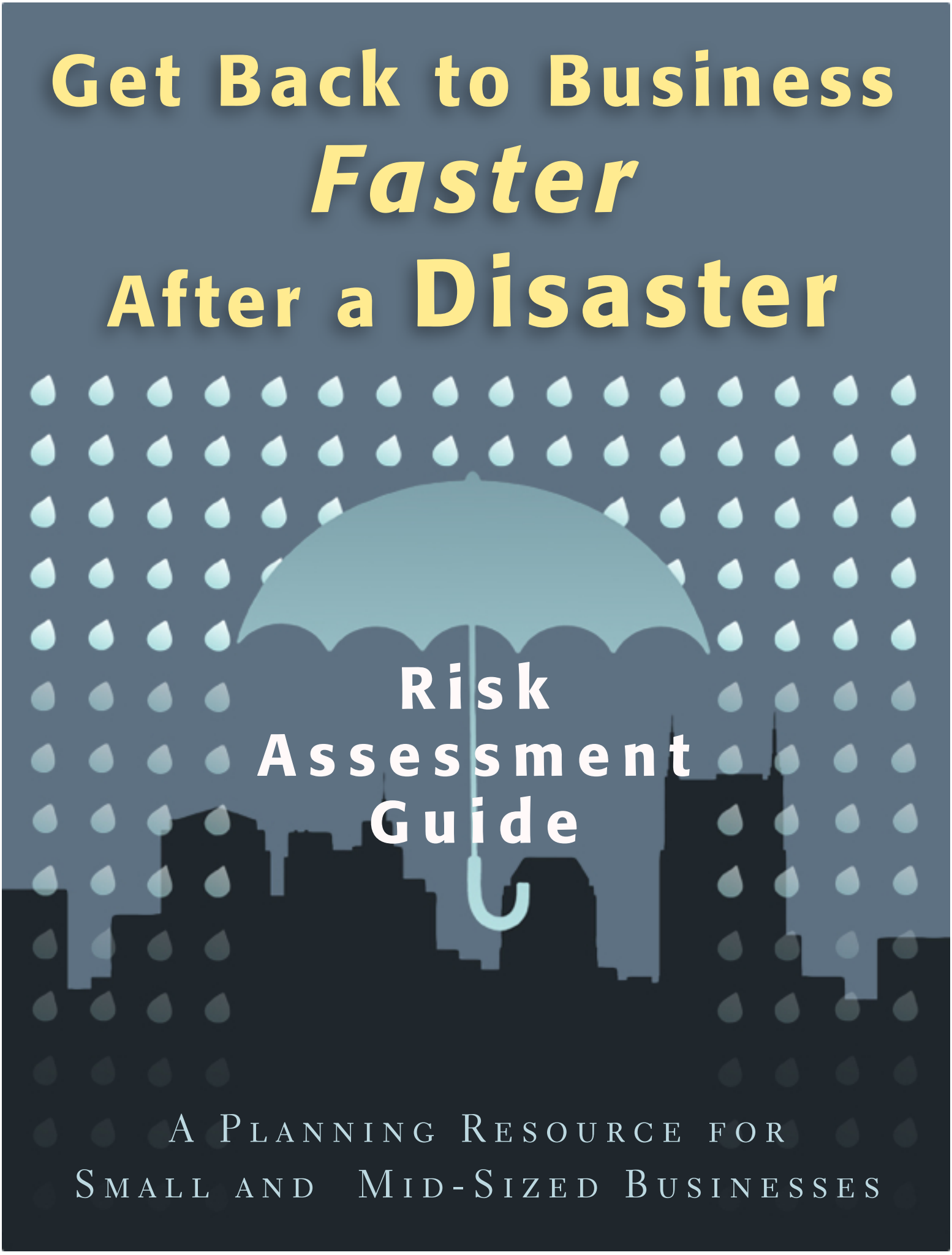
Get Back to Business *Faster* After a Disaster



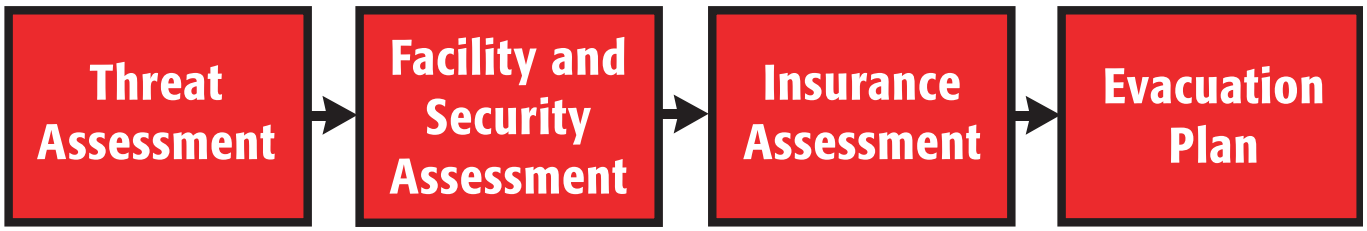
Risk Assessment Guide

A Planning Resource for Small and Mid-Sized Businesses

Understanding My Risks

"What kind of disaster should my business be ready for?"

After you've set the foundation for your Business Continuity Plan (BCP) by performing tasks like obtaining management sponsorship and assigning roles and responsibilities, your next step on the road to a BCP is to understand your company's risks. In this guide we'll walk you through a four-step risk assessment process, providing practical tools and templates for each important step.



Understanding My Risks

Step 1: Threat Assessment

Start your risk analysis process by performing a vulnerability/hazard assessment. During this step, you'll gather information about possible threats and emergencies that could impact your business and determining its ability to respond to and recover from a crisis.

Remember to assess both internal and external threats that can adversely affect your business and its people, data, facilities, and reputation with disruption as well as disaster.

Use our threat analysis template to prioritize a list of possible threats to identify which ones your plan must address.

Threat Assessment Template

Click to access the Threat Assessment Template

These four steps will walk you through using the template so that you can get the most out of it.

1. Identify risks using the risk analysis template.

- Start with the first threat – tornadoes– and determine the likelihood that a tornado could impact your business.
- Rank threats as low, medium, or high in light of the suggested guidelines.
- As you assess the threats, focus on probability, rather than severity. You may find it helpful to gather this information using some of the websites we suggested before completing the template. When you're gathering information, keep in mind relevant regulatory and/or legislative issues.

- If this exercise is being completed by a team, each participant may have a different opinion on the breadth and probability. Consider choosing a methodology for reaching consensus. (For example, you might decide to use the ranking the majority chose.)
- Work either across or down the list to complete the various cells. Sums will be automatically calculated in the "Priority" column.

2. Once risks are identified, outline your core business functions.

Now, think through the various activities, tasks, processes and systems that are most important to your business. We refer to them as "critical business functions." Your critical functions are those activities that are vital to your organization's survival; while these functions are essential to your business, they often seem to be the most challenging to define. Identifying critical business functions is essential in helping your company recover quickly.

3. Assess the risks that threaten your critical business functions.

With the top threats identified, discussed and documented, address these concerns:

- Determine your company's exposure to such an event. For instance, a tornado could result in loss of power, hard-to-replace equipment damaged, difficulty communicating with employees and the necessity to resume operations at an alternate location.
- Identify worst-case scenarios.
- Identify which functions and people are essential in each scenario.
- Be sure to keep in mind cascading events (i.e., a tornado could affect your production and your key suppliers)
- Identify controls and safeguards your plans need to prevent or minimize the effect of the impact. Things to consider:
    - Physical protection.
    - Physical presence and security by employees or police.
    - The role your business may play in the surrounding community.
    - Information security.

- Identify resources for gathering other helpful information for your plan. This may include collecting information across business divisions and organizational locations (questionnaires, interviews, documentation review).
- Evaluate how these risks and exposures will impact essential areas that keep your business operational. These factors include:
    - Availability of personnel.
    - Availability of information technology.
    - Status of infrastructure (i.e., transportation, access to building).
- Consider what controls and changes should be put in place to reduce impact due to risks and exposures.

4. Prioritize these threats to your critical business functions.

The goal of this step is to identify three or four threats that will lead to scenarios your plan will address. You may choose the top three or four top threats (those that have "high" priority) to be the scenarios your BCP plan will address. Or, you might select a combination of three or four threats that represent different types of challenges for your business. Regardless, include one scenario that is a "catastrophic threat." A catastrophic threat scenario is one where your building is uninhabitable, you must establish an alternate location, and systems have been destroyed or incapacitated for an extended period of time.

What will you do with this information?

1. Establish disaster scenarios based on threats that pose the highest risk to your business. Consider basing scenarios on these types of criteria: a) severity in magnitude; b) occurring at the worst possible time; resulting in severe impairment to your organization's ability to conduct business.
2. Develop preventive and pre-planning options by considering:
    - Cost vs. benefit
    - Implementation priority
3. Confirm with management to determine acceptable risk levels. Generally, this involves one of the following strategies:

- Accept the risk (do nothing)
- Risk avoidance (through preparation and mitigation)
- Transfer of risk (through insurance, third-party involvement)

We put together these sample disaster scenarios to guide you as you begin creating your own. You might even consider adapting these to fit your specific needs.

Click to access Sample Disaster Scenarios

Understanding My Risks

Step 2: Good Housekeeping – Perform a Facility and Security Assessment

Now that you've identified and prioritized threats to your business, it's important for your team to assess your facility's proximity to potential hazards and security concerns. Then, use that information to establish the likelihood of different disasters and crises occurring.

Call it your "good housekeeping" practice as your team prepares to build the plan. In this section, we'll focus on minimizing potential hazards that your organization can control related to your facility and security.

There are two important steps to take in order to prevent or minimize the impact of a crisis.

1) Conduct a facility assessment and area review

2) Conduct a security assessment

1. Facility Assessment and Area Review

Use the following steps as a guide for assessing hazards within your facility and area.

Consider your facility's proximity to potential hazards when thinking about the likelihood of different disasters occurring, such as:

- Flood plains
- Major transportation routes and airports
- Proximity to other larger facilities
- Limited access and egress routes for employees
- Companies that produce, store, use or transport hazardous materials

Take time to understand your neighbor's business and the impact it may have on your business. If you are in a multi-story building, visit the firms above you. Ask a representative of a remediation services company how often they've been called to pump water from a business closed down from a water leak from a client above. Analyze the firm's location and proximity to water bodies, gas stations, hazardous materials, and single point of access roads.

Consider traffic and its flow too. Are hazardous materials container trucks passing your building regularly? Could one road closure preclude access to your building? Assess these issues and document them in your plan. If you're leasing/renting, discuss concerns with the landlord. If you own your facility, discuss your concerns with local officials.

Find out about any emergencies that occurred at your facility in the past.

Gather information about other potential hazards related to:

- Human error
- Safety system failure
- Fire, explosions, hazardous material spills
- Telecommunication
- Computer system failures
- Power failure (including heating/cooling system malfunction affecting your data center)

Assess the physical capacity, supplies, equipment and human resources of your facility to resist damage during a disaster. What types of emergencies could result from the design or construction of the facility? Consider:

- Hazardous processes or byproducts
- Facility's physical construction and location
- Layout of equipment
- Facilities for storing combustibles

- Lighting
- Evacuation routes and exits
- Shelter in place
- Protection of critical and hard-to-replace assets

2. Security Assessment

Consult the facility manager or individual charged with security to review your **facility and security assessment**. Consider reviewing the physical accesses to your facility.

- Review physical access controls to ensure they're adequate. Don't confuse convenience with protection.
- Walk around the facility. Are doors open (unchallenged access) that should be closed and locked at all times? Are sign-in procedures for visitors being followed?
- Observe if work areas containing sensitive information or special technology are protected; this is critical if maintaining physical security is important to be in compliance in your industry. Is there a fire-suppression system – ideally not a water sprinkler - where file servers and communications equipment are housed?

Tips

1. Print the facility and security assessment linked below and do a walkthrough of your facility.
2. Examine findings and incorporate strategies to minimize your risks and vulnerabilities

Facility and Security Assessment

Click to here for a Sample Facility and Security Assessment

Understanding My Risks

Step 3: Insurance Assessment

In this section of the workbook, we'll focus on insurance:

- We'll think through your insurance needs to make informed decisions around adequacy of controls you have in place.
- We'll introduce you to various types of insurance and riders available to you that may be important before and after a business interruption.

Most business owners have an overly optimistic understanding of their insurance policy. They often see it as the vehicle that will help get financial resources and in turn, other critical resources to get their business back up and running should disaster hit.

Most insurance policies cover some or all of what was lost. They'll help you get your doors open but won't usually provide enough to recover your business. You most likely won't recover the business income that was lost while your doors were closed or the additional production costs you'll incur to make up for the interruption in operations.

That's why it's important to assess the adequacy of your insurance cover to get your doors re-opened *and* to get your business back up and running. To do this you might consider adding a "business interruption insurance rider" to your property or casualty policy

Getting back up and running as fast as possible is at the heart of the recovery phase – and your company's survival. So before a disaster strikes, review the company's insurance policies.

Generally, for each area of risk, your business will respond in one of the following three ways:

- **Risk Avoidance** – The business takes action to reduce or eliminate the risk.
- **Risk Transfer** – The business reduces the reduction of the financial damages by assigning the risk to an insurance company or other party.

- **Risk Acceptance** – To the extent that it's not practical or possible to avoid or transfer a risk, the business accepts the risk.

Before floodwaters or a tornado send you searching for a copy of your insurance, we strongly suggest conducting an insurance review.

An Insurance Review Questionnaire

Review your insurance needs and existing policy, asking these questions:

1. Are coverage limits and deductibles appropriate?
2. For what types of disasters (events) am I covered?
3. What events are specifically excluded?
4. Does the insurance provide adequate protection to senior management against litigation resulting from insufficient business continuity planning?
5. Does coverage contemplate inflation, improvements, and building code changes?
6. Is coverage for "replacement cost" or "actual value" (cost less depreciation)?
7. Does business interruption insurance cover loss of income and payroll expenses?
8. Is documentation (serial number, date of purchase, cost, receipts, photographs, etc.) current and sufficiently detailed for my insurance company?
9. Is the original of all insurance policies readily accessible (digitized, secured in a fireproof cabinet, and located off-site)?
10. Does coverage include loss from an interruption of power or other critical services?
11. Does coverage include loss from a denial of access order issued by civil authorities?
12. Does my insurance cover losses incurred as a result of a disruption of transportation services?
13. If a "disaster declaration" is made by executive management:

a. Does my insurance cover the costs charged by my alternate site vendor?

b. Does my insurance cover all the extra personnel and other costs associated with activating and operating the alternate site?

14. Is there sufficient life insurance coverage for key executives?

15. Has coverage been reviewed with a professional insurance advisor during the past year?

16. If an effective BCP is implemented, will my insurance premiums go down?

Understanding the Basics of Insurance in the Event of a Business Interruption

Business Interruption Insurance

Business interruption insurance (BII) is insurance coverage that replaces business income lost and pays for additional production costs as a result of an event that interrupts business operations, such as fire or a natural disaster. BII is not sold as a separate policy, but is either added to a property/casualty policy or included in a comprehensive package policy. This type of policy pays out only if the cause of the business income loss is covered in the underlying property/casualty policy. The amount payable is usually based on past financial records of the business or calculated estimates.

General risks covered by BII:

- Fire
- Tornado
- Hurricane
- Property loss (if your property policy has the risk included)

General risks generally NOT covered by BII:

- Server outages
- Terrorist activity

- Flood
- Earthquakes
- Network/data breaches
- Pandemic situations

Typical expenses covered by BII:

- Payroll
- Recovery facility charges
- Recovery services (e.g. SunGard, RentSys, RES-Q)
    - BII will not cover your subscription fees
- Recovery equipment fees
- Travel, hotel, food, and incidentals for personnel to go to a recovery location
- Extra consultants to assist in recovery
- Grief counselors, reputation recovery, legal costs
- Increased supply costs at recovery locations

Additional Riders for Business Interruption Coverage Include:

Extra Expense Insurance

Extra expense insurance reimburses your company for a reasonable sum of money that it spends, over and above normal operating expenses, to avoid having to shut down during the restoration period. Usually, extra expenses will be paid if they help to decrease business interruption costs.

Business Income Insurance

Business income insurance compensates your company for lost income if you have to vacate the premises due to disaster-related damage that's covered under your property insurance policy,

such as a fire. It covers profits you would have earned, based on your financial records, had the disaster not occurred. The policy also covers operating expenses, like electricity, that continue even though business activities have halted temporarily. This type of coverage affords protection in the event of damage to the insured's premises.

Contingent Business Interruption Insurance

Contingent business interruption insurance reimburses your company when you have to suspend operations as a result of a covered physical loss or damage to property of your suppliers and/or customers. This is typically a supply line issue.

Service Interruption Insurance

Service interruption insurance provides coverage for disruptions caused by interruptions in the supply of water, communications or power. Overhead transmission facilities are usually excluded, but can be added back in by endorsement, which is recommended for many companies.

All of the above insurance products are generally provided by a rider or endorsement to a commercial property insurance policy. These business interruption products usually will not cover losses from weather-related evacuations, loss of electricity, or utilities not directly resulting from damage to your property. These are written on separate policies. Most commercial property policies exclude flood coverage in Middle Tennessee. These can be written by endorsement or on separate policies.

Tips:

- Don't count on your standard insurance policy for recovering your business. It will help you open your doors, but won't help you get back in business.
- Understand what your policy does and does not cover. Also understand the exact dollar amount of the coverage and the length of time it will pay.
- Don't rely on your insurance adjuster to interpret your policy or your business loss and needs.
- Following a disaster, timing is critical in terms of loss of income. An extra expense policy can pay for additional workers, such as a disaster recovery specialist, and materials (e.g., technology workarounds) that help you manage the loss and get back on your feet fast.

- Prepare a disaster fund budget that takes into account all your anticipated expenses across the timeline of a post-disaster cycle: response, recovery, and resumption.
- Identify hazards that your organization is exposed to with the assistance of a risk management professional.

Understanding My Risks

Step 4: Creating an Evacuation Plan

During some emergencies, it becomes necessary to evacuate your facility. Follow these steps for emergency readiness and general procedures for evacuation. *Make sure to adapt these procedures to fit your facility and employee needs.*

- Determine the conditions under which an evacuation would be necessary.
- Establish a clear chain of command. Identify personnel with the authority to order an evacuation.
- Designate employees in key roles such as helpers to assist others in an evacuation, account for all personnel, and assist with potential security concerns.
- Create a training exercise for personnel involved in evacuation procedures.
- Establish procedures for assisting persons with disabilities or medical conditions.
- Post evacuation procedures and ensure exits and evacuation routes are clearly marked.
- Include plans for assisting guests, clients, customers and other visitors to the facility during an evacuation.
- Designate personnel who will shut down critical operations while an evacuation is under way. Make sure they receive training to recognize when to abandon the operation and evacuate themselves.
- Involve local emergency management authorities and external resources, such as police and fire departments.

Creating Your Evacuation Plan

Consider adapting this Sample Evacuation Plan to fit your company's needs and the layout of your facility.

Click to access Sample Evacuation Plan

Employee safety is your number one concern. The best approach when creating an evacuation plan is to adhere to existing OSHA requirements.

A plan is only good in an emergency if people know how to respond. Make sure an evacuation plan orientation is part of your new employee orientation. Test the plan annually, and make sure it appears in all the right places. Start by placing your evacuation plan in:

- Your company's emergency response plan
- Your company's employee manual
- Other key employee areas like the break room

Resources:

Tips from the Greater New York Region of the American Red Cross.

Evacuation Plans and Procedures eTool from the United States Department of Labor's Occupational Safety and Health Administration (OSHA).

Patmos, LLC provides services for corporate and nonprofit clients focusing on organizational resiliency. Patmos' diverse and unique set of experiences and skills – business continuity and disaster recovery planning, aligning processes and systems, and strategic planning – provide the fundamentals organizations need to survive and grow, while adapting to today's challenging and complex realities. Patmos has prepared business continuity plans for numerous financial institutions, financial services companies, manufacturing companies, nonprofits, and the Nashville Area Chamber of Commerce.