4 – Selecting Risk Control Techniques

**Objective**: Explain how each of these risk control techniques can be used to reduce loss frequency and/or severity: Avoidance; Loss prevention; Loss reduction

**1 – Using Avoidance, Loss Prevention, and Loss Reduction**

To select the most appropriate risk management techniques, risk professionals should consider the various techniques available so that they can determine which of them most effectively address an organization’s or individual’s loss exposures.

Risk management techniques fall into two categories: risk control and risk financing.

**Avoidance**

***Avoidance*** *– a risk control technique that* ***involves ceasing or never undertaking an activity*** *so that the possibility of a future loss occurring from that activity is eliminated.*

**The aim of avoidance is not just to reduce loss frequency, but also to eliminate any possibility of loss.** Avoidance should be considered when the expected value of the losses from an activity outweighs the expected benefit of that activity. Example, a toy manufacturer may decide not to produce a particular toy because the potential costs of products liability claims would outweigh the expected revenue from sales, no matter how cautious they may be in producing and marketing the toy.

Because loss exposures do not exist in a vacuum, avoiding one loss exposure could create or enhance another. Example, someone who is concerned about dying in an airplane crash, by avoiding air travel, they increase the loss exposure to injury or death from another method of transportation.

Complete avoidance is not the most common risk control technique and is typically neither feasible nor desirable. Loss exposures arise from activities that are essential to individuals and organizations. Therefore, it is not possible to avoid these core activities. Example, it is not possible to avoid core activities. If you are manufacturing motorcycle helmets, you could not stop selling them to avoid liability loss exposures.

**Loss Prevention**

***Loss prevention*** *– a risk control technique that* ***reduces the frequency*** *of a particular loss.*

Loss prevention reduces the frequency of a particular loss without avoiding it. For instance, pressure relief valves on a boiler are intended to prevent explosions by keeping the pressure in the boiler from reaching an unsafe level. The valve is a type of loss prevention, not avoidance, because a boiler explosion is still possible but not as likely.

In the exhibit shown involving a manufacturing company with 500 employees working at a single plant. The WC loss history shows a number of back injuries. They hired a consultant to host a series of educational seminars for its employees. The consultant estimates that, based on the results of their past seminars, this company will see a 20% reduction in the frequency of the back injuries. The frequency distribution prior to the seminar has a mean of 30, a standard deviation of 5.48 and a coefficient variation of 0.1827.

The frequency with the education seminar has a lower mean of 24, standard deviation of 4.20 and coefficient of variation of 0.1750. Based on these figures, the educational seminar would not only reduce the expected frequency, but also reduce their variability from year to year, which would allow the company to budget more effectively for those injuries that do occur.

**Generally, a loss prevention measure is implemented before a loss occurs in order to break the sequence of events that leads to the loss**. Because of the close link between causes of loss and loss prevention, determining effective loss prevention measures usually requires carefully studying how particular losses are caused.

According to Heinrich’s domino theory, most work-related injuries result from a chain of events that includes an unsafe act or an unsafe condition. Workplace safety efforts have therefore focused on trying to eliminate unsafe acts or unsafe conditions to break this chain of events and prevent injuries.

In 1931, H.W. Heinrich published the first thorough analysis of work injuries caused by accidents. He determined that work injuries were actually a result of a series of unsafe acts and/or mechanical or physical hazards (dominoes) that occurred in a specific order. He concluded that if any one of these dominoes could be removed from the chain, the work injury could be prevented. Heinrich’s theory included 5 dominoes: (1) Social environmental and ancestry, (2) the fault of persons, (3) personal or mechanical hazards, (4) the accident, and (5) the injury. If risk control measures could minimize mechanical hazards, the domino chain would be broken and fewer injuries would occur. Many of the principles outlined became the basis of modern risk control measures.

**As is the case with avoidance, a loss prevention measure may reduce the frequency of losses from one loss exposure but increase the frequency or severity of losses from other loss exposures**. Example, a jewelry store that installs bars on the windows is reducing the frequency of theft. However, those bars might make it impossible for firefighters to enter the building through the windows in the event of a fire.

**Loss Reduction**

***Loss Reduction*** *– A risk control technique that* ***reduces the severity*** *of a particular loss*.

Automatic sprinkler systems are a classic example of a loss reduction measure; sprinklers *do not prevent fires from starting, but they can limit or extinguish fires that have already started. Some loss reductions measures can prevent losses as well as reduce them*. Burglar alarms is generally considered a loss reduction measure because an alarm is activated only when a burglary occurs. However, because burglar alarms also act as a deterrent, they can prevent loss as well as reduce it.

As an example of a loss reduction measure, assume the consultant that was hired to conduct the educational seminars suggested they provide back braces for all of its employees because they help prevent back injuries and reduce the severity of back injuries. The exhibit the provide contains the original severity distribution and the new severity distribution with all employees using back braces. As with most severity distributions, it is not symmetrical, but skewed. Most back injuries are grouped in the left portion of the distribution (lower severity values), with some very serious injuries grouped as outliers to the right. This skewed distribution pulls the tail of the distribution to the right and increases the mean.

Note the difference between the means and modes with and without back braces. The use of back braces lowers the average severity (mean) by $15,792 (29,800 – 14,008 = 15,792) as well as the severity of the injuries that would occur most often (mode) by $5,000 (8,000 – 3,000=5,000).

The two broad categories of loss reduction measures are pre-loss measures, which are applied before a loss occurs, and post loss measures, which are applied after a loss occurs. **The aim of pre-loss measures is to reduce the amount or extent of property damaged and the number of people injured, or the extent of injury incurred from a single event**. The use of a back brace is a pre-loss measure; erecting a fire wall is also a pre-loss measure.

**Post-Loss measures typically focus on emergency procedures, salvage operations, rehabilitation activities, public relations, or legal defenses to halt the spread or to counter the effects of loss**. Example, moving an organization’s operations to a new location following a fire so that operations can continue while the damaged property is repaired, thus reducing loss severity.

**2 – Using Separation, Duplication, and Diversification**

**Objective**: Explain how each of these risk control techniques can be used to reduce loss severity and make losses more predictable: **Separation; Duplication; Diversification**. **These are Loss Reduction Techniques**

Before a specific risk control technique is recommended to an organization or individual, several available options should be considered.

In some situations, avoiding risk or preventing a loss is not feasible, either for logistical or financial reasons. Three risk control techniques allow an organization or individual to accept unavoidable risk by making losses potentially less severe and more predictable: Separation; Duplication; Diversification

**Separation**

***Separation – a risk control technique that isolates loss exposures from one another to minimize the adverse effect of a single loss***.

**Separation is appropriate if an organization can operate with only a portion of separate units intact after a loss**. Example, if a company produces products at two factories in different locations, the portion of the activity or assets at one factory must be sufficient for operations to continue if the other location is damaged or destroyed. Otherwise, separation has not achieved its risk control goal.

Separation is rarely undertaken for its own sake, but is usually a byproduct of another management decision. Example, few companies build a second warehouse simply to reduce the potential loss severity of a fire at one warehouse. However, if a company is considering constructing a second warehouse to expand production, the risk control benefits from a second warehouse could support the argument in favor of expansion.

**The intent of separation is to reduce the severity of an individual loss at a single location.** However, by creating multiple locations, separation most likely increases loss frequency. *Example, using two distantly separated warehouses instead of one reduces the maximum possible loss at each location*, but increases loss frequency because two units are exposed to loss. The insurance risk management professional should be confident that the benefits of reduced loss severity from separation more than offset the increased loss frequency.

Under Option A, the severity distribution is just the single outcome of a loss of 500K. There are two possible outcomes in any one year, a fire or no fire. Given a probability of .05%, they would expect a $500k loss 5% of the time and a $0 loss 95% of the time. Therefore, the expected loss in any given year is $25,000 (.05 x $500K = $25,000)

Under Option B, only $250K worth of merchandise is at risk in any one fire. Having two warehouses reduces the severity distribution from $500K to $250K.

*Increasing the number of warehouses increases the number of possible outcomes.*

*The expected loss remains $25,000, but the likelihood of suffering a $500K loss has fallen from 5% to 0.25%, whereas the likelihood of suffering a $250K loss has increased from 0 to 9.5%.*

The results in a total claims distribution for Option B that has a lower standard deviation than the total claims distribution for Option A. *The standard deviation of losses under Option A is $108,973, and the standard deviation for Option B falls to $77,055.18. Therefore, losses under Option B are more predictable than losses under Option A.*

|  |  |  |
| --- | --- | --- |
| **Option A** |  | **Central Warehouse** |
| **Value of Merchandise** | Value of Merchandise | $500,000 |
| **Probability of Fire** |  | .05 |
|  | Severity distribution (Max Loss) | $500,000 |
|  | Probability of fire | .05 |
|  | Expected loss (.05 x $500,000) | $25,000 |
|  |  |  |
| **Option B** |  |  |
|  | **Warehouse 1 (W1)** | **Warehouse 2 (W2)** |
| **Value of Merchandise** | $250,000 | $250,000 |
| **Probability of Fire** | .05 | .05 |
|  | Severity distribution (Max Loss) | $250,000 |
|  | Probability at W1 and W2 (.05x.05) | .0025 |
|  | Probability at W1 but not W2  [.05 x (1 - .05)] | .0475 |
|  | Probability at W2 but not W1  [(1 - .05) x .05} | .0475 |
|  | Probability of fire at either W1 or W2 (.0475 + .0475) | .095 |
|  | Probability of zero fires  (1 - .05) x (1 - .05) | .9025 |
|  | Expected Loss  (.0025 x $500K) + (.095 x $250K)] | $25,000 |

**Duplication**

***Duplication*** *– a risk control technique that uses* ***backups, spares, or copies of critical property, information, or capabilities*** *and keeps them in reserve*.

***Duplication is a risk control technique that involves actions such as maintaining duplicate records, spare parts for machinery, or copies of keys******and keeps them in reserve.*** Duplication differs from separation in that duplicates are not a part of a companies daily working resources. **Duplication is only appropriate if an entire asset or activity is so important that the consequence of its loss justifies the expense and time required to maintain the duplicate.**

**Duplication Example: Using more than one supplier for key raw material.**

Like separation, duplication can reduce an organization’s dependence on a single asset, activity, or person, making individual losses smaller by reducing the severity of each loss. Duplication is not as likely as separation to increase loss frequency because the duplicated unit is kept in reserve and is not as exposed to loss as the primary unit. Example, a secondary vehicle kept in a garage is not as vulnerable to highway accidents is the primary vehicle.

Duplication is likely to reduce the average expected annual loss from a given loss exposure because it reduces loss severity without increasing loss frequency significantly. Similar to separation, duplication can also make losses more predictable by reducing the dispersion of potential losses.

There are several measures an organization can implement that are similar to duplication and that incorporate non-owned assets.

*One option is for an organization to contractually arrange for the acquisition of equipment or facilities in the event that a loss occurs*. In this way the company can continue operations with minimal business interruptions and avoid the expense associated with owning or storing duplicate equipment.

**Diversification**

***Diversification*** *– a risk control technique that* ***spreads loss exposures*** *over numerous projects, products, markets or regions*.

**Although diversification closely resembles the risk control techniques of duplication and separation, it is more commonly applied to managing business risks, rather than hazard risk.**

**Organizations engage in diversification of loss exposures when they provide a variety of products and services that are used by a range of customers**. Example, and insurer might diversify by type of business and geography. Investors employ diversification when they allocate assets among a mix of stocks and bonds.

Aa with separation and duplication, **diversification has the potential to increase loss frequency, because the organization has increased the number of loss exposures. However, by spreading risk, diversification also reduces loss severity and can make losses more predictable**.

Organizations implement risk control techniques and the measures that support them to address one or more specific loss exposures. Each measure should be tailored to the specific loss exposures under consideration. Furthermore, the application of risk control techniques should serve to support an organization’s overall goals, pre-loss and post-loss risk management goals, and risk control goals.

**3 – Risk Control Goals**

**Objective**: Explain how each of these risk control goals benefits an organization: Implement effective and efficient risk control measures; Comply with legal requirements; Ensure business continuity

Different risk control measures will help an organization achieve its risk financing goals with varying degrees of effectiveness and efficiency. Therefore, when assisting other in selecting appropriate risk control measures, risk professionals must first seek to understand the risk control goals the organization is trying to achieve.

Because risk control is an integral part of a risk management program, risk control goals should support risk management program goals.

**Implement Effective and Efficient Risk Control Measures**

An organization generally undertakes risk control measures that have a positive financial effect. Most risk control measures are implemented at a cost to the organization. These costs are typically cash outlays, like the costs of the losses they aim to control, and are considered part of the cost of risk. However, so that risk control does not unduly increase the cost of risk one of the goals of risk control is to employ measures that are effective and efficient.

*A measure is effective if it enables an organization to achieve desired risk management goals, such as the pre-loss goals of economy of operations, tolerable uncertainty, legality, and social responsibility or the post-loss goals of survival, continuity of operations, profitability, earnings stability, growth, and social responsibility*.

The effectiveness of various risk control measures is often based on both quantitative and qualitative standards. Example, determining whether measures to ensure worker safety are effective may rely not only on statistics regarding WC claim, but also on employee satisfaction with the measures taken.

As well as being effective, risk control measures should be efficient. A measure is efficient if it is the least expensive of all possible effective measures. This does not mean an organization should choose the measure that entails the least initial cash outlay. The long-term effects should also be examined to determine which measures can be implemented with the least overall cost to the organization. Example, consider the need to improve security at night. The organization’s risk manager determined the cost of a new security system and stationing a night security guard. Which of these methods if most efficient.

There are several methods available for this comparison, one of which is cash flow analysis. The risk manager can use cash flow analysis to determine which measure will be must efficient.

In the example, both the security system and the security guard are equally effective; they both reduce annual losses by $40,000. Cash flow analysis shows that although the security system requires a larger initial investment, it costs less to operate and maintain each year.

If the risk manager examines these choices over a ten-year period, the annual cost of the security guard over multiple years eventually exceeds the initial investment required for the security system, making the security system ultimately more efficient.

**The major advantage of cash-flow analysis for selecting risk control measures is that it provides the same basis of comparison for all value-maximizing decisions and thereby helps the organization achieve its value-maximization goal.** **It is also very useful for not-for-profit organizations that want to increase their efficiency by reducing unnecessary expenditures on risk control**.

**The disadvantages of cash-flow analysis include the weakness of the assumptions that often must be made to conduct the analysis and the difficulty of accurately estimating future cash flows. Moreover, cash flow analysis works on the assumption that the only goal is to maximize its economic value and does not consider any of the nonfinancial goals or selection criteria**.

**Comply with Legal Requirements**

An organization may be required to implement certain risk control measures if a state or federal statute mandates specific safety measures, such as protecting employees form disability or safeguarding the environment against pollution. These risk control measures are a means of implementing the risk control techniques of avoidance, loss prevention, and loss reduction and they also support the risk management program pre-loss goal of legality. The cost of adhering to legal requirements becomes part of the cost of risk.

Many laws and regulations require organizations to implement specific risk control measures. Example; fire safety codes mandates certain accommodations for people with disabilities. These laws could require risk control measures that support avoidance (such as a ban of some toxic substances), loss prevention (such as safety procedures for machinery usage), and loss reduction (such as fire suppression systems).

**To comply with legal requirements when selecting risk control measures, an organization should consider state or federal statutes regarding fire safety codes, environmental regulations, workers compensations laws, and disability laws**.

Some laws and regulations are amended frequently, so it is important for risk professionals to be aware of these amendments. **Failure to comply with legal requirements exposes the organization to additional fines, sanctions or liability.**

**Promote Life Safety**

***Life Safety*** *– the portion of fire safety that focuses on the minimum building design, construction, and maintenance requirements necessary to assure occupants of a safe exit from the burning portion of the building*.

Safeguarding people from fire has grown in importance from a risk control perspective because of the emphasis on legislative bodies have placed on health and safety issues and because of the increasing frequency and severity of liability claims. In the context of risk control, life safety is the aspect of fire safety that focuses on the minimum building design, construction, operation, and maintenance requirements necessary to assure occupants a safe exit from the burning portion of the building.

**Life safety must consider both the characteristics of the people who occupy buildings and the types of building occupancies (such as residential, office, or manufacturing).** Consideration of the general characteristics of both building occupants and occupancy has led to the development of specific fire safety standards for buildings. These standards are codified in NFPA 101: Life Safety Cod and published by the National Fire Protection Association (NFPA).

**Promoting life safety can be expanded beyond fire safety to incorporate any cause of loss that threatens the life of employees, customers, or others. Therefore, organizations must be concerned about other causes of loss, such as a product safety, building collapse, industrial accidents, environmental pollution, or exposures to hazardous activities that may create the possibility of injury or death**.

**Ensure Business Continuity**

In addition to implementing effective and efficient measures, complying with legal requirements, and promoting life safety, risk control should aim to ensure *business continuity – that is, minimize or eliminate significant business interruptions, whatever the cause.*  Business continuity is designed to meet both the primary risk management program post-loss goal of survival and the post-loss goal of continuity of operations.

*Loss exposures and the associated losses vary widely by industry, location, and organization*. Some organizations are more susceptible to terrorism, some to technology problems and others to natural disasters. Because each organization is unique in its potential losses, each must also be unique in its application of risk control measures to promote business continuity.

**4 – Selection of Risk control Techniques**

**Objective**: Explain how risk control techniques can be selected for property, liability, personnel, and net income loss exposures.

**Property Loss Exposures**

The risk control techniques commonly selected for property loss exposures vary by type of property and the cause of loss threatening the property. Risk control measures used to prevent or reduce fire losses, for example, are substantially different from those used to prevent theft losses. Avoidance, loss prevention, loss reduction, separation, and duplication can all be applied in the same way to the broad array of property loss exposures.

**Commercial property underwriters commonly assess fire loss exposures for buildings and their contents based on each buildings fire construction, occupancy, protection, and external exposure (COPE Factors).** Each Cope factor can be addressed through the application of various risk control techniques.

|  |  |  |
| --- | --- | --- |
| **COPE Factor** | Description | Risk Control Technique |
| **Construction** | Materials and techniques (least resistive to most resistive) | Loss prevention/reduction to minimize frequency & severity |
| **Occupancy** | Residential, industrial with each presenting its own risk | **Loss reduction – safety & training and emergency evacuation** |
| **Protection** | Internal to protect the real property OR external – location of fire department public safety | Internal -Fire detection and suppression  External – select location near highly rated fire station |
| **External Exposure** | Exposed to hazards from outside sources. Neighboring buildings | Relocation away from external hazards |

**Liability Loss Exposures**

To select effective risk control for liability loss exposures, individuals and organizations need to understand the various ways in which their activities or operations can result in their becoming legally liable to others and what measures can be effective in preventing such incidents or reducing the damages for which they are held liable. **Three risk control techniques can be sued to control liability loss exposures.**

* **Avoid the activity that creates the liability loss exposures**
* **Decrease the likelihood of the losses occurring (loss prevention)**
* **If a loss does occur, minimize its effect on the organization (loss reduction)**.

The other risk control techniques of separation, duplication, and diversification are not as effective in treating liability loss exposures.

*Although avoidance is sometimes effective, it is often either not practicable or not possible to avoid undertaking the activity or activities that can lead to liability losses. Therefore, loss prevention and loss reduction measures are more typically used*.

*The most common loss prevention measure is to control hazards* (conditions that increase loss frequency or severity). Limiting the number or magnitude of hazards surrounding the loss exposures can prevent losses from occurring.

After a liability loss has occurred, individuals and organizations can implement loss reduction measures to reduce the severity of the liability loss.

* Consulting with an attorney for guidance through the legal steps necessary to resolve liability claims.
* Property responding to the liability claim and to the claimant in order to avoid feelings of ill will that may increase the claimant’s demands.
* Participating in alternative dispute resolution. Litigation is long and costly process. Alternative dispute resolution often helps resolve liability claims more quickly and more economically than litigation.

**Personnel Loss Exposures**

Personnel loss exposures are unavoidable, because all organizations have key employees. Theses loss exposures can arise from both inside and outside the workplace.

The risk control measures that organizations find most cost-effective are those that can be instituted in the workplace. Therefore, most risk control measures regarding personnel loss exposures involve preventing and reducing workplace injury and illness.

**Loss prevention measures used to control work-related injury and illness typically involve education, training, and safety measures.** An organization may also attempt to prevent personnel causes of loss that occur outside the workplace by controlling key employee’s activities through employment contracts; placing restrictions on hazardous activities. Alternatively, they may use a form of separation, such as restricting the number of key employees who can travel on the same aircraft.

**Loss reduction measures include emergency response training and rehabilitation management.** Although all organizations must comply with OSHA, additional training and safety precautions are often cost-effective.

**Net Income Loss Exposures**

Net income loss exposures can be associated with property, liability, or personnel exposures. Therefore, and of the risk control measures that control these three categories of loss exposures also indirectly control net income loss exposures. Example; to prevent a net income loss associated with a property loss exposure, an organization needs to prevent the property loss from occurring.

Reducing the immediate effect of property, liability, or personnel losses on net income, risk control efforts must also control long-term effects, such as loss of market share that can result from the net income loss. Example; if a manufacturer conducts a product recall, the manufacturer loses sales in the short term, causing temporary loss of revenue. If the manufacturer’s customers switch to purchasing products from other organizations, permanent market share could be lost, which is a long term-effect that translates to permanent revenue loss.

**Two risk control techniques that are directly aimed at reducing the severity of net income losses are separation and duplication**. Separation and duplication enable an organization to reduce net income losses by maintaining operations or quickly resuming operations following a loss. **Diversification is also a viable risk control technique for many because it helps to ensure that an organization’s entire income is not dependent on one product or customer**.

**5 - How Smart Products Apply to Risk Management**

**Objective**: Demonstrate how smart products can be applied to risk management.

Historically, risk managers’ assessments of the probability of adverse events were limited by the boundaries of human perception. Today, however, previously imperceptible risk factors, such as worker’s hydration level, the presence of a hazardous chemical in the air, or the catastrophic intersection of seemingly disconnected financial transactions, can be factored into risk management decision making.

**The new world of risk assessment data has bee revealed by smart products that sense their environment, process data, and communicate with other smart products and smart operations. These interactions generate big data – to which advanced analytics can be applied, ultimately reducing the uncertainty associated with predicting future events**.

***Big data*** *– Sets of data that are too large to be gathered and analyzed by traditional methods*.

As data technology evolves, the availability ad sophistication of **smart products that can help refine risk management techniques continues to grow:**

* **Wearables** such as helmets that monitor fatigue or wristwatches that measure vital sings can sense, monitor, report, and analyze workers’ health or well being and their surrounding environments. Data generated by wearable may be specific to one employee or aggregated for a project, team, or organization.
* **Drones can be used in surveillance and aerial photography; being unmanned and highly versatile makes them ideal for assessing conditions or risks in dangerous or unknown areas**. The data generated by drones relies heavily on other technology, such as computer vision, image recognition, and artificial intelligence, to mine the data collected and form conclusions about detected objects.
* **Robots** can measure, respond to, and produce data for monitored hazards or changing environmental conditions. Sensors in conjunction with high-definition cameras can scan and inspect bridges for erosion or other unsafe conditions.

**Property Management**

Property managers can use *wireless sensor networks (WSNs) to detect and respond to leaks and malfunctions or prevent on-site falls and injuries.* Example, **temperature and water sensors can monitor heat irregularities and detect the first signs of leakage** before tenants (especially lower-level ones in a multistory buildings) sustain water damage to drywall, carpets or furniture. **Temperature sensors provide alerts before a pipe freezes** and useful in vacant or temporarily unoccupied buildings. **Light sensors monitor illumination and provide lighting when needed around the perimeter of buildings, in parking lots, on stairs, and in underground parking garages, eliminating hazards that could lead to liability claims and lawsuits.** **Motion sensors and surveillance cameras can deter crime before it occurs and document suspicious activities**. **Thermal sensors, current sensors, and smoke detectors can detect impending fire conditions.**

*Because the sensors in a WSN work together, multiple buildings can be remotely managed, producing data that shows real-time and historical maintenance reports and service records, as well as comparisons among properties or units, floors, or departments within a property*. Some sensors only need to be placed in the desired locations and activated. Many applications allow further monitoring or interaction opportunities. Surveillance cameras, enabled with computer vision, capture images that can be analyzed for additional insights, allowing for loss prevention and reduction and ensuring continuous climate control, controlled power consumption and compliance with building codes.

**Supply Chain Management**

Supply chain management involves the risk of not only product, service, or shipment disruptions caused by unforeseen events but also the downstream effects that interruptions cause to other products, services, or shipments. Risk assessment, which involves identifying potential or actual disruptions, and risk control which involves preventing or reducing disruptions, use many emerging technologies to manage supply chain risks.

*Radio frequency identification (RFID), which uses radio frequency to identify objects, wireless protocols, and the Global Positioning System (GPS), is particularly important to managing supply chain risks*. Supply chain assets were previously tracked using standard bar codes, which must be in close proximity to a reader. In contrast**, RFID tags identify assets and compile their characteristics without human intervention**.

*RFID technology is wireless, supports and automated process, does not require the reader to be in close proximity to the asset, and provides specific information on each asset to facilitate logistics and transport. This technology, especially when used with GPS for additional location tracking, enables a mixed shipment of freight to be identified and tracked without the need to remove any external wrapping*. Furthermore, each item of freight can be easily cataloged by the reader according to description and condition, manufacture and expiration dates, arrival location and time, and relationship to current inventory. When a shipment is incomplete or damaged, RFID technology can be used to assess the risk, automatically call for replacements, and manage the replacement process.

Additionally, *RFID tags provide unique identifiers, which offer real-time, accurate storage and retrieval in a closed-loop system*. With this readily available, detailed data on supply chain assets, companies can immediately identify discrepancies and interruptions and quickly prevent and reduce supply chain risk. RFID process – automation capability can generate real-time alerts for those who need to receive the information and oversee remediation.

Other kinds of sensors can empower more precise supply chain management. *Sensor data can inform a supply chain manager that weather conditions have interrupted the production of parts or that cargo has been stolen*.

**Transportation Management**

*Transportation management that facilitates risk assessment and control involves incorporating technology from the Internet of Things (IoT) to connect vehicles and their drivers with solutions for awareness, safety, efficiency, and reliability*. These same technologies also help organizations manage their vehicle fleets.

Some of these technologies even provide driver assistance. Example; crash avoidance, self-parking; cameras on the back of trucks, and some cases, full autonomous driving capabilities.

Smart transportation is also key to transportation management. As with many smart operations in a variety of contexts, it can be described as a series of layers.

* *A sensing layer* – uses a variety of sensors, cameras, and data collection
* *A communications layer* – transmits to and from drivers and managers using wireless protocols that ensure necessary capabilities, recording, data uploading, navigating, video recording for both sensing layer and the service layer
* *A service layer*, which uses data processing, cloud computing, and storage analysis of large amount of the data captured by the vehicle sensors and provided by drivers.

The results of this interaction among layers are improved remote diagnostics, prompt driver response from real-time analysis of his or her driving habits or physical condition, fuel and/or vehicle repair savings because of implemented corrections, preventative maintenance alerts before a costly mechanical breakdown, and customizable products and services (such as comparisons of nearby hotels and restaurants) to make rides easier for drivers and more enjoyable for passengers.

These advancements are also attributable to the photos, images, diagnostics, trip logs, and other vase amounts of data and statistics created by the sensing layer, analyzed by the service layer, and supported by the communication layer. The resulting data is, in turn, used to monitor performance and further refine the process.

Accelerometers, devises that measure acceleration, motion, and tilt, are combined with special software to detect and measure linear motion. Through telematics, accelerometer technology can generate information about vehicle fleets, such as operator acceleration and braking. It can also be used for many other applications, such as to detect excessive vibration in an industrial machine that is about to explode,

Augmented reality technology can integrate a digital experience into a user’s physical environment. One example, head-up displays in or near aircraft and car windshields, reduces distractions for pilots and drivers by displaying information, such as speed warnings and warning signals, within their lines of sight.

**Catastrophe Management**

Sensors and WSNs are also used in catastrophe management. As long as a sensor can withstand a harsh environment, it can continuously monitor an area for light, temperature, specific gases, and more. Alternatively, a sensor or WSN can measure local changes when a catastrophe is predicted or has occurred.

An accelerometer can continuously monitor earth movements in earthquakes, underwater sensors can measure water weight and help determine tsunamis, gas sensors, thermal sensors, and anemometers can warn of approaching fires.

Lidar (a sensor similar to radar that uses infrared light to detect nearby objects) is a technology used to, among other things, improve the performance and accuracy of autonomous vehicles. It can work with optical sensors, such as high-definition cameras, to detect images, even through shadows or blind sunshine. Lidar has applications to catastrophe management both before and after a natural disaster.

* It improves images even under inadequate lighting conditions because of cloudiness, intense sunshine, or shadows. It is high-definition three-dimensional mapping.
* It can capture and produce accurate elevation data, enhancing mapping flood prone areas,
* Lidar images after a flood, and the additional data it collects on air pressure, temperature, wind turbulence, and location provide information that assists in rescue and remediation.
* Lidar can help determine the optimal location for emergency communications equipment after a disaster disrupts cell or internet service. Locations for placing Wi-fi terminals, can provide street-by-street or even structure-by-structure analysis of location with the highest risk, helping rescue and remediation resources be deployed efficiently.

**Workplace Safety Management**

Many smart products ultimately may be used to improve workplace safety and productivity:

* Wearables allow workers to wear sensors in comfort and familiar ways (vests, boots) and still have hands free to do their jobs
* Drones provide information and help assess and control risk by going into unknown and potentially dangerous areas. This can be done from the ground, air, or under water.
* Robots – no longer clunky, human like machines, operate in close proximity to workers but do more of the repetitive and heavy lifting jobs. This allows workers to better use their skills and for human and machines to be better integrated in the workplace.

**Construction and Engineering Management**

Mechanical sensors detect and measure a physical quantity and produce a signal that is readable by the user on another device. They are generally used with machinery and have many applications in construction and engineering:

* Motion sensors have many applications, including surveillance and security
* Pressure sensors are similar to strain sensors, which convert pressure or tension into a measurement of electrical resistance.
* Current sensors protecting electronic systems and batteries from heat buildup
* Position sensors are used when components are to be activated only when they are in the optimal places for a particular process to continue. Car wash machinery that senses the size of vehicles and adapts the cleaning process accordingly.
* Proximity sensors, slightly different from position sensors, respond when an object reaches a threshold area within range of the sensor.
* An inertial measurement (IMU) tracks an object’s position using accelerometers and gyroscopes. IMUs are used in navigation systems, as in fitness trackers and gaming systems. Also, key sensors for autonomous vehicles.

**6 – Business Continuity Planning**

**Objective**: Explain how risk mitigation is achieved through business continuity planning

An organization can develop a detailed plan of action to mitigate risk and maintain operations regardless of external and internal events that could otherwise prove disastrous.

Over half of all business subjected to a catastrophic event fail immediately. Of those businesses that survive a catastrophe, half fail within 2 years. While government agencies may not fail immediately, a catastrophe could result in the reassessment of their effectiveness and mission, ca change of leadership, or reorganization, leading to further disruption.

The development of a business continuity plan (BCP) is an important component of business continuity management (BCM). **A BCP allows an organization to analyze all possible eventualities to determine the critical functions that must continue during a disruption so that the organization survives, recovers, and resumes growth.** The development and implementation of BCP entails 7 steps.

**Understanding the Business**

To complete a business continuity plan, an organization must first understand all aspects of its business. This includes determining key objectives and how they will be met, as well as the internal and external parties involved in achieving them.

If the key is to continue to manufacture widgets. It must examine how it uses its facilities, materials supply chain, human resources, communications, information systems, processes, distribution channels, and customers to achieve them. This allows the organization to identify the key processes that will constitute the basis for its Business Impact Analysis (BIA).

**Conducting a Business Impact Analysis (BIA)**

An organization conducts a BIA to identify and assess the risks that may affect it. **A BIA assesses what events may occur, when they may occur, and how they could affect achievement of key objectives. The BIA also measures the financial and nonfinancial effect of risk and explores organizational vulnerabilities, critical elements in developing strategies to protect organizational resources.**

**The analysis also distinguishes between critical and noncritical process. This allows the organization to use the BIA to determine its recovery time objective, which is the time period within which a critical process must be recovered in order for the organization to resume its operations after a disruption of operations**.

Various international standards, such as ISO 3000:2009, take different approaches or use different terminology for the BIA. In some standards, the BIA and risk assessment are combined. In other standards, the BIA goes beyond a more traditional risk assessment, which often focuses only on hazard risks and fails to assess the full impact of all risk on all aspects of the operation.

**Performing a Risk Assessment**

*An organization performs a risk assessment to identify and evaluate potential exposures and the probability that certain events will occur*. It also indicates how susceptible the organization may be to particular disruption. This helps the organization prioritize its BCM strategy and risk controls and assists management in making decisions regarding organizational risk appetite. *A thorough risk assessment will reveal exposures and can assist in establishing methods for future risk mitigation efforts. Finally, the risk assessment helps the organization determine an action plan*.

Assessments can be conducted at various levels.

* Enterprise assessment – global assessment of risks that could affect the enterprise’s overall business goals
* Site assessment – an assessment by risk owners at risk centers of risks associated with particular sites or locations or even specific geographies
* Program or project assessments – assessment of a project’s capabilities, resources, and limitation in relationship to viable recovery strategy

**Develop the Continuity Plan**

After it has conducted the BIA and performed a risk assessment to establish recovery time objectives, an organization can begin to develop strategies to maintain critical functions during disruptions. **Organizations may use one strategy or a combination of strategies to ensure resiliency:**

* **Active backup model – establish a second site that includes all of the necessary production equipment housed at the primary site. Staff may be relocated to the second sit if operations are disrupted at the primary site.**
* **Split operations model – maintain two or more active sites that are geographically dispersed. Capacity at each site is sufficient to handle total output in the event of disruption at either site.**
* **Alternative site model – maintain a production site and an active backup site that functions as the primary site as needed.**
* **Contingency model – developing an alternate way to maintain production, perhaps suing manual processes**.

All of theses strategies involve 3 levels of planning

* BCM Organizational strategy
* BCM Process level strategy
* BCM Resource recovery strategy

These planning levels require the organization to examine its basic processes, determine potential points of failure, and create alternate operational methods.

Strategic choices for addressing a disruption of operations include these options:

* An insurance policy – to recover some of its financial losses if it suffers an insurable loss
* Transfer processing – entering into reciprocal arrangements with another company or division to perform a necessary function in the event of a disruption of operations.
* Termination – cease production of the affected product or service
* Loss mitigation – implementation of risk controls and plans to reduce, minimize, or divert any loss
* Do nothing – if an organization does nothing in the event of a disruption of operations, it absorbs the potential loss. This represents an increase of risk appetite.

**Implementing the Continuity Plan**

Senior management must impress upon the organization that the BCP is integral to its survival and success. The business continuity coordinator (BCC) assists and directs each department in formulating a departmental plan. This ensures that the organization’s component parts work effectively for the entire organization.

Each departments plan must include these elements

* Statement of acceptable level of functioning
* Recovery time objectives, resources needed, and potential failure points
* Tasks and activities required
* Procedures or processes
* Supporting documentation and information
* Structure to support the plan
* Description of division teams – purpose, team members, mission
* Explanation of interdependencies among the various division teams

The BCC presents the drafted BCP to senior management for approval. One the BCP is approved, the BCC and senior management begin to influence the organization’s culture to accept, practice and maintain BCP.

**Building a BCM/BCP Culture**

**Senior management provides the vision statement and support for the BCP. It must also set expectations and objectives for middle management concerning maintenance of departmental plans**.

Staff must be educated on the importance of maintaining the BCP. One way management can achieve this is to hold semiannual exercises in which staff members react to a hypothetical disaster scenario by using the plan to maintain operations. If successful, these exercises may fine “holes” in the BCP that need to be addressed. External suppliers and customers should know that the organization has a BCP and be encouraged to provide their own contingency plans. When key suppliers and customers are prepared for a disruption of operations, their relationship with the organization is improved.

**Maintaining and Updating the Plan**

Organizational environments, processes, and products change rapidly in today’s business environment, and so too should the BCP. A BCP is effective only if it is kept fresh and updated. The BCP should be reviewed in detail and amended as internal or external conditions warrant. Analyzing the written BCP is essential and should be done semiannually or when a significant change has occurred in product line, processes, or management. An organization must also determine how best to store its BCP.

Business continuity planning may not be effective in all cases. When an organization’s survival is threatened, strategic redeployment planning is required.