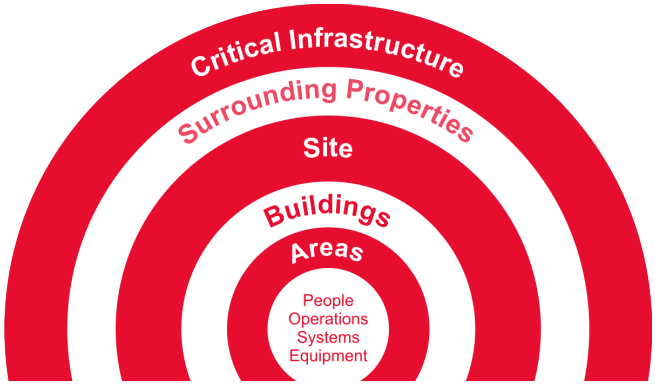
Risk Assessment

Understanding threats and hazards and their potential impacts on people, property, operations, the environment, and your image and reputation.

Original Issue: August 2014 Subscribe to Preparedness Bulletins Reissued 2017

In the aftermath of a disaster, you will see news reports with victims saying they never thought it could happen. That's human nature—we avoid thinking about the "bad" things that can happen. If we give a pass to the uninformed, then how do we explain situations where professionals responsible for taking action to manage risk didn't foresee what ultimately happened? The simple answer is that understanding risk is challenging. There are numerous areas of risk—strategic, financial, operational, and hazard-based. There are numerous "hazards" or causes and a seemingly limitless number of possible scenarios.



Understanding the vulnerabilities of infrastructure, site layout, surrounding properties, building construction, and areas within buildings that house people, critical operations, systems, and equipment is essential to understanding the potential scope and magnitude of human, property, operational, and environmental impacts.

Risks are managed by every entity in the private and public sectors. Managers make frequent decisions to accept, avoid, transfer or finance risk. Safety and security professionals build loss prevention and hazard mitigation programs. Emergency managers and business continuity practitioners build preparedness programs.

Understanding hazard and operational risks—their likelihood and potential impacts—is a prerequisite for effective risk management. Loss prevention, hazard mitigation, and preparedness programs including emergency management and business continuity must be based on an accurate and realistic understanding of potential risk. Completing a thorough risk assessment is the only way to truly understand risk.

Risk Assessment

A risk assessment seeks to identify the threats and hazards that could cause unacceptable impacts to the assets of an entity. Potential impacts are determined through analysis of the type of hazard, the location and magnitude of the hazard, and vulnerabilities that could cause or increase impacts. The risk assessment should identify:

- Threats and hazards
- Likelihood or probability of occurrence
- Assets at risk
- Vulnerabilities of the assets at risk
- Scope and magnitude of potential impacts
- Overall hazard rating

There are numerous threats and hazards to consider when conducting a risk assessment. A lengthy list can be found in Annex A of NFPA 1600, and an abbreviated list is presented on page 2.

For each type of threat or hazard, there are many possible scenarios. The magnitude of the hazard could be minimal or it could be cat-

astrophic. A tropical storm is the lowest category of tropical cyclones. A category 5 hurricane is the highest category. A small fire may be extinguished by an automatic fire suppression system, or a flammable liquids fire may overtax protection and destroy a building.

For each threat or hazard it may be difficult to estimate the likelihood or probability of occurrence. Estimating frequency is difficult because of the limited body of scientific knowledge. For many hazards, the greater the magnitude, the lower the probability that it will occur. Earthquakes are a good example—"micro" earthquakes occur every day, but catastrophic quakes are infrequent. The risk assessment should consider a range of potential magnitudes.

Scenarios should take into account the proximity of a hazard to a facility or its location within the building. If the potential location (or path) of the hazard exposes critical assets (e.g., people, high-value property, or mission-critical operations within a building), then it should receive greater scrutiny. The timing of hazard occurrence is also important for emergency planning. An earthquake occurs without warning, so preparations must be in place at all times. Conversely, hurricane forecasters now provide warning days in advance of landfall allowing for safe evacuation and facility preparation. Timing is also an important consideration for estimating operational impacts. For example, if the delivery of consumer goods to retailers prior to and during the holiday shopping season is delayed, it will have a greater impact at that time than at other times of the year.

Every entity has many assets at risk including people; facilities; property (including intellectual property and electronic information); operations and processes; the environment; and its brand, image and reputation.

The first priority of any risk assessment should be to assess threats and hazards to life safety. Potential injuries to employees, contractors working on site, and visitors from physical hazards such as fire,

List of Hazards

Natural Hazards

Geological
- Earthquake
- Tsunami
- Volcano
- Landslide, mudslide, subsidence

Meteorological
- Flood
- Snow, ice, arctic freeze
- Tropical cyclone (hurricane)
- Thunderstorm and tornado
- Wildland fire
- Lightning
- Geomagnetic storm

Biological
- Foodborne illness
- Pandemic/infectious/communicable disease

Human-Caused Hazards

Accidental
- Hazardous material spill or release
- Explosion/fire
- Entrapment and/or rescue
- Transportation accident
- Product defect or contamination

Intentional
- Strike or labor dispute
- Physical or information security breach
- Acts of violence, kidnapping, extortion, hostage-taking
- Product contamination
- Demonstrations, civil disturbance, riot
- Bomb threat, suspicious package
- Arson
- Terrorism (explosives, chemical, biological, radiological, nuclear, cyber, electromagnetic pulse)
- Geopolitical events (terrorism, war)

Technology Hazards

Information Technology
- Computer systems (hardware failure; loss of network connectivity, loss of electronic data interchange or e-commerce, loss of domain name server, denial of service; malware, virus, worm, Trojan horse; spyware, hacking; cyber terrorism, fraud; power surge; and water damage)
- Computer software or application interruption, disruption, or failure
- Loss, deletion, corruption, or theft of digital information

Utilities/Infrastructure/Equipment
- Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control, or sewage)
- Mechanical breakdown

Supply Chain
- Supply chain interruption or failure
- Transportation interruption

accidents, medical emergencies, and workplace violence should be assessed.

Assessment of potential damage to property should consider scenarios that impact critical infrastructure such as loss of voice and data telecommunications, power outages and surges, and restricted site access. Property includes electronic information and intellectual property, so the adequacy of data backups and information security should be factored into loss estimates.

A business impact analysis should be conducted to identify the minimum resources required to continue business operations at a minimally acceptable level.

Many incidents such as hazardous materials spills or release and fires result in environmental contamination. If there are quantities of hazardous materials on site that exceed regulation defined threshold quantities, a risk assessment and emergency planning is required.

There are many weaknesses or vulnerabilities in the siting (location) and construction of buildings and supporting infrastructure that make them susceptible to multiple hazards. There are many points of failure in process systems, voice and data telecommunications systems, computer networks, computer operating systems and applications, and the equipment that is needed to manufacture products and provide services.

The risk assessment is an excellent opportunity to identify vulnerabilities or weaknesses, which can be exploited by hazards to cause impacts. Strategies to prevent a hazard or mitigate the potential impacts from a hazard should be identified during the risk assessment.

After the assessment of vulnerabilities, the next phase is to analyze and estimate potential impacts on people, property, operations, the environment, and the entity.

Objective criteria for rating impacts should be decided in advance, so there is consistency in all ratings. Example criteria for impacts to people could include: "low" impact: an injury requiring only first aid treatment; "moderate" impact: lost-time injury; and "high" impact: a life-threatening injury or fatality. If a five-level rating system is used, the criteria would be expanded.

Each scenario should be assigned an overall hazard rating. The rating should be a combination of the likelihood the hazard scenario will occur and the potential impacts that may result. There are many methodologies for rating impacts.

Scope & Methodology

Begin the risk assessment process by engaging staff that have institutional knowledge of your facilities and operations. Solicit the participation to ensure you have the expertise to evaluate all hazards. Internal risk experts to call upon include those from risk management, environmental, health & safety, physical and operational security, human resources, facilities management, engineering, manufacturing management, information technology, and others. Risk experts

Methodology

1. Assemble the required expertise into a working group.
2. Agree upon scope, methodology, and deliverables.
3. Gather information, survey facilities, interview people, conduct research, and compile scenarios with estimated probabilities and potential impacts.
4. Sort and group results to highlight the scenarios with the highest overall hazard rating.
5. Validate scenarios, probabilities, and potential impacts with the working group.
6. Present the completed risk assessment to senior management along with recommendations for loss prevention; hazard mitigation; and risk avoidance, retention, transfer, and or financing.
7. Evaluate emergency management, business continuity and crisis communications plans to determine whether they adequately address the identified scenarios and potential impacts.
8. Take agreed upon action on recommendations.
9. Monitor hazards periodically and adjust prevention, mitigation, and preparedness capabilities as necessary.

Asset at Risk	Hazard Scenario (Hazard, Magnitude, Location, Warning Time)	Likelihood of Occurrence	Vulnerabilities (to be addressed by Prevention/Mitigation)	Estimated Impacts					Overall Rating[2]
				People	Property	Operations	Environment	Entity[1]	
Main Building	Forecast Category 3 hurricane tracking within 50 mi.	M	■ Roof covering improperly adhered; flashing in disrepair; large amount of exterior glass ■ Lack of drainage for ground surface water ■ Limited site access ■ Single power feed; no backup	L	H	H	L	M	MH
Data Center	Contractor damages voice and data connections while excavating at the property line; extended period of connectivity interruption; gas leak involved	L	■ Single connection to internet service provider ■ Daily incremental and weekly full backup to tapes stored on-site ■ Incoming utilities exposed and unprotected; no contractor safety or management of change programs	L	L	H	L	M	LH
Employees and visitors	Terminated employee enters lobby and shoots receptionist; proceeds into the building shooting numerous people	L	■ Lack of physical and operational security to prevent unauthorized access ■ Inadequate security policies and procedures ■ No lockdown protective action or training; limited ability to broadcast warnings	H	L	M	L	M	LH
Employees, customer, and visitors	Numerous customers and employees sickened following an outdoor reception on a hot summer afternoon	M	■ Lack of vetting of caterer's food safety and security program; no special event planning ■ Inadequate supervision of food ■ Lack of refrigeration of food during the special event	H	L	M	L	M	HM

[1] "Entity" includes brand, image, reputation, finances, etc.

[2] Overall Rating is a combination of likelihood of occurrence and highest estimated impact. If numerical ratings are used for likelihood and impacts, then the overall rating could be calculated by multiplying the likelihood of occurrence by the sum of the five categories of impacts.

may also be found within other divisions or facilities of your organization.

Seek out external expertise from property and casualty insurance company loss prevention staff, industry trade groups, and public safety agencies (fire departments and law enforcement). If necessary seek out the guidance of recognized external experts that can provide insight into hazards and potential impacts that are not well understood.

Organize participating experts into a working group to define the scope and methodology of the risk assessment process.

The scope of the risk assessment should be defined at the outset. All risk assessments should consider all hazards as specified in our national preparedness standard, NFPA 1600. A top priority for the risk assessment is to identify threats and hazards that could cause significant injury to, or death of, employees, contractors, and visitors.

The scope should incorporate regulatory required assessments including occupational safety and health, environmental, process safety, information security, and others. Process hazard analyses in high hazard industries and job hazard analyses for specific processes or equipment are examples.

The working group will be faced with a decision about the depth of the analysis of specific scenarios. Assuming regulatory requirements have been satisfied, the depth of analysis should be sufficient to provide information for emergency management and business continuity planning. Analyses should also provide sufficient information for management to make decisions to accept, avoid, or transfer risk and how much to invest in loss prevention and mitigation strategies.

Multi-facility entities can benefit from identifying and assessing scenarios that could impact multiple facilities that are in geographic

proximity or exposed to a common hazard. Dependencies and interdependencies between company facilities should be identified, and the operational impacts resulting from downtime at one facility on other facilities calculated. Identify and assess potential impacts resulting from the interruption or disruption of critical infrastructure and the supply chain.

Once the risk assessment scope and methodology have been established, gather and review documents such as the following that may provide insight into past incidents. Review analyses that identify possible loss scenarios.

- OSHA logs, first aid logs, first reports of injury
- Worker's compensation, general liability, and property loss runs
- Insurer loss prevention reports
- Process hazard analyses
- Job hazard analyses
- Environmental risk assessment
- Information security assessments
- Internal audit reports

Working group members should be asked to provide the details of threats, hazards, scenarios, vulnerabilities, and potential impacts. After existing information has been compiled, ask working group members to review it. With sufficient advance preparation, a facilitated workshop is an excellent means to identify and attempt to quantify the most significant areas of risk. Priorities should quickly emerge, and areas for further studies can be identified.

About Preparedness, LLC

Preparedness, LLC is a client-focused risk consulting company. Our mission is to safeguard people, protect property, minimize business interruption, and protect an entity's image and reputation. Our vision is to thoroughly understand each client's business and become a long-term, trusted advisor.

If you have questions, or need assistance with the development, implementation, or evaluation of your preparedness program, please contact us.

Additional Resources

Links to numerous documents on the subjects of loss prevention, hazard mitigation, emergency response, and business continuity can be found on the "Resources" page of the Preparedness, LLC website. Check out the program self-assessment checklist based on NFPA 1600.

Subscribe to Preparedness Bulletins

Click here and sign up for our Preparedness Bulletins. You can unsubscribe at any time.

PREPAREDNESS, LLC

643 MASSAPOAG AVE, SHARON, MA 02067

(781) 784-0672

INFO@PREPAREDNESSLLC.COM • WWW.PREPAREDNESSLLC.COM

PREPAREDNESS