

- Alert banks or credit card companies of travel plans
- Learn what forms of payment are accepted – cash only? chip cards?
- Company credit cards – Are there foreign transaction fees? How is currency converted?

## Exchange rates

- Currency conversion apps assist with currency calculations
- If currency exchange will be required, know where and how this can be done most efficiently and cost-effectively
- Prepare for transactions that may require local currency, such as public transportation

## Transportation

- Know safe travel options – public transportation, hired cars, etc.
- Car rental
  - Driving permits required
  - Insurance requirements
  - Damage waivers
- Carry a business card from your hotel or office to show taxi driver

## Communication

- Cell phone coverage
- Internet access

## Packing and luggage

- Chargers and adaptors
- Extra clothes in carry-on
- Luggage restrictions – checked bags or carry-ons
- Luggage delays/lost luggage



## Health and safety

### Research

- Determine vaccination recommendations/requirements – also check if country requires proof of certain vaccinations for entry (the CDC is a good resource)
- Be aware of regional health concerns and appropriate precautions – Are there medications you can have prescribed prior to travel, e.g., antimalarial pills?
- If travelling with a chronic or preexisting condition, make sure you know where you can go should treatment be necessary. How available or accessible are medical facilities? Do you need disability accessibilities?
- Check travel alerts and advisories (<https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html>)

### Prepare

- Carry basic medicines and first aid supplies; be mindful that some medications may be illegal or regulated in the destination country
- Insurance coverage – travel insurance (be sure to read the exceptions and limitations); Is foreign coverage included in your health plan or do you need a supplemental policy?
- Consider registering with your home country's embassy for notifications and potential assistance – Smart Traveler Enrollment Program (STEP)
- Know what embassies and consulates are available to you in which countries; <https://travelmaps.state.gov>
- Have an exit strategy

Understanding the complexities of cultural differences and practicing cultural sensitivity is crucial for successful business interactions.



1. **Language and communication styles** – What is the country’s official language? Do you have translation available? Is communication more formal or informal?
2. **Customs** – religious observances, holidays, beliefs or superstitions (e.g., in the U.S., Friday the 13<sup>th</sup> causes concern, but in Spain, it is Tuesday the 13<sup>th</sup>)
3. **Etiquette**
  - Behavior – proper greetings, hand gestures, hand holding, table etiquette at meals
  - Dress – head coverings, legs exposed, traditional costumes, colors
  - Activities
    - In the U.K. you cannot “hold a salmon under suspicious circumstances”
    - You must keep your feet on your bicycle pedals in Mexico
    - Chewing gum is illegal in Singapore, and selling it can earn you a \$100,000 fine
    - Feeding the birds in St. Mark’s square in Venice can result in a \$700 fine
    - It is illegal to let your chickens cross the road in the town of Quitman, Georgia
4. **Alcohol, tobacco and drug regulations** – the laws around certain substances can vary widely; think Amsterdam vs. Malaysia
5. **LGBTI (Lesbian, Gay, Bisexual, Transgender, Intersex)** – acceptance of alternative lifestyles will also vary greatly by country

USNews  
13 Superstitions  
Article





### Learning Objective 3:

With a knowledge of available insurance programs, **policy mechanics and costs**, participants will be able to positively influence decisions regarding the **insurance needs and legal requirements** for international operations.

The successful implementation and ongoing program administration for multinational risks can be one of the most arduous to execute. It requires an extensive amount of planning, communication, coordination and monitoring to achieve the optimal results.

1. **No global standard** – Insurance regulations, compliance requirements and application of law fluctuate widely across the globe. Unlike in the U.S. where much has been done to bring consistency to insurance programs, other parts of the world are in various stages of evolution. Europe is most mature, China is growing, and Latin America is in the beginning stages of evolution.
2. **One size DOES NOT fit all** – Each organization and exposure present distinctive opportunities and objectives. This requires a tailoring of risk management and insurance programs, broker networks, carrier partners and other service professionals.
3. **Learning curve for all parties involved** – Various internal & external stakeholders are involved in identifying, quantifying and comprehending the risks and exposures.

<i>Internal Stakeholders</i>	<i>External Stakeholders</i>
Strategic Planning	Outside Auditors
Operational Management	Insurance Carriers
Legal Departments	Global & Local Insurance Brokers
Human Resources	Forensic Accountants
Treasurer, Finance & Accounting	Asset Appraisal Companies
Real Estate Department	Outside Counsel with Country Expertise



1. **Compulsory insurance** – Any line of coverage which is required by law in a specific jurisdiction (country) for a company with operations in that same respective country. Auto coverage is typically a compulsory coverage requirement in most countries.
2. **Regulatory compliance** – A body of statutory law, administrative regulations and jurisprudence that governs and regulates insurance coverage requirements within respective country. The rules governing requirements for “admitted” coverage in a country is an example of regulatory compliance.
3. **Admitted coverage** – Policies are covering risks in a country. This is underwritten by an insurance carrier licensed to write coverage in the same country where risks exist. Admitted insurance programs are typically “local policies” issued in the native language.
4. **Non-admitted coverage** – Policies are covering risks in a country where the insurance carrier is NOT licensed to write coverage in the same country where risks exist. Non-admitted coverage is commonly known as a “global” policy.

## Program Structures

The three types of program structures utilized in most multinational risks are: Global, Controlled Master and Local Policy.

### GLOBAL PROGRAM

**\$200M Limit**

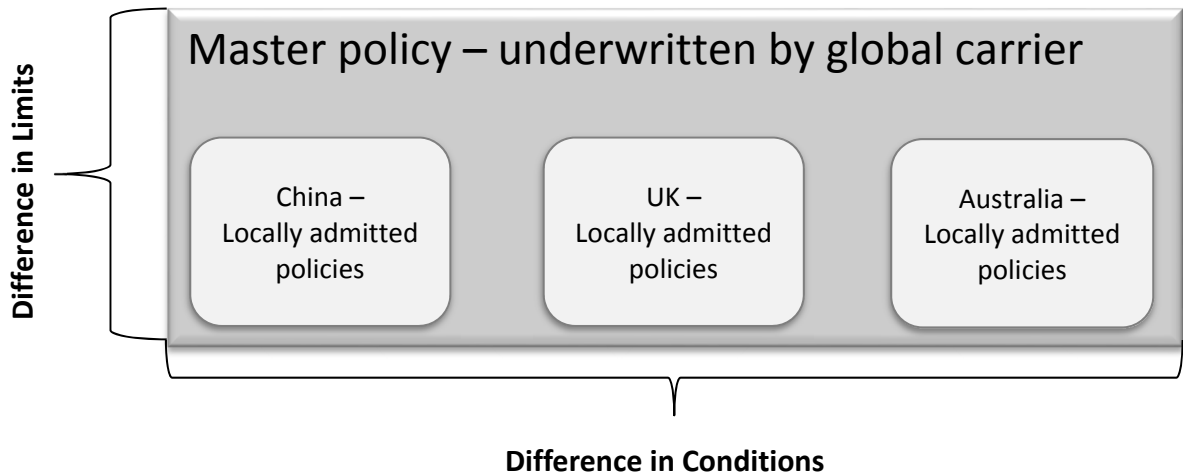


*Limits can be provided by one of multiple insurance carriers*

8

Pros	Cons
Terms, conditions & limits consistent across all locations & exposures	Coverage may not be “admitted” in certain countries, depending upon insurance carrier status
All risks are pooled, usually resulting in more efficient pricing	May not have ability to provide local claims service & engineering in all countries
Mitigates exchange rate issues	May not be fully compliant with local regulations
	No access to government pools (terrorism)

## CONTROLLED MASTER PROGRAM



Pros	Cons
Master policy acts as a backstop for local policies with DIC/DIL (difference in conditions/difference in limits) feature	A limited number of global carriers have ability to write these programs, creating less competition
Local admitted policies provide ability to pay claims & conduct engineering in country	Some countries may require “fronting” if global carrier is not licensed; this can increase the frictional cost of programs
Consolidates all policy terms and loss information into one program for easier administration	
Ability to add on new countries with same terms & conditions	Development & implementation time for this type of programs is increased
Provides non-admitted coverage in countries with no locally issued policies	

## LOCAL POLICY PROGRAM



Pros	Cons
Programs tailored to local regulations and provided in local language	Administration in placing, tracking & paying premiums to multiple insurance carriers with various renewal dates and policies can be overly burdensome
Typically, these programs have lower deductibles and retentions	Insurance programs can be more expensive because of the inability to pool exposures and gain cost efficiencies
Allows organizations access to reinsurance pools (terrorism)	Inconsistent coverage, terms & conditions across the organization/company

Given the multitude of choices in program structures, companies should consider their specific needs within four main categories before determining which insurance program best suits their risks.



Services  
Required

Jurisdictional

Claims  
Handling

Tax  
Strategies

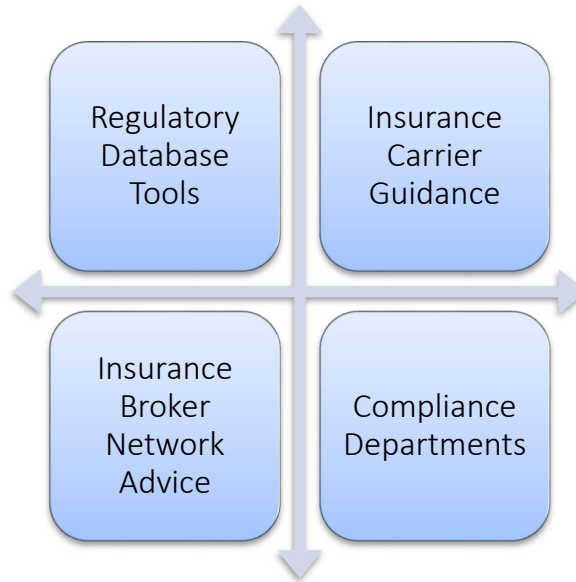
### ***Services Required Locally***

1. Are certificates of insurance, evidence of auto coverage and/or claims administration needed locally?
2. What type of legal representation will be needed in-country? Does the organization have adequate in-house counsel or should outside counsel be arranged with appropriate jurisdictional expertise?



## ***Jurisdictional Regulatory***

With the emergence of better communication technologies as well as increased local insurance market and regulatory tax sophistication, governmental agencies can track and monitor compliance in a manner not seen before. A common platform to assist in understanding regulatory compliance requirements in each country includes four elements.



1. Regulatory database tools such as AXCO ([www.axcoinfo.com](http://www.axcoinfo.com)) provide extensive resources for regulation and tax compliance
2. Insurance carrier guidance – many global carriers have developed their own technology tools which incorporate best practices for regulatory compliance in each country; these tools are commonly available to the insured organization
3. Insurance broker networks and local brokers in-country are a critical resource to understand compliance issues by jurisdiction
4. Compliance departments – these may be in-house or outsourced to compliance consultants who specialize in risk management and insurance programs

## ***Claims Handling***

Proper claims handling requires preparing for both pre-loss and post-loss activities:

<b>Pre-Loss</b>	<b>Post-Loss</b>
Adequacy of coverage to protect assets and revenue as respects policy wording, legal venue, arbitration clauses and duties in the event of loss.	Where does the organization want the claim to be paid? If claim needs to be paid in-country, then the admitted coverage must be written in-country.
Claim payment expertise and reputation as respects insurance carrier and resources.	How should the claim be paid? Determining the currency utilized, foreign exchange issues, services required.
Insurance carrier financial strength.	

## Tax Strategies of the Organization

A portion of the decision-making process concerning how an organization will address their multinational risk exposures is to understand each organization's unique tax strategy in designing the appropriate risk management and insurance programs. The two areas of focus are:

Premiums	Claims
<ul style="list-style-type: none"> <li>• Under a master controlled or global program, premiums will be allocated to the local subsidiary</li> <li>• The Organization for Economic Co-operation and Development (OECD) has transfer pricing guidelines that require a transaction which is controlled between commonly owned affiliates meet specific standards</li> <li>• Namely, the allocation must be consistent with what would have been charged if the subsidiary engaged in the same transaction as a non-affiliate</li> </ul>	<ul style="list-style-type: none"> <li>• Tax ramifications for claims payments made locally or corporately exist and should be considered for each jurisdiction/territory</li> <li>• If a claim is paid on a non-admitted basis, the organization could potentially face a corporate income tax in the home country where claims are paid and/or a capital infusion tax when transferring claim payments to the local operating subsidiary</li> </ul>
<ul style="list-style-type: none"> <li>• If premium payment is being deducted locally, it's important for the deduction to be coordinated with the parent company to avoid any adverse tax implications</li> <li>• It is required that premium taxes be paid in each country where the risk is located</li> </ul>	



1. **Good Local Standard** – Policy wording which most insurance carriers licensed to write coverage in the respective country would quote competitively to most local clients.
2. **Difference in Conditions (DIC)** – Policy feature whereby coverage provided under the master policy is broader than the underlying local policy.
3. **Difference in Limits (DIL)** – Policy feature whereby limits provided under the master policy are greater than those provided by the underlying local policy.
4. **Financial Interest Clause** – Amends an insurance policy to cover only the multinational’s financial interest in its worldwide subsidiaries. The parent company is the only legal entity covered under this clause in the global policy. These provisions have not been tested widely in claim scenarios and therefore may trigger undesirable and/or unforeseen adverse tax consequences. In addition, for clients who are required to place coverage on a “shared or layered” basis to achieve required limits, this coverage may not be concurrent throughout the limit tower. Some insurance carriers will not follow this endorsement.
5. **Tacit Renewal** – Contract of insurance renews automatically without either insured or insurer having an obligation to act. This renewal happens at a predetermined date, calculated by deducting the “notice period” (most often expressed in a number of days) from the anniversary date of the contract. These “notice periods” can also vary by both country jurisdiction and coverage line of business. For example, in Germany, a 93-day notice period is required; for Canada that notice period is only 15 days and only for automobile lines of coverage. The obligation to notify the current insurance carrier that coverage is not being renewed has some complexities as well. In some countries, it is required that the local client (not the corporate home office) notify the respective insurance company of intent not to renew.
6. **Cash Before Cover** – Regulatory requirement in particular countries whereby insurers will not guarantee any coverage until all related premium payments have been received from the insured. China, Taiwan and Nigeria are all cash before cover jurisdictions.

7. **Tariff Rates** – In international insurance, refers to rates and coverages set and published by the rating bureau having jurisdiction in a country. These rating agencies may be controlled either by an association of companies or by a government, depending on the jurisdiction. Tariff rates vary by country and line of coverage.
8. **Taxes (non-admitted)** – Paid by the *insured*.
9. **Taxes (admitted)** – Paid by the *insurer*.
10. **Exportability of Premium** – The percent of premium allowed by each jurisdiction (country) to be exported from local policy to non-admitted (master) policy.
11. **Exportability of Risk** – The percent of exposure allowed by each jurisdiction (country) to be exported from local policy to non-admitted (master) policy.

## TCOR Allocation

When setting up a multinational insurance program, organizations must decide how to share financial responsibility across locations or divisions.

As in typical TCOR allocations, insurance premiums, fees, taxes and other expenses related to the risk management program need to be accounted for in your TCOR calculation. However, this process may be complicated by varying laws, tax regulations, exchange rates and stakeholders. Some of the stakeholders include:

- Corporate (home office), which needs to ensure that the organization is adequately covered with an optimal financial structure
- A local company that will require costs be justified based upon a fair assessment of risk
- Insurance carrier will need to satisfy regulators that oversee the insured's local insurance operations that the premiums are fair, reasonable and commensurate with the risks being covered; many jurisdictions are savvy to allocation, which may avoid higher tax rates in specific countries

# TCOR

Sum of all RM costs and expenses

## INSURANCE COSTS

premiums, letters of credit,  
security deposits, etc.



## RETAINED LOSSES

deductibles, SIRs,  
ALAEs, etc.



## RM DEPARTMENT COSTS

salaries, RMIS, training,  
travel, overhead, etc.



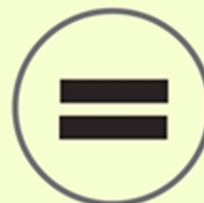
## OUTSIDE SERVICE FEES

TPAs, vendors, consultants,  
actuarial, legal, etc.



## INDIRECT COSTS

disruption in production/  
sales, replacement costs,  
overtime, reputation, etc.



# TCOR

## Review of Learning Objectives

1. By understanding the various company structures and types of operations, participants will be able to adjust the risk management program to address international exposures.
2. With an understanding of the various exposures related to international travel and the cultural sensitivities that exist, participants will be able to advise and prepare others for international travel and interactions.
3. With a knowledge of available insurance programs, policy mechanics and costs, participants will be able to positively influence decisions regarding the insurance needs and legal requirements for international operations.



