

Risk Management



The book provides an overview of Emergency Preparedness and Business Continuity for facility managers. It focuses on preparing them for their challenging role by delving into the purposes and benefits of these programs.

The competency explores principles and activities involved in developing, implementing, and evaluating plans, covering aspects like risk management and emergency response planning. Ultimately, the book highlights how these measures, when implemented together, play a crucial role in minimizing damage from incidents and fostering an efficient recovery process.



Emergency Preparedness and Business Continuity

✦ Introduction

Role of facility managers as related to *Emergency Preparedness and Business Continuity* competency

In terms of emergency preparedness and business continuity, a competent facility manager should be able to:

- Participate in and support the organization's emergency preparedness program. In some organizations, it may be the responsibility of facility management to lead this effort. This will require the following skills:
 - Develop a risk management plan to reduce the likelihood of a loss occurring or to reduce the magnitude of loss.
 - With input from functional representatives and experts, develop emergency management plans and procedures, metrics to evaluate the plans and tools to support execution of the plans.
 - In collaboration with functional representatives and experts, design and manage/oversee simulations or exercises to test emergency response and business continuity plans and use results to improve plans.
 - In collaboration with security and IT, ensure the continued security of technology systems and services and secure redundant or replacement services if necessary.
- Participate in and support the organization's business continuity program. This requires the following skill:
 - In collaboration with functional representatives and experts, develop a business continuity and disaster recovery plan that prioritizes facilities, operations and systems; defines protocols for initiating plans; and includes metrics to evaluate the program's effectiveness.

This competency introduces key terms, which are defined in Exhibit 1-39.



Exhibit 1-39: Key Terms in Emergency Preparedness and Business Continuity

Term	Definition
Business continuity	Maintenance and/or recovery of business operations during and after conditions of duress (a disaster).
Business continuity planning	Ongoing process supported by senior management and funded to ensure that (1) the impact of potential losses of operation is fully understood, (2) effective strategies are developed to continue critical processes during the emergency and to recover other business processes within defined recovery times and (3) plans are supported through testing, training of personnel and periodic review. The business continuity plan is also referred to as the continuity of operations plan (COOP) by government agencies.
Disaster recovery planning	Developing and testing plans to resume processes, restore/replace the affected site and meet the temporary and long-term needs of occupants and community. Plans also include processes for post-incident debriefing to improve prevention and preparation efforts.
Emergency planning	Process of identifying hazards and exposures; mitigating risk; developing training, policies and procedures to prevent or minimize loss during a disaster; developing procedures to guide the actions and decisions of key personnel during a disaster; rehearsing responses to ensure that the procedures are effective and roles and responsibilities are clear; and learning from incidents or near misses to correct and improve emergency preparedness.
Emergency preparedness	The state of being prepared for all types of emergencies and ready to respond to save lives and property and to support a return to normalcy as soon as possible.
Emergency management	Organized analysis, planning, decision making and assignment of resources to mitigate, prepare for, respond to and recover from the effects of all hazards, which may be natural or human-made, accidental or intentional.
Emergency response	Activities that address the short-term, direct effects of an incident. Emergency or incident response includes immediate actions to save lives and property and meet occupant needs and execution of emergency preparedness plans.
Risk management	Process of identifying and analyzing potential hazards or threats and selecting an appropriate management strategy.
Risk management strategies	Organizational responses to the possible impacts of risks. Strategies include: • Tolerance of a risk without taking further action. • Avoidance of the risk. • Prevention of a risk event. • Mitigation or reduction of the impact of a risk event. • Transfer or sharing of risk.



Overview of Emergency Preparedness and Business Continuity competency

To help prepare facility managers to fulfill this complex role, this competency focuses on emergency preparedness and business continuity programs—their purposes and benefits, principles and activities focused on developing, implementing and evaluating plans. Emergency preparedness includes the processes of risk management and emergency response planning.

Together, emergency preparedness and business continuity help decrease damage and harm from incidents and contribute to an efficient recovery.

Exhibit 1-40 provides a brief overview of the chapters and the content covered.

Exhibit 1-40: Overview of *Emergency Preparedness and Business Continuity* Competency

Chapter	Content
1. An Overview of Emergency Preparedness and Business Continuity	• Purpose and benefits of emergency preparedness and business continuity programs • Narrative of an emergency—how organizations prepare for and react to incidents • Alignment of programs with an organization's and FM's strategy • Emergency preparedness and business continuity model
2. Manage Risk	• Risk management overview • Risk identification and assessment • Identification of critical assets and processes • Risk management strategy • Managing technology risks
3. Develop Plans	• Emergency response concepts and terms • Emergency response plan components • Business continuity concepts and terms • Business continuity plans
4. Train, Test and Drill	• Training/testing strategies • Conducting drills
5. Respond, Recover and Learn	• Immediate response • Damage assessment • FM role in restoration/replacement
6. Evaluate and Revise Plans	• Annual and ad hoc review and revisions of plans • Program audits

Chapters 2 through 6 also include segments of a fictional case study of one organization's experience with emergency preparedness and business continuity.



Chapter 1: An Overview of Emergency Preparedness and Business Continuity

After completing this chapter, students will be able to:

- Describe organization and facility stakeholder needs during and after emergencies.
 - Describe how FM is involved in emergency preparedness and business continuity in organizations with different experience in these programs.
 - List benefits of emergency preparedness and business continuity to the organization and FM.
 - Trace the narrative of emergency response from planning through restoration and recovery.
 - List the principles of emergency management.
 - Describe factors that may affect alignment of emergency preparedness and business continuity programs with the organization's strategy.
 - Diagram the emergency preparedness and business continuity model, describing actions taken at each step.
-

✦ Topic 1: Purpose of Emergency Preparedness and Business Continuity

Since the beginning of the 21st century, organizations have unfortunately been reminded often about the importance of emergency preparedness. Headlines have told of devastating hurricanes, tsunamis and terrorist attacks on all continents. Gathering less attention are the more common and costly risks that facilities face every day: fires, small floods, windstorms, disruptions in utilities, loss of communication or accidents that release hazardous materials such as asbestos or environmental contaminants such as fuel oil or solvents. These events may not make headlines, but they can mean loss of use of all or part of the facility, loss of access to the facility, inability to perform essential processes related to the organization's mission and threats to the health and well-being of occupants, employees and visitors.

Estimates about the impact of disasters and incidents on businesses vary widely, but even the most conservative—the Insurance Information Institute—estimates that 25 percent of small businesses closed due to a disaster never reopen. Some may succeed in reopening but fail within a couple years.



FM understands the costs of poor emergency preparedness. A global survey conducted in 2011 by IFMA documented that FM is increasingly engaged in emergency preparedness and business continuity:

- 88 percent of the respondents felt that their organizations were better prepared.
- 92 percent had implemented emergency evacuation procedures.
- 80 percent had a crisis communication plan.
- 80 percent had a disaster recovery plan.

This trend has been encouraged by a better understanding of the costs and benefits of emergency preparedness and business continuity programs at both the FM and senior management levels. While the scope, severity and timing of an incident affect its impact and the organization's recovery, a critical factor in an organization's ability to recover from an incident is its state of preparedness for incidents and process interruptions.

Importance of emergency preparedness and business continuity to stakeholders

When an emergency or disaster occurs, an organization must act promptly to fulfill its obligations to multiple stakeholders:

- Facility occupants, whose safety must be secured and for whom an adequate workplace must be provided for resumption of business processes. An adequate workplace is safe, clean, comfortable and equipped with the resources needed to perform essential functions.
- Owners and investors, whose interests in the organization must be protected. This means securing the organization's assets—human, physical and processes—and returning the organization to full function as soon as possible. The quality of an organization's response to a crisis can also affect an organization's value. A coordinated response that preserves business operations and public image indicates a well-managed organization that can recover from crises. A poor response damages reputation and customer relations for years.
- Customers, whose own organizations may be affected by an interruption in service caused by an incident.
- Occupants' families, who must be apprised of occupants' conditions and locations and provided support for communication among themselves possible.
- Neighboring communities, which must be notified and warned about the impact of the situation on their own health and safety from the crisis through restoration.
- First responders, who must have access to the information they need to do their jobs and to secure their own health and safety.



- Local emergency management agencies, who must communicate a consistent message about an incident and ensure that the organization's and the agency's recovery objectives are aligned.
- Government agencies, which must be informed of the incident and possible impacts on services and society.
- Vendors, which must be informed of the event and how it may affect orders, invoices and potential deliveries. Vendors should be involved in a recovery plan.

FM involvement

The facility manager plays a natural role in emergency preparedness and business continuity. The facility manager:

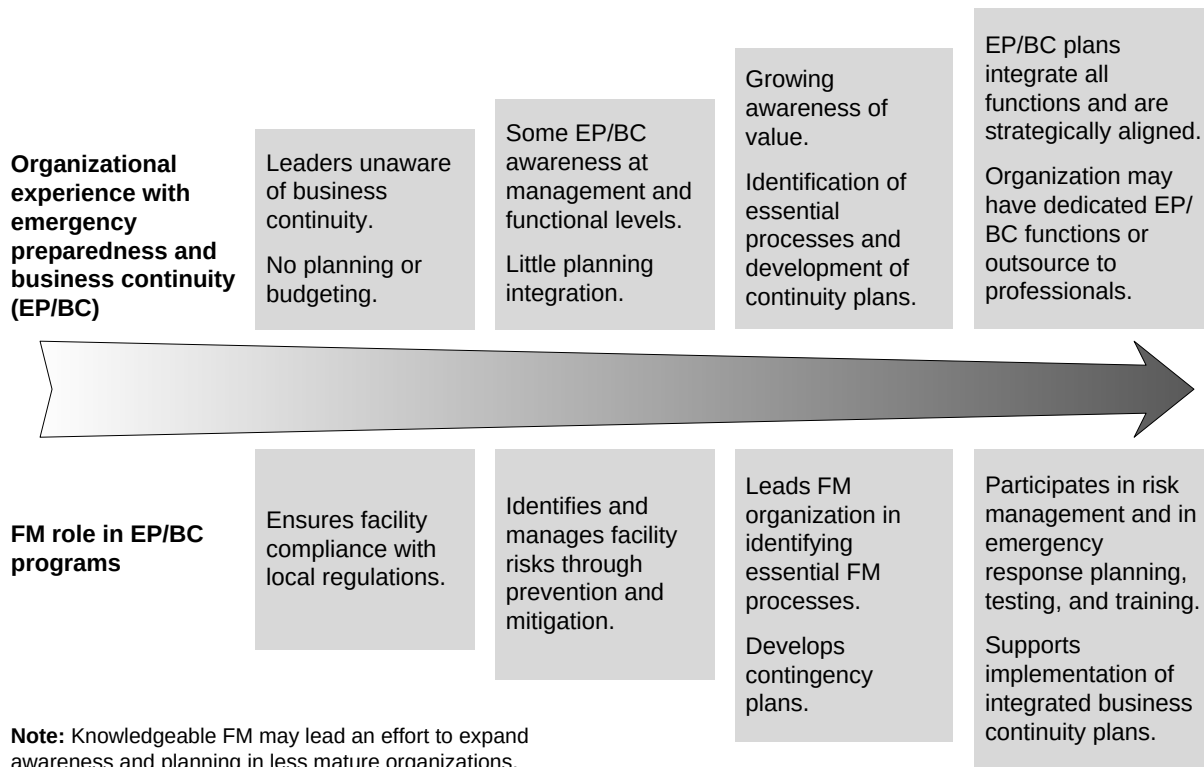
- Has an ethical and possibly a legal obligation to protect the health and safety of all facility occupants and visitors.
- Is accountable to management for facility assets.
- Is charged by the organization to provide an infrastructure to support business processes.
- Ensures appropriate testing, training and updating of all emergency response and business continuity plans and the appropriate involvement of stakeholders in exercises.
- Works with first responders (e.g., police, fire, hazardous materials teams) in the aftermath of an emergency or disaster.
- Works to minimize the impact of the event and the response on the environment.
- In many cases, directs the recovery and restoration effort in the organization's facilities.

As Exhibit 1-41 on the next page illustrates, the extent of FM's involvement in emergency preparedness and business continuity will vary, depending on a number of factors, such as size, type of business and the organization's familiarity with these programs.

As an organization matures and becomes more aware of the value of emergency preparedness and business continuity, it becomes more proactive in its efforts. Simple compliance is no longer sufficient. Increasingly, planning is less focused on what functions must do in an emergency and more focused on those processes that are necessary for the organization's survival. These processes are analyzed to understand their dependencies in functions throughout the organization. In the most aware organizations, these programs are strategic activities. The organization may have functions assigned to these tasks or may outsource their needs to professional risk or emergency managers or business continuity specialists.



Exhibit 1-41: FM Role in Emergency Preparedness and Business Continuity



FM's role changes as well. As the needs of the organization grow in number and complexity, FM's role evolves from simply ensuring the facility's compliance with local regulations to a more proactive management of facility risks. FM continues to take a leading role in emergency preparedness efforts, but now FM may also begin to apply business continuity principles at the functional level. Eventually, in strategically managed organizations that recognize the integration of their functions and processes, FM becomes part of an enterprise-level team. In this capacity, FM provides information, participates in planning and supports plan implementation.

It is critical that facility managers develop competency in this area so that they are fully prepared for whatever role they may play in their own organizations. Because of FM's essential responsibilities to occupants, management, community and the environment, FM is often involved in developing plans for or contributing components to the organization's risk management, emergency response and business continuity plans. However, in small or less mature organizations, FM may become a leader and champion of emergency preparedness and business continuity. Whatever FM's scope of involvement



may be, facility managers must be familiar with the language and principles of emergency preparedness and business continuity.

Summarizing the benefits of emergency preparedness and business continuity

Developing and implementing emergency preparedness and business continuity programs require that organizations invest time and money to varying degrees and occasionally sacrifice convenience. This investment is not for the purpose of generating income but as insurance against possible threats that will jeopardize the organization's mission, assets and people, including employees, occupants and visitors. In the 2011 IFMA survey cited earlier, a majority of responding facility managers admitted that finding the time, personnel and funding to support emergency preparedness and business continuity planning was a challenge in their organizations.

Facility managers may have to advocate vigorously for investment in planning, preparedness and prevention/mitigation projects. They must be able to define specific costs of emergency response and business continuity activities and justify them to management, using both economic and noneconomic benefits. These benefits could include:

- **Protection of organizational assets.** Assets (human and property, tangible and intangible) are protected from loss or damage.
- **Ability to continue mission-essential processes.** This can have obvious economic benefits. Processes that generate income can be continued. Contractual or regulatory requirements can be fulfilled. Nonprofits can honor their missions; for-profits can win customer loyalty.
- **Improved compliance with laws and regulations.** National and local governments may require documented emergency response plans. Organizations, particularly those that are publicly held, may be required to have business continuity plans. A risk analysis and strategy is the first step toward meeting these requirements. Improved compliance can mean a better reputation with regulators, stronger relationships with governments and agencies and avoidance of fines and penalties.
- **Lower insurance rates.** A vigilant, resilient organization will minimize its losses, which will help control insurance premiums.
- **Increased stakeholder satisfaction.** Customers who rely on the organization's products or services will feel more secure knowing that the organization has risk management and business continuity plans in place. Employees and occupants have more confidence in an employer's/landlord's



ability to provide safety and security when emergency preparedness and business continuity programs are in place and tested regularly.

- **Better communication and teamwork.** Creating these plans requires cross-functional collaboration. As a result, functions gain a deeper understanding of each other's perspectives and challenges.
- **Increased efficiency.** During the process of analyzing business processes, organizations often discover redundant processes being performed by different groups or redundant resources that could be shared by different functions rather than designated for the use of one function only.
- **Fostering of a proactive orientation.** This can help the organization focus on strategic plans rather than simply reacting to current crises.
- **Decreased vulnerability to litigation.** This protects the organization's financial assets.

FM should be aware of another, more subtle benefit of emergency preparedness and business continuity programs. The final stage in the change management process is to make the change part of the organization's culture—to institutionalize it in some manner. Once an organization commits to the goals of emergency preparedness and business continuity, it begins to assimilate these changes into its culture. Values and priorities are recognized, responsibilities are assigned, and specific processes, such as drills and new hire/occupant training in emergency preparedness, become part of the organization's standard procedures. Considering possible effects of decisions on emergency preparedness and business continuity becomes part of the decision-making process, a habitual perspective, a basic management discipline and a part of the organization's character.

In this way, emergency preparedness and business continuity become more than a way for the organization to handle identified risks. The organization can now rise to the challenge of responding to unplanned events because it has become more robust and resilient.

✦ Topic 2: The Narrative of an Emergency

Emergency preparedness and business continuity set the stage for the full narrative of how an emergency unfolds and how an organization responds to the incident and manages its recovery.

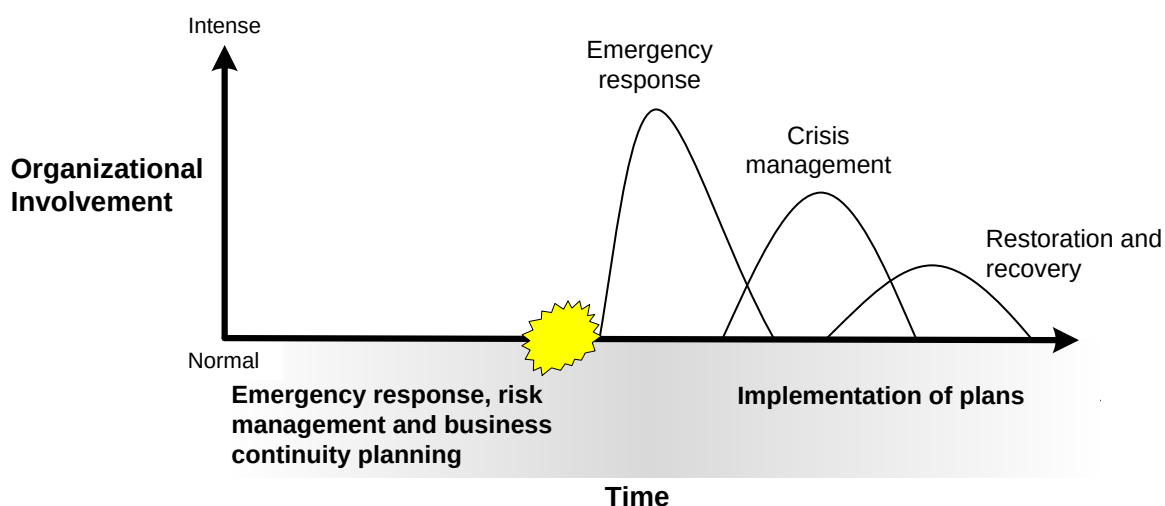


As Exhibit 1-42 shows, the emergency narrative has four phases that unfold over time and that vary in the extent of organizational involvement:

1. **Emergency preparedness, risk management and business continuity planning.** Emergency planning, which includes exercising plans, should be seen as part of an organization's normal state. Emergency response and business continuity planning committees are involved most directly, with occasional involvement of senior management and occupants.
2. **Emergency response.** In the immediate response, plans are implemented. Resources are deployed and occupants evacuated as needed, depending on the nature of the incident.
3. **Crisis management.** As the facility gains control over the incident, a crisis management team manages the long-term effects of the incident. Occupants begin a return to normal operations, although perhaps under different conditions. Critical processes are continued as needed.
4. **Restoration and recovery.** The facility returns to normalcy through restoring or replacing assets and recovering function. All business processes are continued at previous levels.

Each of these phases is described in more detail below.

Exhibit 1-42: The Narrative of an Emergency



Planning

The planning phase lays the foundation for the rest of the narrative. What happens later depends on whether the organization has been effective in:

- Risk management—identifying risks and planning to prevent their occurrence or mitigate their impact.
- Planning, testing and exercising its emergency response plan (which may also include plans for crisis management and emergency communications).
- Planning how to sustain essential business processes during and immediately after the incident.

During the planning phase, the organization gains a deeper awareness of the risks to which it is vulnerable and the essential processes that must be continued without interruption or recovered quickly. It then assesses its emergency preparedness and develops plans that meet the organization's goals and that comply with local requirements.

Emergency response

When an incident occurs, the organization implements its emergency response plan and its incident management team and support teams. The team leader or incident commander on the scene quickly assesses the nature and severity of the incident and implements the necessary immediate response. The goal is to safeguard life, limit injuries, stabilize the situation and prevent escalation of physical damage.

Crisis management

During crisis management, senior management acts to preserve the organization's value after the incident by managing its impact, supporting recovery and taking advantage of opportunities, such as available aid or strategic improvements during recovery. Crisis management planning may include crafting a communication strategy aimed at preserving the organization's reputation, prioritizing recovery goals and funding programs.

As soon as the immediate incident is under control, local teams and/or management assess the situation and decide whether to implement the business continuity plan. Quick and appropriate response is critical during crisis management, and the organization's ability to make quality decisions—and then implement and monitor them—depends on the effectiveness of business continuity planning.

The level of coordinated organizational involvement (the highest points of the three arcs in the diagram) is highest during the initial response period. As time passes, a decreasing proportion of the organization will be involved in the crisis management and recovery phases.



Restoration and recovery

During the final phase of the narrative, restoration and recovery, damage is assessed and the organization (and its insurers) decide whether to repair or replace (and possibly relocate) the affected assets. Fewer individuals may be involved in this effort, but their involvement may be extended, depending on the severity and scope of the event and the recovery strategy.

The duration and expense of the effort to manage an emergency from start to finish depends on the nature of the incident, but these effects are also directly related to the soundness of the organization's planning and preparation. Lack of planning and coordination will slow incident response and immediate and long-range recovery. As the Insurance Information Institute reported, some may never recover.

Principles of emergency management

In 2007, on the sixth anniversary of the World Trade Center disaster, a consortium of organizations focused on emergency management (including the U.S. Federal Emergency Management Agency and professional associations such as the International Association of Emergency Managers) announced the culmination of several years of analysis and discussion. The *Principles of Emergency Management* was intended to provide organizations with a common framework on which to model their emergency preparedness programs.

The eight principles describe emergency management as:

- **Comprehensive.** Programs consider all risks and impacts, the perspectives of all stakeholders and the entire process of emergency management, from planning and mitigation through response to recovery and response evaluation.
- **Progressive.** Organizations are proactive rather than reactive. They take steps before disasters occur to reduce their vulnerability. By doing this, they make themselves more resilient to crises.
- **Risk-driven.** Organizations prioritize allocation of resources for emergency management based on risk management principles, including identification of risks and analysis of organizational vulnerability and potential impact on business processes.
- **Integrated.** Organizations, government and nongovernment agencies and communities partner in their planning so that the needs of each can be addressed in the response.



- **Collaborative.** Effective programs are built on trust and team efforts—among the organization’s own functions and also with government agencies and local communities.
- **Coordinated.** Programs synchronize all participants’ activities toward a common purpose.
- **Flexible.** Programs allow responders to modify tactics and develop alternative solutions during emergency responses as the event requires.
- **Professional.** Emergency management is a science- and knowledge-based discipline. Ongoing training in best practices and new technology is essential.

These principles underlie the basic approach toward emergency preparedness and business continuity planning in this competency.

✦ Topic 3: Strategic Alignment of Emergency Preparedness and Business Continuity

Emergency preparedness and business continuity programs are successful only when they are aligned with the organization’s mission, values and strategic goals.

Business continuity consultant Robert Hall lists four priorities for any organization in responding to a crisis:

- Safeguarding people, physically and psychologically. This includes occupants and their families.
- Stabilizing essential business processes. This is essential to ensuring the organization’s financial health and its ability to satisfy contractual and regulatory requirements.
- Securing the organization’s reputation.
- Supporting business recovery—a return to “normal” as quickly and efficiently as possible.

The relative importance of these priorities may vary, however, depending on the organization’s culture, values and strategy. It is important therefore that, before developing emergency preparedness and business continuity programs, those involved—including FM—know the answers to certain questions:

- **What is the organization’s central mission?** The answer to this question will help identify the organization’s mission-essential functions or processes. These processes will be discussed in Chapter 2.



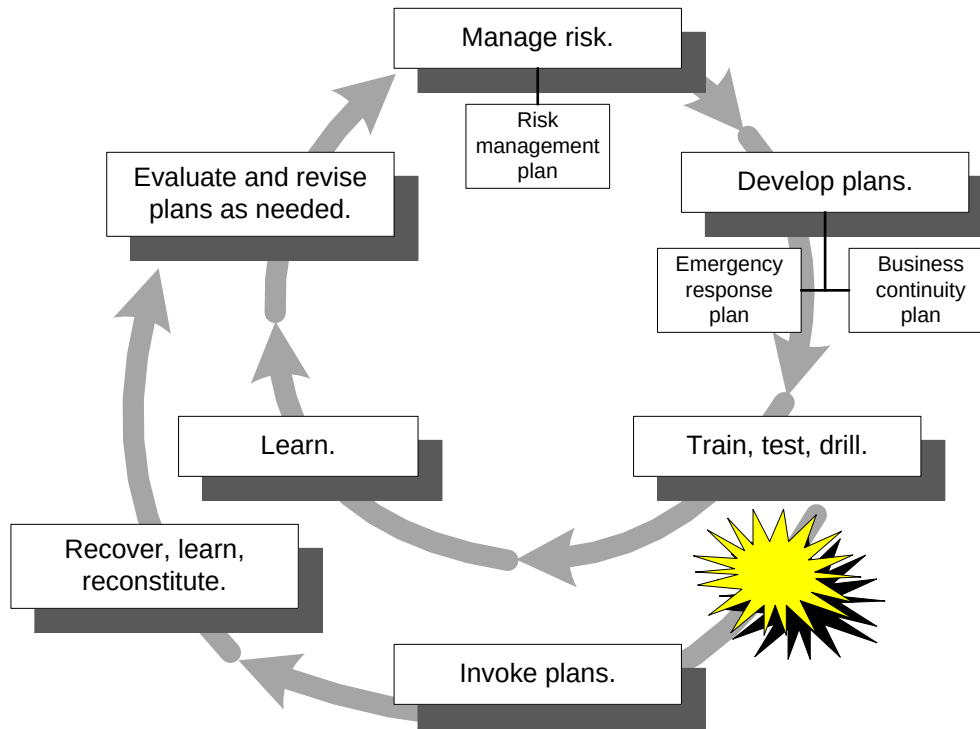
- **Are emergency preparedness priorities aligned with the organization's strategic priorities?** This will affect management's allocation of resources to mitigation efforts and business continuity planning. For example, a strategy dependent on continuous production to achieve market dominance will require greater focus on protecting production assets and speeding recovery from events.
- **How aware and committed to the concepts of risk management, emergency preparedness and business continuity is senior management?** Management must be fully engaged for emergency preparedness and business continuity programs to succeed. It may be necessary for FM to make a business case for these programs and to form alliances with other functional leaders to champion them.
- **How familiar with the principles and benefits of emergency preparedness and business continuity are occupants and other functions?** Their participation in developing, testing and implementing plans is critical. Will they fight the process or support it?
- **How do the priorities of the organization's management align with FM's priorities during an emergency?** Will the facility manager meet resistance from senior management to plans related to people needs, such as evacuation drills? Is management not placing enough emphasis on continuing essential business processes? This can happen if management feels overwhelmed by the complexity of business continuity planning. If FM believes the organization's priorities are askew, FM may have an ethical responsibility to educate senior management about the possible negative outcomes.
- **Is the organization's level of risk tolerance realistic?** Is the amount of uncertainty that senior leaders accept based on reality or is it too optimistic? FM may need to educate management about costs that can be avoided through mitigation. They must also be educated about the financial cost of doing nothing.
- **How will the organization's decision-making structure affect emergency preparedness programs?** What decisions is management comfortable delegating to temporary emergency managers?
- **Will the culture of the organization support the level of collaboration and trust required to develop and implement plans?** Steps may have to be taken now to demonstrate understanding of the needs and perspectives of other functions and to cultivate alliances.



✦ Topic 4: Emergency Preparedness and Business Continuity Model

This competency is organized around the model shown in Exhibit 1-43. It superimposes the traditional project management steps of planning, doing, checking and acting onto the emergency narrative discussed in Topic 2. This topic overviews each step to preview later, more complete discussions.

Exhibit 1-43: Emergency Preparedness and Business Continuity Model



The responsibility to document actions applies to many steps in this model, whether to comply with internal governance standards or with local regulations. FM should be aware of all documentation requirements and ensure that they are included in standard operating procedures written to support plans and in training designed to support plan implementation.

The other factor that applies throughout this model is external communication—collaborating with first responders and insurers who can provide useful advice on preparedness. FM must ensure that first responders are provided with facility information (e.g., facility maps, lists and locations of hazardous materials) and with access to the facility itself during an emergency.



FM must understand insurance requirements, both in terms of prevention and mitigation but also during the restoration/replacement and recovery periods.

Note: Some of the terms and concepts mentioned in the previews below will be defined and illustrated in later chapters.

Manage risk.

During this phase, the organization:

- Identifies, analyzes and manages risks to the organization and the FM function.
- Conducts a business impact analysis. Processes that are central or essential to the organization's or FM's function are identified, and the effect of losing the ability to perform those processes or functions is studied. Priorities and recovery time objectives are established.
- Develops and implements a risk management plan to manage risks. This may involve different types of programs: prevention (e.g., installing security locks to prevent unauthorized entry, installing uninterrupted power supplies on critical equipment to protect it from power surges), mitigation of the effects of an event (e.g., fire suppression systems that could limit the spread of a fire, emergency lighting systems, backup power supplies or facilities) or risk sharing (e.g., insuring).

The outcome of this process is a risk management plan that guides the organization's and facility's risk prevention and mitigation program.

These activities are discussed in Chapter 2, "Manage Risk."

Develop plans.

During this phase, the organization develops emergency response and business continuity plans. A communication plan may also be developed separately as part of the emergency response plan. The planning process requires management support since the plans will require funding and time, and the planning products—the plans themselves—will need management approval before they can be tested and implemented.

The emergency response plan describes an organization's response to an emergency—how each component of the response system performs. This entails defining roles and responsibilities, collecting and maintaining requisite supplies and identifying contractors to provide support during an emergency.

The business continuity plan identifies strategies for continuing essential processes during the incident and resuming identified processes within the



specified recovery time. Like the emergency preparedness plan, roles and responsibilities must be defined and resources must be secured.

The planning process and components of these plans are discussed in Chapter 3, “Develop Plans.”

**Train, test, drill/
learn.**

This phase may contribute the most to successful emergency preparedness and business continuity programs. Everyone in the organization must be informed to the extent of their involvement in these processes. Those in charge of evacuating facility areas must be trained in their responsibilities, the location of supplies and critical areas, the process of evacuation and how to act in different situations. Occupants may need to be trained only in the location of emergency systems and the evacuation process itself. Those involved in mitigation efforts will need to be trained in correct procedures, location of equipment and supplies and compliance requirements. Employees must know where and when they should report for work and any changes in work processes.

The plans must be tested and the participants drilled to ensure that they understand what is expected of them and will perform as required. Testing and documentation of training may be required by law and/or contracts with insurers.

Each drill presents an opportunity to learn from the experience—to analyze plan specifics and participant performance and to implement changes and additional training as needed.

Approaches to testing and recommendations for conducting drills are discussed in Chapter 4, “Train, Test and Drill.”

**Invoke plans/
respond, learn and
reconstitute.**

In the event that an emergency is recognized and announced, the emergency response plan is invoked and responses appropriate to the incident taken. The emergency response team members must assume their roles, quickly gather and share necessary information, assess the situation and make appropriate decisions. Sound and prompt decisions can affect the safety of occupants, ensure security of facility assets, support business continuity and shorten recovery time and cost.

As with training and drills, actual emergencies offer the organization an opportunity to learn and improve their emergency preparedness and responses. Debriefing sessions can identify both weaknesses and opportunities.



Activities during and following an emergency are discussed in Chapter 5, “Respond, Recover and Learn.”

Evaluate and revise plans.

Either on a regular basis or when organizational circumstances have changed, the risk management, emergency response and business continuity plans must be revisited, analyzed for possible gaps or inadequate protection and revised as needed. Whenever there are significant changes in the organization’s strategy, processes and assets, existing plans must be reviewed and revised to ensure that occupants and assets are adequately protected and that priorities are properly aligned with the organization’s strategy and mission.

The evaluation phase is discussed in Chapter 6, “Evaluate and Revise Plans.”



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. Recovery from an incident may depend on the scope, severity and timing of the incident but also on _____.
2. In which of the following organizations is FM involvement in emergency preparedness and business continuity programs probably restricted to implementing risk prevention and mitigation measures?
☐ a. Small manufacturing facility that has just opened and has no budget for risk management
☐ b. Large multinational with multiple facilities and risk management officers
☐ c. Growing organization that is aware of vulnerabilities but has not developed formal plans
☐ d. Large organization that has incorporated risk management in its business strategy
3. FM seeks support for an emergency preparedness and business continuity budget but faces resistance from a senior manager. List at least four benefits of these programs to the organization that FM could mention.

4. In the narrative of an emergency, in which phase is senior management most directly involved?
☐ a. Planning
☐ b. Emergency response
☐ c. Crisis management
☐ d. Restoration and recovery
5. List the eight principles of emergency management articulated by a consortium of emergency management agencies and professional associations.

6. Why is it important for FM to be aware of senior management's level of risk tolerance?



Progress check answers

1. Recovery from an incident can also depend on an organization's state of preparedness for incidents and process interruptions. (p. 1-143)
2. c. This organization has not developed its awareness of the importance of emergency preparedness and business continuity to the point where it has developed strategies and plans. However, it is aware of the need for protection against threats. FM is likely to focus on addressing facility vulnerabilities through specific prevention and mitigation activities. (p. 1-145)
3. FM might mention:
 - Protection of organizational assets.
 - Ability to continue mission-essential processes.
 - Improved compliance.
 - Lower insurance rates.
 - Increased stakeholder satisfaction.
 - Better communication and teamwork.
 - Increased efficiency.
 - Fostering of a proactive orientation.
 - Decreased vulnerability to litigation. (p. 1-146)
4. c. Senior management is indirectly involved in planning and recovery but is directly involved in crisis management. (p. 1-149)
5. Emergency management should be:
 - Comprehensive.
 - Progressive.
 - Risk-driven.
 - Integrated.
 - Collaborative.
 - Coordinated.
 - Flexible.
 - Professional. (p. 1-150)
6. Management's risk tolerance will affect its support of risk management, emergency preparedness and business continuity programs. FM must ensure that management's assessment of risks is realistic so that programs receive the required support. (p. 1-152)



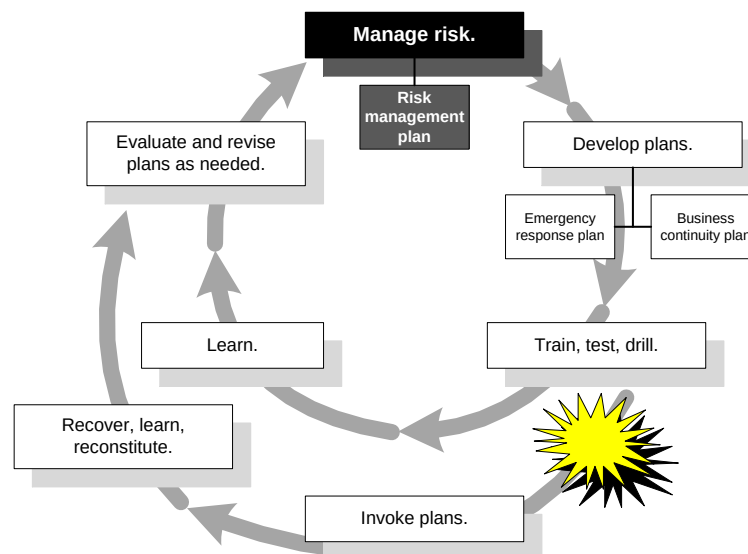
Chapter 2: Manage Risk

After completing this chapter, students will be able to:

- Define risk management.
 - Describe FM's role in the risk management process.
 - List the steps in the risk management process.
 - Characterize the nature and sources of risk.
 - List tools for identifying facility risks.
 - Define the risk factors, probability and vulnerability.
 - Describe tools used to analyze risk.
 - List tools to identify facility assets.
 - Distinguish among mission-essential functions, supporting functions and nonessential functions.
 - Describe the purpose and outcomes of a business process analysis.
 - Describe the purpose and outcome of a business impact analysis.
 - Illustrate risk management strategies.
 - Given specific risk scenarios, identify appropriate mitigation tactics.
 - Describe the impact of risk management strategies on FM policies and processes.
 - Describe FM's role in managing technology risks.
-

This chapter focuses on the first phase in the emergency preparedness and business continuity model, highlighted in Exhibit 1-44.

Exhibit 1-44: Emergency Preparedness and Business Continuity Model—Manage Risk



Risk management is an essential first step in planning for emergency preparedness and business continuity. During the risk management process, FM and the organization gain greater awareness of the hazards the facility and the organization face and how their occurrence could affect the facility, occupants and organizational processes. This information will be used to decrease the facility's and the organization's vulnerability to hazards, but it is also integral to the other planning processes.

This chapter focuses on:

- Assessing and analyzing risks to the organization and facility.
- Conducting a business impact analysis.
- Managing risks to the facility and essential organization and FM processes and assets.

The chapter begins, however, by overviewing the process of risk management.

✦ Topic 1: Risk Management

Overview of risk management

The ISO 31000:2009 risk management standard defines risk as “the effect of uncertainty upon objectives.” In other words, risk is the possibility that something will not turn out the way it was intended.

In the *Finance and Business* competency, risks associated with contracting with vendors are discussed. In *Project Management*, risk is discussed in terms of factors that can prevent a project from producing the desired outcomes and from being completed on time and within budget. In the context of emergency preparedness, business continuity and FM, risk is essentially anything that threatens people, property and processes—in other words, occupant health and safety, the facility's physical assets, and the infrastructure that supports the organization's productivity.

Risk management is a way to live with the uncomfortable reality of risk. It has become a critical component of strategic management. By practicing risk management, organizations decrease the occurrence or impact of certain risks but are still able to pursue opportunities in the face of uncertainty. Major decisions can be evaluated to identify their risk benefit ratio, and organizations may develop characteristic risk appetites—how much risk they are comfortable assuming. Organizations may also balance the risk levels of different parts of their portfolio. For example, opening a facility in a politically unstable area may offer enough potential benefit to justify the action, but this risky venture may be balanced by several other facilities with much lower risk profiles.



FM's role in managing risk

Strategically managed organizations have high-level risk management strategies that influence risk management plans for each of their functions, including facility management. Facility managers must understand the organization's risk management goals and strategies to ensure that FM's risk management plan is aligned with the organization's risk management goals and approaches.

Facility managers will be directly involved in managing risks to the FM function—in conducting a risk assessment and developing a facility risk management plan. Facility managers must be prepared to support requests for funding for risk management programs and to help senior management fully and accurately understand the impact of facility risks.

With their breadth of contact both inside and outside the organization and their direct contact with the infrastructure that supports the organization's work, facility managers have an obligation to help management gauge their appetite for risk more accurately.

Did You Know?

In 1992 and again in 1993, after the first bombing of the World Trade Center, Morgan Stanley's director of security Rick Rescorla advised senior management of the risks associated with staying in their WTC office. He cited the building's structural issues, its visibility and desirability as a target, and the vulnerability to the type of attack that eventually did occur on September 11, 2001. The recommendations could not be implemented for good and common business reasons, among them the fact that Morgan Stanley's lease at the WTC ran until 2006. Nevertheless, Rescorla had performed ethically in advising management of the risks and, as will be discussed later, in attempting to manage the risks that the facility's location entailed.

To create a sound facility risk management plan that is properly aligned with the organization's strategy, facility managers:

- Must be familiar with the kinds of risks that can occur—e.g., power failure, bad weather, flooding, fire, failure of structural elements—and the frequency and likelihood of their occurrence.
- Understand the vulnerabilities of the organization's structures and infrastructure to these risks.
- Know the impact of damage to facility equipment and systems or disruptions in FM processes on key organizational functions.
- Balance the critical nature of the organization's missions and functions against the possible occurrence and impact of a risk event.



In addition to FM's role in managing risk to facility assets and FM processes, FM may also participate in organization-level risk assessments and the development of risk management strategies.

Risk management process

Exhibit 1-45 shows the steps in the risk management process that FM, as well as the organization, will use. The organization proceeds through three steps:

1. Identify and assess potential risks.
2. Identify critical assets/processes and analyze the impact to the facility and organization of their disruption.
3. Develop a risk management strategy.

Exhibit 1-45: Risk Management Process



Throughout the process, ongoing communication—between leadership and the risk managers, among function managers, with experts and regulators—is essential. The process is also cyclical. The organization's risk position must be reevaluated regularly and every time a change to the risk profile is identified. If the risks have shifted, if the organization's strategy has changed or if the risk strategies have proven ineffective, the process should be repeated.

The first three steps are discussed in Topics 2, 3 and 4 of this chapter. The activities of monitoring, evaluating and revising risk management, emergency preparedness and business continuity plans are discussed in Chapter 6.

This chapter focuses on FM's activities in managing risks to the facility and the FM organization. However, as mentioned earlier, the risk management process applies to the entire organization, and FM may participate in organizational risk management programs.



✦ Topic 2: Identify and Assess Risks

The risk assessment process focuses on prioritizing risks to the facility by identifying relevant risks; assessing the impact of risk events to facility operation, occupant and visitor safety and organizational processes; and assessing how well protected the facility or function is against the occurrence of this risk event.

The nature of risk

The assessment process is driven by participants' perceptions about what risks they are subject to. So, before addressing the issue of assessing risk, it will be useful to consider what risk may look like to a facility manager. Risk can take many forms, and FM must consider the entire range of possible risks to the facility.

- **Risk can derive from internal and external sources.** Internal risks in a facility might be a poor building envelope that makes the facility vulnerable to moisture infiltration, or it might be reliance on highly specialized staff who cannot perform the full range of functional tasks in the event of a staffing emergency. An external risk could be a freight railroad track adjacent to the facility, where an overturned freight car with ammonia or some other toxic material could threaten the facility.
- **Risk is created by humans, natural forces and technology.** Exhibit 1-46 lists examples of risks stemming from each of these categories. These examples are only illustrative. Risk may take many forms, and many may be site-specific.

Exhibit 1-46: Categories of Risks to Facilities and Organizations

Natural	Human-Made	Technological
Weather or environmental disturbances, such as: • Rain. • Drought. • Fires caused by weather conditions. • High winds (or lack of wind if a facility depends on wind energy sources). • Snow, ice, hail. • Earthquakes. • Tornadoes. • Floods. • Coastal flooding and tsunamis. • Hurricanes or typhoons. • Temperature extremes.	Voluntary and involuntary events such as: • Fire. • Water damage from plumbing. • Theft and vandalism. • Employee negligence. • Workplace violence. • Terrorism. • Bombs. • Civil unrest. • Damage to key systems (e.g., power, gas or water lines) caused by construction or poor/no maintenance. • Release of toxic materials (e.g., radiation). • Release of harmful biological agents. • Unhealthy air or water quality.	• Building system failures (e.g., HVAC, communications) • Equipment failure • Cyber attack • Large network failures: • Internet outages • Satellite failures • Transmission line damage or malfunction • Pipeline malfunctions • Inaccessible or inadequate transportation systems



- **Events that pose risk can be both predictable and unpredictable, occurring with little or no warning.** For example, modern meteorology can predict weather events such as hurricanes fairly accurately, and facilities will know if they are located in earthquake zones. However, thunderstorms can turn into tornadoes quickly and rainstorms can stall unexpectedly in their paths and cause flooding. From a social perspective, a facility manager might predict vandalism during labor unrest, but violence can occur without much warning as the result of an individual experiencing a psychotic episode or mental breakdown.
- **Risk can be geographically close or distant.** Organizations are usually much more aware of risks in their immediate environments, such as a neighboring facility that works with hazardous chemicals or vandalism to vehicles in the facility parking lot. However, some risks derive from events occurring in remote locales. In a global organization, for example, political unrest might force the closing of certain facilities, which will disrupt business processes. Remote emergencies can also affect the supply chain.

Did You Know?

Events such as the terrorist attacks on September 11, 2001, in the U.S., attacks on London and Madrid public transit in 2004 and 2005 and in Mumbai in 2008 or the tsunamis in the Indian Ocean (2004) and Japan (2011) tend to dominate perceptions of risks to facilities—perhaps because of their scope and suddenness and the associated loss of life. In focusing on risk, however, facility managers should remember more mundane possibilities. The Chartered Management Institute in the U.K. reported that from 2002 to 2011, the most common disruptions to businesses were related to severe weather or loss of IT, telecommunications or access to the facility. A good example was the winter of 2010 to 2011 with its heavy snowfalls, an influenza epidemic and a disruption in air traffic due to volcanic ash fallout from the eruption of a volcano in Iceland.

Identifying risks

To compile a list of risks to which a specific facility might be vulnerable, FM may use the following sources:

- Government bodies, such as meteorological, economic development or emergency management agencies. (Emergency management agencies or ministries of the interior may have guidance documents that list risks, such as flood zones or areas prone to earthquake, and may be able to provide more specific local guidance on the frequency and scope of different types of events. Economic development agencies or consultants can provide information about the adequacy of a region's roads or electrical distribution systems.)



- First responders (e.g., fire, police), who can draw on direct experience as well as records.
- Insurers, who base their services on careful analysis of a broad base of experience.
- Facility and organization records as well as organizational memory of previous events the organization has survived. (For example, records on facility damages sustained due to weather can help identify particular facility vulnerabilities during hurricanes, typhoons and high winds.)
- Discussions with other facilities in the area and with comparable facilities in other areas.
- Consultation engagements with experts in risk management.

FM should also study maps of the facility itself and of its surrounding setting to identify problematic adjacencies that may have escaped previous notice. Exhibits 1-47 and 1-48 on the next page show two examples from the U.S. Federal Emergency Management Agency (FEMA).

Exhibit 1-47 shows the way in which critical, nonredundant functions have been collocated near a point of vulnerability—in this case, the facility’s loading dock and warehouse. The detonation of an explosive device or chemical/biological/radiological attack in that area would compromise the telephone switch, data center and uninterrupted power supply and cut off a means of evacuation (the stairs).

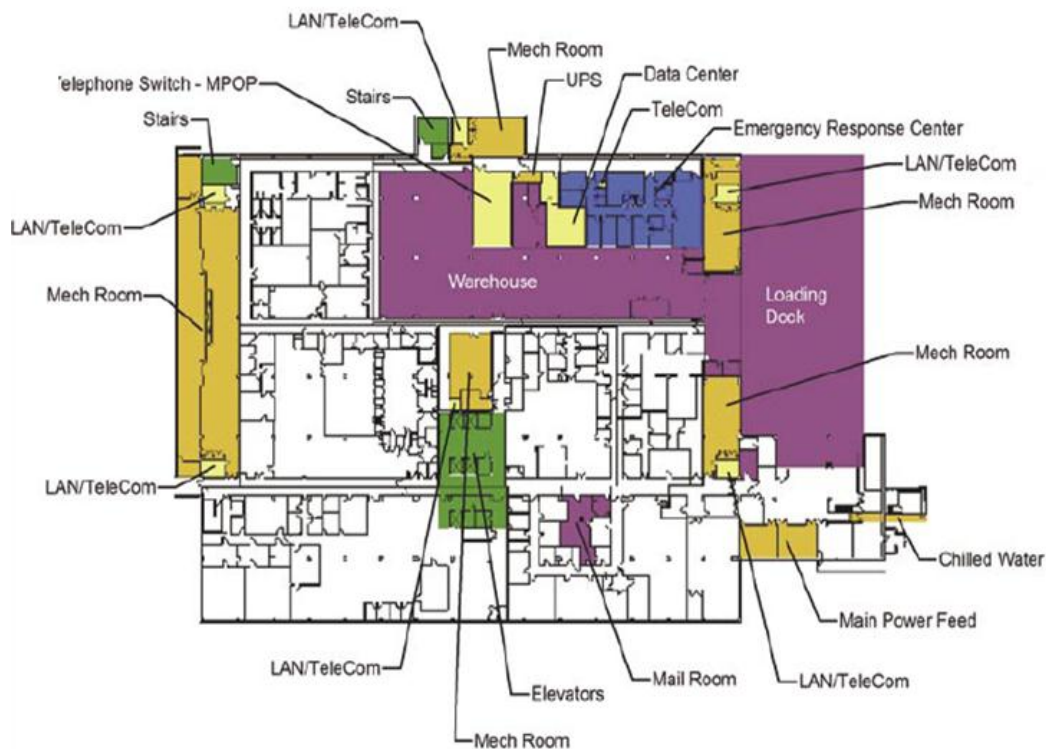
Exhibit 1-48 shows the possible impact of a plume of chlorine gas released during a rail accident in Washington, D.C., spreading with the help of a southwestern wind across a large area. When a facility is selecting a location, careful study of a detailed map of the proposed site’s surroundings is in order. Analysis might uncover features, such as the freight train line in Exhibit 1-48, that pose risks. The location and/or number of highway ramps may suggest vulnerabilities for evacuation. A neighborhood map can be used to understand risks posed by adjacent businesses. For example, a neighboring facility may use toxic chemicals in a manufacturing process, posing a risk to occupants in the event of a spill or release of chemical fumes.

Did You Know?

In April 1995, the Alfred P. Murrah Federal Building in Oklahoma City was bombed, using a homemade truck bomb. The facility housed multiple government agencies, and a child care center for building employees was located on the second floor, above the loading lane in front of the building where the truck bomb was detonated. Nineteen children were killed.

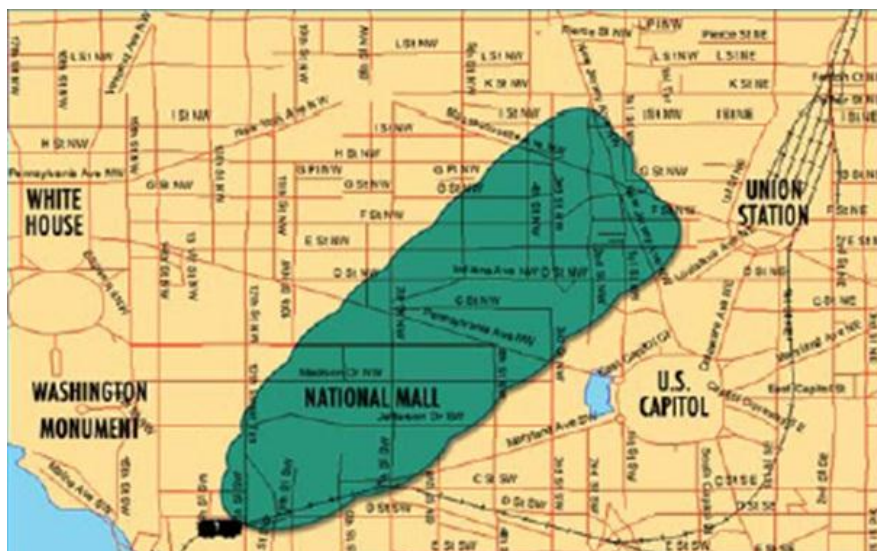


Exhibit 1-47: Mapping Facility Vulnerabilities



Source: *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*.
U.S. Federal Emergency Management Agency, Risk Management Series, December 2003.

Exhibit 1-48: Mapping Facility Environment



Source: *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*.
U.S. Federal Emergency Management Agency, Risk Management Series, December 2003.



Risk assessment

Risks are traditionally assessed according to two perspectives:

- Probability or vulnerability
- Impact

Probability or vulnerability indicates the degree to which a facility is likely to experience a given risk. For example, a facility has a one percent chance each year to experience a “100-year storm event,” the parameters of which are defined locally. A facility built in an area designated a flood zone is vulnerable to flooding. A facility built near an active geological fault will be more vulnerable to damage from earth tremors. A facility whose occupants rely heavily on public transportation to access the site will be vulnerable to disruptions in public transit.

Impact refers to the effect of the event on the organization’s assets, occupants and/or processes. A power outage for eight hours may have only light impact on a university library, but the same outage could have severe impact on the university’s research labs. Other factors affecting impact include:

- **Timing.** Does it make a difference to the organization if the event happens at different times of the day or month, week or year? Does disruption at a particular point in a process do more harm than at other points?
- **Duration.** Can the function absorb an interruption of access for an entire day or two? Or will the interruption begin to affect essential processes immediately?
- **Coincidence.** What if two risk events occur at the same time? Is the impact the same or does it increase?

Risk assessment tools

Risk assessment tools are used to gather functional perceptions of identified risks. The tools can be distributed to multiple raters and the results analyzed by the entire group of risk strategists. The results are useful in supporting decisions about how to allocate limited risk prevention and mitigation resources.

Two tools are shown here.

Exhibit 1-49 is based on an online survey that asked function representatives to rate certain event scenarios in terms of a scenario’s probability and its likely impact. The example includes a cross-section of the type of threats that a facility might face. Respondents rate each event according to probability, speed of onset, impact and effectiveness of existing mitigation. Ratings are multiplied to produce a total for each event, and responses for each event are aggregated. This approach



can highlight key weaknesses and opportunities for improvement. For example, for the accounting function in this organization, events that would cause a sudden or prolonged disruption of their processes are a concern as are theft and sudden loss of key personnel. While FM cannot address the function's staffing and succession issues, it could explore vulnerabilities to theft to see if security mitigation steps would help. It might also explore business continuity strategies to continue essential processes.

Exhibit 1-49: Sample Risk Assessment Spreadsheet Tool

Function: Accounting					
Event/Threat	A: Event Probability	B: Speed of Onset	C: Existing Mitigation	D: Severity of Impact	Threat Ranking Index
	1 = Unlikely 2 = Possible 3 = Probable	1 = Very slow 2 = Gradual 3 = Sudden	1 = Strong 2 = Average 3 = Weak/none	1 = Little 2 = Considerable 3 = Severe	Multiply ratings for each event/threat (A*B*C*D).
Water supply interruption exceeding 4 hours	1	3	3	2	18
Chemical spills	1	3	2	1	6
Power outage exceeding 4 hours	2	3	2	2	24
Hurricanes	3	2	2	2	24
Loss of database exceeding 4 hours	2	3	2	2	24
Winter event causing loss of access to facility	3	2	1	1	6
Theft	2	3	3	2	36
Sudden loss of key personnel	2	3	3	3	54

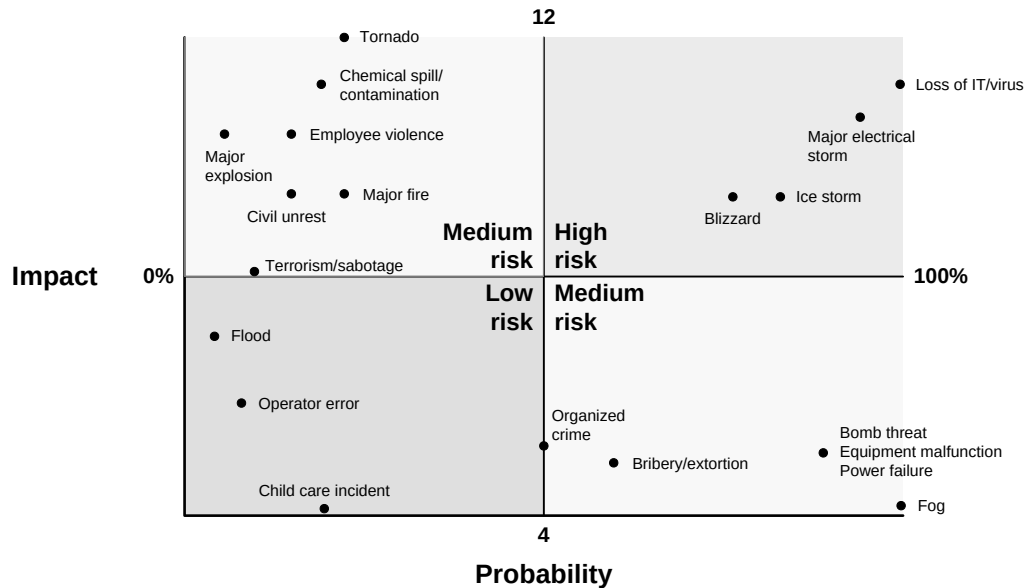
Exhibit 1-50 on the next page illustrates another, more graphic approach to risk assessment—the risk matrix. A risk matrix asks risk assessors to place specific risks on a matrix with two axes: likelihood and impact of loss. A risk matrix is especially useful as a tool to support allocation of resources toward mitigation efforts.

Events are placed within four quadrants:

- **Low impact/low probability.** This is the lower left quadrant. Events here happen infrequently, have little impact and are considered low risk events. For example, operator error would have some impact but is unlikely to occur. Spending on additional operator training is probably not merited.



Exhibit 1-50: Sample Risk Matrix



- **High impact/high probability.** This is the upper right quadrant. Events here are both likely to happen and will have significant impact on the organization. Consequently, they are considered high risk events. Loss of IT and weather-related events are a particular concern for this organization. The adequacy of security and backup systems should be carefully analyzed.
- **High impact/low probability.** This is the upper left quadrant. Events here happen infrequently but can have significant impact and are considered medium risk events. For example, a major explosion would be an unusual event but, because of its effects, must be controlled and anticipated. Occupants should be drilled in evacuation procedures. First aid supplies must be on hand, and designated employees should be trained in delivering aid.
- **Low impact/high probability.** This is the lower right quadrant. Events here happen more frequently but have little impact and are considered medium risk events. For example, fog appears to be a very common weather phenomenon but has little impact on operations—perhaps because the organization has already learned to control its possible effects.

The following example illustrates the interaction of different factors in assessing risk. This example will be referred to again in Topic 4 of this chapter.



Call Center Case Study

An organization is looking for a call center location in a particular region. FM has identified a site, but preliminary risk analysis shows that the area has been flooded during the rainy season in five of the last 10 years. The likelihood of flood risk to this facility would be very high.

Probability	
	X

Rating the impact of the risk is affected by several factors:

- The organization has multiple call centers located around the world. In the event of a flood that disables this call center, calls could be automatically routed to another center.
- Meteorological reports almost always allow enough time for facility managers to secure vulnerable equipment and notify workers not to come to the facility.
- The cleanup required would be substantial, but the center could be returned to service after necessary cleaning and repairs.

So the impact of a flood is rated as close to medium for this facility—inconvenient and costly but not devastating to operations. Once impact has been considered, the event moves down to the lower part of the high impact/high probability quadrant.

Impact	Probability	
		X

✦ Topic 3: Identify Critical Assets and Processes

The next step of the risk management process is to identify critical facility assets and business processes. Since emergency response usually involves triage—identifying and focusing energies on the most critical issues first—planning must begin by identifying those assets and processes that are essential to the organization's survival. FM must cultivate awareness of what kinds of activities are occurring throughout the facility, the relationship between these activities and the organization's mission and goals, and the risk scenarios to which these activities are vulnerable.



Critical assets

Implicit to risk management is a thorough understanding of what exactly is at risk—what assets the organization possesses. These assets may be tangible, such as buildings or infrastructure, or intangible, such as public image or credibility with clients and suppliers, the community and government agencies. Assets can include the occupants involved in producing the organization's products and/or services. They also include the facility's environment—supplies of uncontaminated water, air and soil to support continued operations.

Useful tools or partners in this step include the following:

- An enterprise asset management application can locate and provide information about properties and equipment at each site.
- A facility register can help identify high impact building/customer assets and infrastructures.
- The organization's human resource function can provide lists of occupants at each site.
- Functional leaders can identify employees with unique knowledge or skills.

Critical processes

Certain processes will have to be continued or quickly resumed for an organization to survive an emergency. These activities are referred to as mission-essential functions, because they contribute directly to the purpose that drives or justifies the organization's existence.

For more information on the concept of organizational missions, learners should refer to the *Leadership and Strategy* competency.

The nature of a mission depends on the type of organization and its business. For example, the mission of a health-care facility may be to restore and protect the health of its patients, and the mission of a nongovernmental organization that operates orphanages and schools may be to provide security, nourishment and education. As its mission, a property management firm may commit to ensuring that the workplaces it leases are able to support tenant occupancy and productivity.

A mission entails the performance of certain activities. Exhibit 1-51 provides examples of the types of activities the organizations mentioned in the preceding paragraph perform in support of their missions.



Exhibit 1-51: Mission-Related Functions

Health-care facility	
Ensure sanitary, comfortable and safe surroundings for patients. Provide supportive services to patient family members.	Support technology for care providers. Document compliance with guidelines (e.g., anti-infection protocols).
NGO orphanage	
Operate buildings to provide comfortable surroundings for children and staff. Provide 24-hour security against intruders. Deliver meals three times day in each building, including at least one hot meal.	Support on-site clinic services and referrals to hospitals. Operate classes. Operate library.
Property management firm	
Ensure operation of building systems to support tenant workplace activities. Minimize impact of moves on tenants. Support and contract tenant amenity services.	Balance cost of operation with quality of services. Increase value of property for owners.

Within these activities are mission-essential functions, supporting functions and nonessential functions. It is important to distinguish among these types of activities because, in an emergency, limited resources must be directed to the most critical functions, and emergency preparedness and business continuity plans must incorporate those priorities.

- **Mission-essential functions (MEFs).** If an abrupt interruption in a given function for more than a defined time would interfere with the organization's mission, the function is considered a mission-essential function. Loss of these functions precipitates loss across the organization, measured in human lives or injuries or currency, but also in damage to supplier or customer confidence, to public reputation and to compliance with laws and regulations.
- **Supporting functions.** Supporting functions are often needed to continue essential functions. For example, runway maintenance is not an MEF at an airport but it is an essential supporting function. Maintaining the electrical system at the Fukushima nuclear power plant was not an MEF, but its importance as a supporting function was highlighted during the power plant failure after the 2011 earthquake and tsunami in Japan.



- **Nonessential functions.** These activities sustain normal operations but are usually not necessary during brief emergency interruptions. For example, training new insurance adjusters is important to an insurance company, but during a business disruption, training can be temporarily suspended with little, if any, damage to the company's mission of responding to customer requests for service.

Exhibit 1-52 lists mission-essential, supporting and nonessential functions for the three organizations described earlier.

Exhibit 1-52: Types of Functions

	Health-Care Facility	NGO	Property Management
Mission-essential	Oxygen delivery	Perimeter security	Comfortable climate control
Supporting	Maintenance of oxygen delivery system	Operation of power and lighting systems	Building system maintenance
Nonessential	Cleaning of gift shop	Power and lighting to library area	Parking facility maintenance

Identify essential business functions

There must be organizational consensus about what constitutes a mission-essential process. This must be accomplished with candor, trust and a disciplined commitment to the organization's agreed mission. It can be difficult for an organization to declare which of its many functions are truly essential. Those involved in a process often see it as central and critical to the organization's continuance. However, if too many functions are designated essential, the organization will spread its resources too thinly and truly essential processes will suffer. If all departments are not included in the process of determining essential functions, it is also possible that an essential function will be missed and the organization left vulnerable.

Emergency planners must therefore gather perspectives from throughout the organization and compare this picture with the organization's business strategy and mission. The resulting list of mission-essential functions must have the clear support of both management and all department leaders. In order for the emergency response activities to receive necessary funding and resources, management must recognize the functions that must be supported. To achieve a truly coordinated emergency response, all departments must commit to mutual support.



Business process analysis

Since FM is responsible for providing adequate physical space and supporting systems for the organization's business processes, it should be familiar with the business process analyses that have been created by the organization's business units. It should also have its own analyses for FM MEFs.

A business process analysis can be used to understand the requirements of an essential process. FEMA defines a business process analysis (BPA) as:

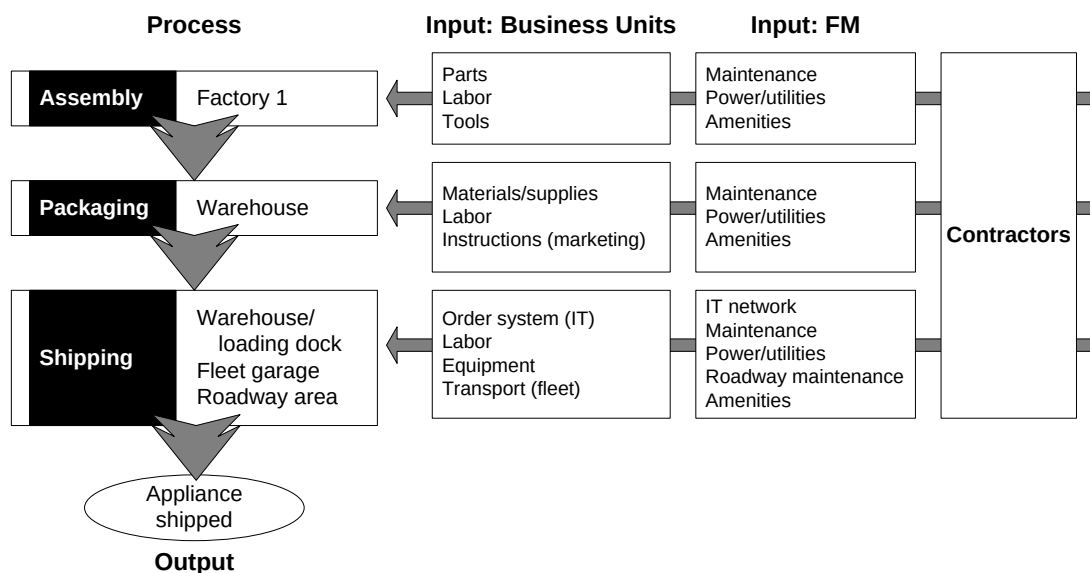
A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, partnerships, controls, interdependencies, and facilities inherent in the execution of [an essential function].

A BPA is a business tool that is commonly used to identify ways in which a process can be made more efficient, but because it clearly describes the required inputs and steps to generate a desired output, it is also a valuable emergency planning tool. The BPA may show:

- Responsibilities at each step.
- Number of employees needed to perform that step.
- Skill level required.
- Duration of each step.
- Special factors about the process (e.g., seasonal factors, time-sensitive steps or deadlines).

Exhibit 1-53 shows a flowchart approach to mapping business processes—in this case, a very simplified process used to assemble, package and ship an appliance.

Exhibit 1-53: Business Process Analysis



By analyzing inputs and outputs, organizations can identify interdependent processes that could be affected by a disruption that involves one or more departments or the entire facility.

As the flowchart example shows, the phases of the process occur in different parts of the facility, and the inputs are provided by the business unit and supporting functions—FM, IT, marketing. The assembly phase is directly dependent on having trained employees in a facility that is secure, safe and equipped with light, power and amenities and access to the parts and tools and supplies employees will need for assembly. The employees in packaging depend on receiving the assembled appliance, any other materials that are included in the packaging (e.g., operating instructions produced by marketing), and access to power, packaging materials and tools in a space that is maintained by FM. Shipping needs the packaged appliance but also needs to communicate with enterprise systems maintained by IT (e.g., customer orders, invoicing, shipping and tracking). It also needs access to transport—i.e., trucks must be able to enter, load and depart the facility. This means that, in addition to the usual services, FM must support the IT network used for order processing. It must also maintain the hard surfaces used for transportation as well as the fleet facility, which will have its own requirements that FM must fill. Throughout this process, the business unit and FM may also depend on one or more contractors, who may be providing parts and supplies. They may also depend on a contractor to support the enterprise system.

While FM may be responsible only for maintaining infrastructure, there are numerous places in which failure in the infrastructure will disrupt the process.

If there is a power failure in the assembly area, there may not be work for employees in packing. Orders for customers will be delayed. A roof leak in the warehouse area may damage packing supplies, including instructions, which then have to be resupplied. And orders are delayed again. If the network goes down in shipping, data cannot be accessed and orders for customers will be delayed. If the roadways are not cleared after a snowstorm, orders will be delayed.

Nonlinear functions can be analyzed as well. For example, one of the primary functions of an educational facility is to deliver classroom instruction. This function requires a variety of support functions from FM: infrastructure support in classroom buildings, janitorial services, voice and data network support, security, campus transportation. Some support functions may be identified as



essential (e.g., power, light, heating/cooling, sanitary amenities) and others as nonessential (e.g., campus transportation, daily janitorial services).

Constructing business process analyses requires considerable investment of time, but they support business continuity planning by:

- Ensuring that all interdependent activities are considered during emergency planning.
- Supporting estimates of what resources will be required to continue essential functions at an acceptable level.
- Serving as training tools for workers who may have to fill in during an emergency.
- Identifying duplicate equipment or similar processes that can be repurposed to continue essential processes.

There are general organizational benefits as well. The organization's members gain a clearer sense of how the organization's parts are related and why teamwork is so necessary. Functions can begin to appreciate each other's perspectives and needs and develop the trust and support that will enable the organization to survive a crisis.

Business impact analysis

During the business impact analysis (BIA), an organization team and/or consultant gathers information about what resources will be needed to resume essential functions after an emergency and continue them until normal operations can be restored. Information can be collected via standard (possibly automated) questionnaires and/or interviews with department heads and key personnel.

Some experts recommend that tools include a brief outline of a hypothetical risk scenario so that respondents can think about the situation in a more concrete, detailed way. The hypothetical case should embody the organization's most serious vulnerabilities, such as loss of access to and use of the facility, loss of data or loss of personnel. It should also propose a time frame for the disruption and any time-sensitive factors—for example, the loss of access to a manufacturing line for two weeks during the peak production period for holiday merchandise.

Respondents are asked to:

- Describe what their departments do (their business processes, showing interdependencies with other processes and functions).
- Identify internal and external stakeholders.
- Describe the number of employees engaged in these processes, including part-time and contract workers.



- Rate the importance of continuing each of these activities in the event of the facility disruption described in terms of supporting the organization's mission.
- Describe the minimal output or level of activity in these processes that would be sufficient to avoid creating serious harm to the organization during the disruption.
- Define a recovery time objective for priority processes, the point at which the minimal output level would have to be resumed or risk causing significant harm to the organization. It is important to quantify recovery time, since goals such as "as quickly as possible" mean different time frames to different functions and in different geographical regions.
- Describe any existing alternative ways to continue the process that would not require new resources or redundant systems.

Some BIA templates also ask respondents to quantify the revenue their processes generate. This will help organizations prioritize their risk mitigation efforts. However, organizations should note that they will not necessarily lose all of this revenue if an emergency occurs. The activity may be continued at a diminished level. It is also possible that the lost revenue will be recouped when the organization regains full functionality.

There are two key points in the preceding bulleted list. First, managers surveyed and interviewed must understand that they are being asked to think about resuming a process at a sufficient level, not necessarily the same level. It may be the case that the organization can survive a disruption with reduced capacity for a defined length of time: commitments can be renegotiated with customers and suppliers, universities can adjust course or exam schedules, and regulatory agencies can issue waivers for certain requirements. If managers request resources to continue operations at the same level—with the same head count and equipment and space—there will be fewer resources for other essential functions.

Second, before creating contingency plans that require additional budget, managers should consider if there are any ways to achieve the process output without activating a special contingency plan. For example, if one location is put out of commission by a fire or flood, can the work of that unit be shifted to another work unit that is performing less critical work? If key personnel are not available to supervise or perform a task, are there other personnel who have been cross-trained in this task?

The outcome of the BIA is a list of essential processes that cannot be sufficiently insulated from risk by prevention or mitigation controls and that cannot be resumed and continued at an adequate level with the resources already at hand.



Having identified and assessed risks and identified MEFs and minimal outputs needed to sustain the organization, the organization can now plan its risk management strategy.

✦ Topic 4: Develop Risk Strategy

Approaches to managing risk

There are five basic approaches to managing risk:

- Tolerate the possibility that the event will occur and accept its possible impact.
- Avoid the risk entirely.
- Devise a strategy to prevent the risk from happening.
- Mitigate or reduce the impact of the event.
- Transfer or share vulnerability to the event.

These strategies are discussed below.

Tolerance

Organizations will often choose to tolerate or accept a risk without further action when the risk is relatively unlikely and its impact low. For example, a facility with underground parking is aware that one level will be subject to flooding during an extremely heavy rainfall that lasts more than an hour. Fixing the problem would be expensive, and it is possible that correcting the grading to direct water flow away from the parking structure could cause more serious problems to other structures. And events such as these probably occur once every five years. For now, simply announcing the impending situation to occupants so that they can move their cars may be the best strategy.

Avoidance

The avoidance strategy is usually adopted when a risk is highly likely and its impact higher than any offsetting benefits. For example, an organization that produces critical components for scientific projects is looking for a new location for a facility in which prototypes will be developed, tested and produced. All of these activities are highly vulnerable to vibration. In identifying possible locations, FM is alert to possible sources of vibration that could affect the organization's mission-essential function. FM consults experts on local seismic activity, identifies adjacent transportation systems that could generate vibration (e.g., highways, rail, airports) and investigates neighboring facilities whose processes might pose a risk of vibration.

Prevention

Strategies to prevent risk would include installation of systems to detect certain risks before they become events—for example, to detect excessive heat or smoke before a fire develops. Prevention may rely on processes, technology or structural elements. A simple example is preventive maintenance of cooling system components prone to condensation and the development of mold.



Ensuring that surfaces are properly insulated and condensate drains are operating prevents the risk of mold contamination. In the case of intrusion, a facility may install alarms on certain unattended doors. If the door is opened, a security person is dispatched to investigate the situation immediately to prevent theft or vandalism. Adding a sea wall can prevent the possible effects of high water levels during storms. Barriers can prevent vehicles armed with explosives from approaching within a certain distance of the facility.

Mitigation

Mitigation strategies are used when a risk cannot be avoided or tolerated or when the benefits of the risk exposure may be greater than the potential losses. In these cases, risk managers seek to minimize or mitigate the impact of the threat. For example, a headquarters facility located in an area prone to hurricanes may choose to accept the risk of property damage and disrupted business processes because of its investment in the facility, better access to its customer base and manager and occupant preferences. To offset this risk, the facility may take the following mitigating steps:

- Routine inspections include roofing and window and door seals to minimize moisture infiltration and damage from wind, but additional inspections are scheduled before the hurricane season.
- Buildings and grounds are audited regularly to identify and trim vegetation/trees that may pose a hazard to adjacent building structures, windows, entrances, drives or walkways in the event of high winds.
- Large objects that could be blown into windows during a storm are securely anchored or removed.
- Batteries and water supplies are stored to support occupants through the normal duration of a storm.
- The business continuity plans include shifting certain processes to regional offices until headquarters is able to resume function. Data processes are continually backed up to a secure location.

Some mitigation may not be necessary or practical, given the organization's business continuity needs. For example, the facility mentioned above considered but rejected the idea of buying backup generators. The facility can be closed for up to three days without serious issues since all data is backed up to off-site locations and can be accessed from remote locations. As long as occupants can find electrical power and communications, processes can continue.

Risk mitigation is a key part of the risk management process for FM and will be discussed further below.



Transfer or share

Transfer/share strategies are used when the risk cannot be avoided, when the benefits outweigh the impact and when the impact cannot be effectively mitigated—perhaps because of cost or uncertainty of effectiveness of the mitigation effort. In some cases, organizations may be able to transfer risk by outsourcing activities to one or more suppliers and requiring them to carry certain kinds of insurance and take steps to provide continuity of service. Insurance is a common form of sharing risk. For a fee (the premium), an insurer accepts all or some of the possible losses associated with certain types of risks. Insurers provide various types of risk transference mechanisms, including property and business interruption insurance. Another form of risk sharing is a memorandum of understanding among organizations. Organizations such as business centers and college campuses agree to share facilities in the event of an emergency. If a business center is incapacitated, the college agrees to provide temporary office facilities for the business center's essential functions.

Topic 2 introduced the case of an organization that is locating a new call center. FM identified and analyzed the risks posed by a certain location and now must make recommendations about managing this risk.

Call Center Case Study (continued)

FM has assessed the risk of flooding as medium high and at first thinks that the best strategy would be to avoid this risk entirely and continue looking for a new site. In discussing the site with senior management, FM sees that there are factors that argue for considering strategies other than avoidance:

- This would be an excellent opportunity to fulfill the organization's commitment to assisting local populations by providing work opportunities. This is a very economically depressed area, and the organization could afford to pay better-than-average wages.
- Even at a higher-than-local average rate, labor costs would be low relative to other global areas. And the organization needs a call center in this time zone.
- Alternative location options in the same time zone have similar issues or do not have the necessary infrastructure.
- Calls could be transferred for up to one week to other call centers. History of the area indicates that flood water recedes within two days and the facility could be returned to an acceptable level of service within the recovery time objective.
- Some employees could work from home for the affected period, but others might not have access to electricity and communication—or a home.

The organization agrees to proceed with the site but will consult with architects and designers to create a more robust structure that can prevent a large portion of flood damage. IT will work with FM to ensure that facility technology can support call load and data sharing with other sites.



Risk management programs

Effective risk management programs usually combine the various strategies just discussed. The choice of strategy will depend on many factors, including:

- The type of loss posed by the risk. An event could mean loss of access to the facility, occupants, power, communication (both voice and data), property and supply.
- The type of hazard (e.g., chemical spills or releases of noxious gases from an overturned railcar, wind and water damage from a hurricane, physical violence and terrorism).
- Proximity to first responders (e.g., fire, police, medical).
- Whether the facility is shared and, if so, the type of tenants sharing the facility. For example, a neighboring law firm will pose different risks from a biotechnology firm.
- How long the organization could sustain a loss of occupant access to the facility or power/communication before the loss begins to harm the organization's mission—the recovery time or point objectives.
- The mitigation budget. Completing a benefit-to-cost analysis of the mitigation versus potential losses can help prioritize projects and support budget requests. A very simplified example would be the addition of a security camera near a less visible facility exit. The camera may cost US\$1,500. The possible loss from theft or vandalism may be US\$50,000. The benefit-cost ratio would be more than 33:1. This example, although simplified, underscores the fact that sometimes small investments can create large improvements in an organization's risk exposure. As the investment increases, however, so does the complexity of the analysis. If the consequences of a risk are very costly, the organization should ensure that the analysis includes discount and sensitivity factors. Discount factors reflect the cost of money over time. Sensitivity factors, such as the degree of uncertainty, modify the analysis output to provide a more accurate benefit-cost estimate.
- Applicable building codes (which may require certain types of fire suppression systems and emergency lighting systems) and regulations, such as regulations regarding access for the disabled.
- Whether the facility is leased or owned. A lease may be structured to transfer some risks and responsibility to landlords.
- Confidence in the effectiveness of the control and that the control can be implemented without introducing other risks that may be difficult or costly to control. For example, installing a diesel



generator can mitigate temporary power loss, but storage of fuel oil can pose additional risks that must be controlled.

- The organization's culture and business strategy (e.g., a culture prone to risk taking, a business strategy that rests on reliably delivering products or services during an emergency).

Exhibit 1-54 on the following pages lists some typical risk scenarios and risk management strategies that might be applied to protect the organization.

The strategies listed are only examples; others are possible. Not all of these strategies will be desirable for various reasons, including those listed above. For example, in the scenario involving loss of potable water from a municipal system, the avoidance strategy of installing a private well may not be feasible from an economic or compliance perspective. In the scenario involving terrorist bombing threats, moving government functions to civilian buildings may put those facilities at risk and might introduce additional risks, since those facilities will not be as easy to secure.

The strategies must be evaluated in terms of their effectiveness and their cost. The plausibility, effectiveness and possible costs of avoidance, prevention and mitigation strategies are indicated in the exhibit in uppercase letters after each strategy. These are subjective evaluations and are meant only to indicate the need to evaluate strategies before selecting them.

Risk management and FM

When FM acquires the habit of looking at facilities and their operation from a risk management perspective, the way FM approaches its responsibilities during the facility life cycle changes.

Design for better risk management

For new or remodeled facilities, FM will seek to become involved at the occupant needs assessment and building design stages to ensure that prevention and mitigation factors are included from the beginning of the facility's life cycle.

Many mitigation elements, above and beyond those required by building and safety codes, can be designed into new facilities.



Exhibit 1-54: Risk Management Strategies (continued on next page)

Risk Scenario	Avoidance	Prevention	Mitigation	Transfer
Hurricane of sufficient force limits travel to headquarters facility, causes damage to building envelope and grounds and causes loss of power for two days.	Choose another facility site. POSSIBLY IMPRACTICAL	Regular inspections of roofing and seals. LOW Board up windows. LOW Trim trees. LOW Secure heavy objects around exterior and on roof (e.g., chillers). LOW	Implement shutdown plan six hours before storm landfall. MEDIUM Implement policies and protocols for telecommuting. MEDIUM Secure backup power generation. HIGH Secure off-site computer data access. MEDIUM FM emergency staffing plan.	Damage and business interruption insurance.
Mass transit strike essentially prevents key FM personnel from accessing facility for strike duration.	Require key FM personnel to have cars or live within walking distance of the facility. PROBABLY IMPRACTICAL	Monitor pre-strike situation and press agency to reach agreement before strike. LOW Cross-training so personnel can fill in for employees who cannot reach the facility. LOW	Implement policies and protocols for occupant telecommuting in case facility must close. MEDIUM Contract with service to transport key personnel. LOW Provide on-site temporary shelter for staff to avoid commuting. LOW	Business interruption insurance.
City announces municipal water supply is unsafe and may not be safe for a week.	Install private well. HIGH	Press city for investigation and changes to system. LOW	Implement emergency communication plan, including signage at sinks. LOW Turn off water at drinking fountains. LOW Provide bottled water. MEDIUM	
Thieves steal servers from data center and vandalize several office areas. Replacement and installation of servers will take two days. Damage repair will make areas unavailable for one week.	Off-site data centers. MEDIUM	24-hour security system. MEDIUM/HIGH	Implement data backup policies and back up to off-site servers. MEDIUM Implement policies and protocols for telecommuting for affected occupants. MEDIUM Agree with neighboring facilities to provide emergency workspace. MEDIUM	Insurance.



Exhibit 1-54: Risk Management Strategies (concluded)

Risk Scenario	Avoidance	Prevention	Mitigation	Transfer
Grease fire in food service causes facility evacuation and extensive damage to food service area and adjacent work areas. No on-site food service is available for one month.	Restrict level of food service to eliminate fire risks. LOW	Routine cleaning. LOW Detectors and suppression systems. MEDIUM Regular inspections. LOW No adjacency of food service to work areas. LOW	Design firewalls. MEDIUM/HIGH Inspect and test emergency systems (e.g., emergency lighting) regularly. LOW Replace/use furnishings that do not produce toxic fumes in fires. MEDIUM Contract with food truck vendors. LOW	Insurance.
Unavailability of critical component from supplier halts production.	Implement rigorous due diligence in vendor selection process. LOW Reengineer process to use another part. HIGH/POSSIBLY IMPRACTICAL	Set up safe and economic reordering point in inventory system. LOW Contract with multiple suppliers. LOW Partner with supplier to gain greater control over supply. HIGH	Scale back manufacturing and implement plan to ensure delivery to prime customers. HIGH	Redesign to purchase as part of assembly from supplier.
Protest outside bank prevents occupants from leaving safely through customary exits.	Transfer critical functions to more remote location. MEDIUM	Install bollards to limit access to facility. MEDIUM Design alternative exits, including through neighboring businesses. LOW	Implement plan to continue food service and support communication with families. LOW	
Government building is targeted by terrorist groups known for using bombs delivered by vehicles or pedestrians.	Locate facility within larger, more secured area. POSSIBLY IMPRACTICAL Eliminate identifying signage. POSSIBLY INEFFECTIVE	Install bollards to limit access to facility and near vulnerable equipment (e.g., main electric distribution panel, gas and water connections). MEDIUM Increase stand-off distance from facility. MEDIUM	Install shatterproof glass. Decrease hazardous materials that could be released in an explosion. Locate vulnerable functions in more protected areas. Implement responder training and provide equipment.	Separate and transfer individual functions to multiple nongovernment buildings.



These could include the following:

- Extending entrances creates greater physical separation from external threats.
- Shatterproof glass can reduce injury in vulnerable areas. A state health department survey of 405 people injured in the Oklahoma City bombing found that 66 percent attributed their injuries to flying glass or falling on glass.
- Shelter-in-place options for events are a necessary alternative to evacuation in certain instances, such as tornadoes.
- Barriers keep car/truck bombs away from facility entrances.
- Emergency evacuation systems can tie in to building automation systems. Emergency lights can be activated automatically. Different-colored lights could demarcate the exit route occupants should take.
- Flexible signage could be used to alert occupants about risks and advise next steps.
- Sound systems can be included so that verbal directions can be issued throughout the facility.
- Video surveillance systems can be tied into building controls and used to gather more information about a threat and support decisions about occupant evacuations.

Operate to support risk management

During the facility's operating life, FM can support:

- Regular inspections by insurers or risk management experts.
- Rapid correction of identified risks (e.g., electrical system malfunctions).
- Maintenance of resources needed for emergency response and business continuity.
- Staff and occupant training necessary for emergency response and business continuity.

Contract with risk management in mind

FM will perform due diligence in contracting with suppliers to prevent disruptions in service and supplies. Leases will be structured to share risk and to incorporate emergency preparedness and business continuity needs. Whether a landlord or tenant, FM can ensure coordinated, announced and unannounced evacuation drills; designate and train floor wardens for emergency evacuations; and ensure coordination with first responders.

✦ Topic 5: Managing Technology Risks

In the emergency preparedness and business continuity competency area, IFMA's global job task analysis emphasized the importance of managing technology risks. Organizations and FM are increasingly dependent on technology to meet the function's strategic objectives. This dependence



underscores the need for a proactive stance in managing technology risk. As a user of technology and in its role as supporting facility infrastructure and business continuity needs, FM must understand the risks involved in technology and measures that must be taken to manage these risks.

Technology risks include:

- Loss of system functionality.
- Loss of system integrity.
- Loss of data.

Sources of technological risk

Technology risks can be caused by human intentional actions or errors and negligence. System security can be breached internally or externally and data stolen or corrupted. Malware (which includes viruses, worms, Trojan horses, spyware and other malicious software) can be introduced to disable systems or steal data or processing ability. Internal or external power sources or network cables can be cut during construction or remodeling. Operators may make mistakes or omit necessary steps. Users may unknowingly download viruses.

Nature in the form of windstorms can damage transmission systems, and natural events, such as typhoons or earthquakes or avalanches, can destroy or damage facility infrastructure.

Technology itself can create certain threats. Surges in the electrical grid or in the facility's power distribution system can damage systems. Errors in code can cause systems to malfunction or crash. Unseen incompatibilities between old and new systems can cause enterprise systems to fail. Systems that have not been thoroughly tested under probable load and conditions may fail when they go online. Whole systems may fail when critical components fail. This includes facility support systems for data centers, such as cooling and air filtration. Excessive demand for power to operate technology itself can cause large-scale power grid disruptions—one of the suspected causes for the almost nationwide power outages in India in 2012.

Managing technology risks

These risks must be assessed to select the most appropriate control strategies and to prioritize mitigation efforts. Although the risks are different, the same strategies can be used. For example:

- **Avoidance.** FM can collaborate with IT when planning FM systems that will integrate with enterprise systems and databases. This allows IT to ensure that the proposed system meets the organization's IT



standards. FM and IT can also collaborate on the design of data centers to ensure that all needs are identified and addressed. When planning new facilities, organizations may choose to avoid areas that do not have a stable power infrastructure.

- **Prevention.** Prevention strategies protect the power supply and security. Uninterruptible power supplies can protect systems against brief loss or fluctuations in power sources. Logical security measures include user identification and password verification and user-defined levels of access. Physical security measures include securing areas that contain IT equipment with locks that require keycards or biometric identification (e.g., fingerprint, iris scans) and installing surveillance systems. Prevention might also include training personnel about secure use of computers (e.g., not leaving laptop computers in an unsecured areas, using security features on computers, ways to avoid infecting computers) and policies about computer use (e.g., rules against leaving laptops in cars or sharing passwords).
- **Mitigation.** Redundant equipment or systems can allow a facility to recover quickly from a failure. For example, a redundant cooling system can be brought online if the primary fails or if it requires maintenance. Data backup systems and policies regarding backup practices mitigate the loss of information from a system failure. If the risk of a power outage is likely and its impact on the organization severe, facilities may install backup power generators. In India, for example, a private hospital decided that, because power outages were so common, they would lease generators. Because of this mitigation strategy, the hospital was able to power its dialysis machines and cool its wards during the 2012 outage.
- **Transfer.** Some organizations may opt to use cloud computing to transfer the risk of function or data loss to a service provider. In cloud computing, a user purchases software or storage as a service for a fee. The service provider is responsible for maintaining the software and equipment and providing security.

The *Technology* competency provides more information about the particular needs of data centers and matching data center business requirements to recommended risk management strategies.



✦ Topic 6: Emergency Preparedness and Business Continuity Case Study

Throughout the following chapters, the case of a fictional organization grappling with the task of emergency preparedness will unfold. The organization described is an office-based, services-focused company, but it could just as easily be a manufacturing concern, a large shopping mall or chain of malls, a university campus or an international bank. The challenges are similar and the process used to meet them very similar.

Emergency Preparedness and Business Continuity Case Study

LGH is a 75-year-old business services firm. It began as a business consultant service but over time acquired or developed other capabilities. It now has four divisions and maintains offices in the U.S., Brazil, England, China and Bahrain. The facilities include owned buildings in two U.S. cities and Rio de Janeiro and leased offices in four other locations.

Since the organization had recently grown extensively and added a new focus on enterprise management tools, senior management assembled a global team to develop a new risk management strategy. The team included the facilities director, representatives from the four divisions and the directors of the IT, finance and HR functions.

In the first meeting with senior management, the team discussed the operational priorities created by LGH's current business strategy, future actions of which the team should be aware (a pending acquisition of a small software company) and the values that the organization's emergency preparedness and business continuity programs must embody. The current strategy rests on maintaining close relationships with long-term clients, gradually expanding those relationships to include LGH's new capabilities. It is essential that service development be dynamic, staying current with emerging business needs and technologies and continually introducing new company services or new versions of current services. It is also extremely important that LGH deliver on its commitments and that it preserve the confidentiality of all client information.

The team decided that it would direct its divisions to complete risk management planning and incorporate these plans into an organizational risk management strategy. This case study will follow the risk management process at LGH Enterprise Management Services (LGH-EMS). LGH-EMS occupies a five-story office building in an office park some distance outside a large metro area. About half of the occupants are involved in system design and programming assigned to five product lines. This area also employs approximately 20 contract programmers who work remotely at offices in various parts of the country.



Since LGH-EMS relies heavily on knowledge workers, management has funded facility amenities designed to attract and retain employees. These include a large cafeteria and cafes with espresso machines on each floor, a physical fitness area with showers and lockers, and a subsidized child-care center that operates 15 hours a day because of the programmers' schedules.

The building is equipped with a wireless system, a virtual private network and a Web/videoconferencing room.

The first step in the risk management process is to identify and analyze risks.

Senior management asked business leaders at the facilities to form risk management teams. The division business manager brought together the on-site facilities manager, the IT manager and representatives from product management and from the design and programming units.

The facility manager, the IT manager and the HR manager completed probability and vulnerability assessments for their areas of expertise—site-based, technology-based and people-based, respectively. The unit leads joined the team to provide more information about how the identified risks would affect their functions.

The risks receiving highest scores reflecting risk probability and impact were:

- Fire that would result in loss of access to the facility and loss of data and communications capability.
- Water damage that would affect the data center and/or network equipment.
- Loss of key personnel.
- Loss of communication.
- Loss of networking access and capability.
- Network compromise and data theft due to cyber intrusion/attack on the network systems.
- Widespread illness.

Fundamentally, however, the management at LGH-EMS was most concerned about any risks to their employees. The company has a strong culture that values teamwork. The result has been strong relationships among the different units and between different levels of employees. Loss of personnel in an event would hurt the company from an operational perspective but would also create a psychological impact that might require years to heal.



The next step in the risk management process is to identify critical assets and processes.

Using the enterprise resource planning system, the facilities manager prepared a current description of the division's assets. The team then worked together and separately to identify critical processes at LGH-EMS.

The division business manager distributed business impact analysis questionnaires to all department leaders at the site, including the facilities manager and HR and IT managers, and then conducted follow-up interviews. The managers were asked to analyze the impact of three possible scenarios: loss of the facility for over three weeks, loss of the network for over two weeks and loss of 50 percent of their staff for three weeks.

Product managers explained that they performed three functions:

- Supporting, monitoring and reporting on the economic performance of a product
- Managing the client support function, which worked directly with clients to answer questions and solve problems
- Providing a point of contact between clients and the technical development side of the company to plan product improvements and new products

Of these functions, the most essential were client support and client-development liaison. The client support area would be seriously affected by the event, and an outage of more than one day would damage the company's reputation with its clients. Without access to the databases, support would be essentially offline. Product managers could, however, resume their client contact outside the facility.

Systems design/programming is structured in teams of systems analysts and programmers who are fluidly assigned to the different products as needed. The processes most affected by this event would be the product line closest to release date. No one would be able to work on the project at the facility or remotely without the data and networking capabilities. Every day during which the facility was not fully operational would mean a full day of delay in product delivery and potential lost sales.

Based on this input, the team concluded that, since the central mission for LGH-EMS was to support client services and develop new services, the division's activities would be identified as mission-essential functions or supporting functions in this manner:

Mission-essential functions:

Product management (five lines)	Programming unit
Systems design unit	Customer support

Supporting functions:

Facility operations	Administrative support
Technical support	Human resources
Graphics	Library resources
Finance and accounting	Marketing services



The final step in the risk management process is to manage the identified risks to protect the organization's assets and continue its essential processes. Business continuity planning focuses on providing what those functions identified as essential or supporting need in order to continue at necessary levels within stipulated recovery times. The risk management strategy will focus on lowering the probability that incidents will happen and the impact on the organization in the event that risks do occur.

Given a limited budget for prevention and mitigation, the team agreed to gather as much information as they could about alternative strategies. The facilities manager issued a request for information (RFI) for upgrades to the fire detection and suppression systems to determine the potential cost of this work. The facilities manager also analyzed information in the facility building information modeling system to identify potential water leakage issues. She requested bids to reroute pipes, and, as much as possible, lines were visually inspected. Routine inspections were added to the maintenance schedule. She also assigned one of her managers to communicate with neighboring facilities in order to compare assessments and share knowledge.

So that they would be able to provide the costs to management, IT and systems design/programming put out an RFI for moving critical servers to an off-site location.

The division manager worked with HR and the unit heads to discuss whether job rotation or cross-training could address the risk of losing key personnel. The conclusion was that knowledge was too specialized for these practices to be of much use. They could, however, hold flu vaccination clinics, distribute hand sanitizers at each desk and encourage their use, and implement policies to require sick employees who were still well enough to work and could work remotely to stay home.

The team worked hard to balance business and employee needs in their final recommendations to senior management. The facilities director would lead development of an emergency preparedness program that would support employee safety and well-being as much as the organization could. At the same time, the team would work with function leads to develop business continuity plans that defined requirements, responsibilities and processes needed to protect the organization and its other stakeholders.

The next chapter discusses the work that lies ahead for LGH-EMS as the team proceeds to the next phase of emergency preparedness and business continuity—developing emergency response and business continuity plans.



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. What must FM do to ensure that the facility risk management plan is aligned with organization's risk management strategy?

2. In the risk management process, the first step is

- ☐ a. develop a risk strategy.
☐ b. identify and assess risks.
☐ c. establish communication channels.
☐ d. identify critical processes.

3. List at least three sources FM could use to identify possible risks to the facility.

4. The risk matrix and similar tools are used primarily to

- ☐ a. guide insurance pricing.
☐ b. develop evacuation plans.
☐ c. protect assets.
☐ d. prioritize resources.

5. Which of the following best describes a mission-essential function?

- ☐ a. The organization's culture and identity are deeply rooted in the performance of this function.
☐ b. The function is the first process that must be performed in a sequence of actions.
☐ c. Interruption or serious delay in the performance of this activity will seriously impair the organization.
☐ d. This function employs the highest number of employees hired by the organization.



6. Which of the following statements best describes a business process analysis?
- ☐ a. Shows the effect of disruption to an essential business activity
 - ☐ b. Identifies potential vulnerabilities at each stage of a business process
 - ☐ c. Highlights inefficiencies and redundancies in a sequential business activity
 - ☐ d. Outlines the inputs, outputs and required resources of a business process
7. What is the primary purpose of a business impact analysis (BIA)?
- ☐ a. Identifying requirements for resumption of an essential process
 - ☐ b. Quantifying the impact of business interruption
 - ☐ c. Identifying essential functions
 - ☐ d. Testing an appropriate emergency response
8. List at least three factors that may affect an organization's choice of risk management strategy.

Match each activity on the right with the risk management strategy on the left that it illustrates.

Risk management strategy	Risk management activity
9. _____ Tolerance	a. Smoke detector
10. _____ Avoidance	b. Business interruption insurance
11. _____ Prevention	c. Choose to ignore
12. _____ Mitigation	d. Equipment for remote work
13. _____ Transfer/share	e. Background personnel checks

14. List at last three operational tactics FM might implement to manage facility risks.

15. Which of the following is an example of preventing technology risks?
- ☐ a. Relocating a facility to an area with a more stable electrical distribution system
 - ☐ b. Installing a backup generator
 - ☐ c. Using cloud computing for off-site storage
 - ☐ d. Restricting access through physical measures to IT equipment



Progress check answers

1. FM must:
 - Understand the type of risks to the facility that may occur.
 - Understand the facility's vulnerabilities.
 - Know the impact of facility damage or interruption in FM processes on organizational functions.
 - Balance the organization's mission against the likelihood of incidents and their possible impact.
(p. 1-161)
2. b. The first step in the risk management process is to identify and assess risks. (p. 1-162)
3. Resources to identify facility risks could include:
 - Government agencies.
 - First responders.
 - Insurers.
 - Facility records.
 - FM colleagues in comparable facilities.
 - Risk management experts. (p. 1-164)
4. d. Risk assessment tools, such as the risk matrix, weigh the probability of risk against its impact. This is useful in prioritizing limited risk management resources. (p. 1-167)
5. c. A mission-essential function is one that, if discontinued for any significant time, could seriously impair an organization's performance of its mission activity. (p. 1-172)
6. d. A BPA outlines the inputs, requirements and outputs of a specific process. (p. 1-174)
7. a. A BIA gathers information about how essential functions are affected by given threats, how quickly they must resume to avoid significant impact to the organization and what will be required to resume activity at an adequate level. (p. 1-176)
8. The following factors can affect choice of risk management strategy:
 - Type of loss
 - Type of hazard
 - Proximity to first responders
 - Number and type of tenants sharing a leased space
 - Impact on mission
 - Budget
 - Building codes
 - Leased or owned facility
 - Confidence in tactic
 - Culture (p. 1-181)
9. c (p. 1-178)
10. e (p. 1-178)
11. a (p. 1-178)
12. d (p. 1-179)
13. b (p. 1-180)



14. Operational tactics that could help FM manage risk include:
 - Inspections by insurers or other experts.
 - Rapid correction of identified risks, such as malfunctions.
 - Maintenance of resources.
 - Staff and occupant training in programs. (p. 1-185)
15. d. Using physical or logical programming measures to restrict access is a way of preventing risks from occurring. (p. 1-186)



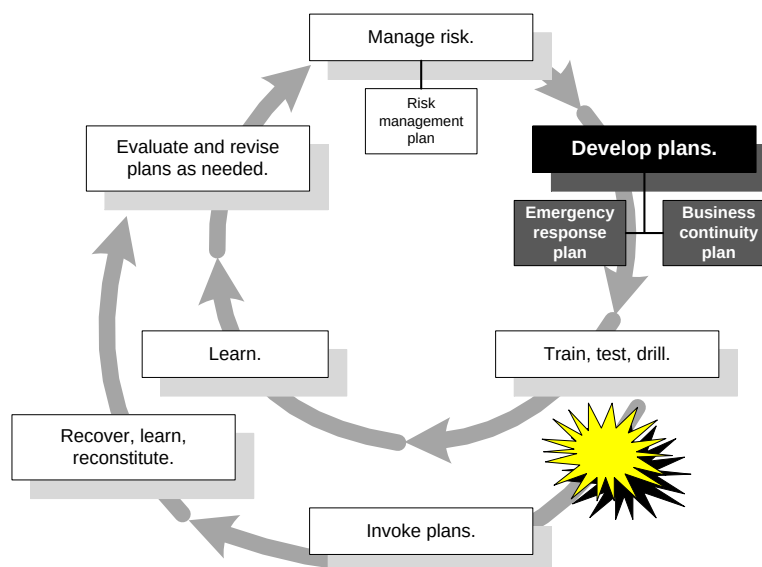
Chapter 3: Develop Plans

After completing this chapter, students will be able to:

- Define key terms in emergency response, such as continuity of operations, chain of command and incident commander.
 - Explain the purpose behind the emergency response concepts of command, coordination and organization.
 - Describe the role of the incident management team.
 - List the components of an emergency response plan and describe their content.
 - Describe ways in which communication during an emergency can be supported and performed effectively.
 - Summarize FM's role in emergency response.
 - Define key terms in business continuity, such as contingency strategy, recovery time and hot site.
 - Provide examples of the range of continuity requirements.
 - Provide examples of ways in which an organization's and FM's vital records can be protected in the event of an emergency or business disruption.
 - List possible components of a business continuity plan and describe their content.
 - Describe activities that take place as part of the plan implementation process.
-

This chapter focuses on the second phase in the emergency preparedness and business continuity model, highlighted in Exhibit 1-55—developing emergency preparedness and business continuity plans.

Exhibit 1-55: Emergency Preparedness and Business Continuity Model—Develop Plans



As described in the emergency narrative in Chapter 1, an effective emergency response includes both the immediate response to the incident and short, medium and long-term actions—crisis management and restoration and recovery.

Achieving a quality emergency response takes planning, however. During this phase of the emergency, the organization's functions work together to define requirements for emergency preparedness, develop answers and institutionalize roles and responsibilities, policies and processes.

This chapter will discuss:

- Emergency management concepts and terms.
- The emergency response plan.
- Business continuity concepts and terms.
- The business continuity plan.
- Implementing plans.

In addition to planning, a quality emergency response will require organizational training, testing of the plans and drilling of occupants and incident response/business continuity team members. These topics will be discussed in the next chapter.

Topic 1: Emergency Management Concepts and Terms

To understand the requirements of the emergency response plan and, more importantly, to communicate more effectively with first responders during an emergency, facility managers should be familiar with some of the methodology and terminology of the emergency management discipline. These ideas and terms were developed by first responders and emergency management agencies to improve the effectiveness of emergency management, from planning to response and post-incident debriefing. Having a common methodology and language makes coordination and communication between facilities and first responders easier, faster and clearer. Incident management teams may also incorporate some of these principles in their own emergency response planning.

A common source of emergency management terminology is the Incident Command System (ICS), which was developed in the U.S. in the 1970s and is now part of the National Incident Management System (NIMS). ICS is defined as follows.

A standardized approach to incident management that:

- Enables a coordinated response among various jurisdictions and agencies.
- Establishes common processes for planning and managing resources.
- Allows for integration of facilities, equipment, personnel, procedures and communications operating within a common organizational structure.



The United Nations has recommended its use as an international standard, and the system is used in different countries. However, facility managers should research their own local emergency management systems and terminology so that they can communicate effectively with their local first responders.

Exhibit 1-56 lists key terms that are often used in discussions of emergency preparedness and will recur in this competency. Many of these terms derive from governmental agencies and reflect formal structures. However, they are meaningful on a facility or organizational level as well. Some key terms are discussed further after the exhibit.

Exhibit 1-56: Emergency Management Terminology (continued on next page)

Term	Definition
After-action report	Document that describes the incident response and findings related to system response performance. The after-action process is also referred to as “lessons learned.”
Chain of command	Series of management positions in order of authority.
Check-in	Process whereby resources first report to an incident. Could include incident command post, camps or staging areas.
Delegation of authority	Statement provided to the incident commander delegating authority and assigning responsibility. The delegation of authority can include objectives, priorities, expectations, constraints and other considerations or guidelines as needed.
Emergency assembly area	Predesignated safe location to which occupants are evacuated and where they can be accounted for, receive essential services and await directions from first responders and emergency response teams.
Emergency operations center	Physical location at which the coordination of information and resources to support incident management activities normally takes place. This may be a temporary facility or may be located in a more central or permanently established facility.
Functions	In ICS includes command, operations, planning, logistics and finance/administration. A sixth function, intelligence, may be established if required to meet management needs. Intelligence ensures that information is handled in a way that not only safeguards the information but also ensures that it gets to those who need access to it to perform their missions effectively and safely.
Incident commander	Individual responsible for all incident activities, including the development of strategies and tactics and the ordering and release of resources. The incident commander has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.
Incident command post	Field location at which the primary tactical level, on-scene incident command functions are performed. The incident command post may be colocated with the incident base or other incident facilities.
Lockdown	Situation in which occupants are directed to lock or barricade themselves into a secure area without glass doors or walls, turn off lights and maintain silence until first responders provide further directions.



Exhibit 1-56: Emergency Management Terminology (concluded)

Term	Definition
Memorandum of understanding (MOU)	Document that describes very broad concepts of mutual understanding of goals and plans shared by parties. An MOU may precede a more detailed memorandum of agreement (MOA) that describes in detail the specific responsibilities of, and actions to be taken by, each of the parties so that their goals can be accomplished.
Shelter in place	Situation in which occupants are directed to stay inside the facility because of unsafe conditions outside the building.
Span of control	Number of individuals a supervisor is responsible for, usually expressed as a ratio of supervisors to individuals. NIMS recommends a span of control between 1:3 and 1:7.
Staging areas	Location established where resources can be placed while awaiting a tactical assignment.
Unity of command	Concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.

Command and coordination

One of the key concepts of emergency management is the command structure. Effective emergency plans address the potential for chaos and disorganization during an emergency by defining and delegating authority for different decisions.

The chain-of-command concept aims at removing confusion and conflict from the activities of order issuing and order taking. The chain of command is a hierarchical structure. Each participant reports to and takes orders from only one supervisor. A clear chain of command ensures that responders will not be receiving possibly conflicting orders from two different supervisors. This is especially important because, during an emergency, a responder may now be reporting to someone other than the person's usual supervisor. It also provides a more controlled communication channel so that commanders do not waste time interpreting possibly redundant or secondhand information.

Although the structure is hierarchical in terms of decisions and orders, it should not discourage the exchange of information between areas and functions. If someone needs information, it should be provided, regardless of whether the request is coming from inside or outside one's chain-of-command structure.



The chain of command reflects levels of decision-making authority:

- Strategic decision making on issues that affect the entire organization. This may be the crisis management team or senior management.
- Tactical decision making on issues regarding the operational aspects of the organization's emergency response plan—in other words, how the strategy will be implemented at a facility level. Tactical decisions are usually made by the emergency or incident management team. This team is discussed further in the next topic.
- Functional or local response on how tactics will be deployed locally. These individuals may be building emergency coordinators, support function leaders or floor wardens.

The incident commander is the person most qualified to handle a particular situation. For example, at a fire the chief officer of the fire department responding will be the incident commander. At a natural disaster, the incident commander may be from an emergency management agency. In ICS, the incident commander performs five management functions:

- Command—setting objectives for the response, creating strategies, defining priorities and assuming overall responsibility for the incident
- Operations—conducting operations on a tactical level to achieve objectives
- Planning—tracking resources, collecting information and maintaining documentation
- Logistics—arranging for resources and services to support response objectives
- Finance and administration—monitoring and analyzing costs, including time, and analyzing processes, such as procurement

Depending on the complexity of the emergency, the incident commander may appoint deputies to perform some of these functions.

Coordination also requires that individuals know where to report during an emergency. This is especially important if individuals are off site when the emergency occurs. Employees and contractors responding to an emergency should check in, at a designated spot such as the command post, so that they can be logged in as present at the site and deployed by command.

The chain of command also defines the order in which authority may devolve to other specific individuals in the leader's absence. It is critical that organizations have layers of trained and knowledgeable managers who can



assume authority when primary leaders are not present or cannot fulfill their responsibilities.

Organization

Emergency management methodology also organizes the resources available to respond to an incident by defining certain spaces and assigning them specific functions. Resources include people and their expertise as well as materials.

An incident command post is a secure location, on- or off-site, from which an incident commander directs emergency response actions. (The incident command post may also be called the emergency operations center or the department operations center.) There is only one incident command post per incident, although it may be relocated if necessary. Some organizations also identify alternate command rooms/assembly stations in the event that the primary location is compromised and inaccessible.

The command post is equipped with tools emergency leaders will need, including communication resources and useful documentation, such as building plans, manuals and catalogs, and lists of occupants with disabilities. All information about the ongoing event should funnel toward the command center. The centers should be large enough to accommodate the number of people likely to be involved in response and immediate recovery. Command centers can incorporate “virtual reality” as well, using videoconferencing and chat rooms to facilitate discussion in global organizations. In fact, in global organizations, the incident command post may be virtual, with communication and coordination occurring through a Web conference or on a Web site.

Did You Know?

The location of the incident command post should be carefully considered. ICS indicates that it should be outside the present and potential hazard zone. So the potential for vulnerability must be weighed when choosing a command post site. Before September 11, 2001, the incident command center for New York was located in 7 World Trade Center—the site of a previous terrorist bomb attack. That building collapsed on the afternoon of September 11 as a result of the terrorist attack that morning on the World Trade Center complex. Its collapse effectively destroyed the city’s emergency operations center as well.

A staging area is designated as a space where resources awaiting deployment can be located. Like the incident command post, the staging area should be in a safe area. However, it needs to be close enough to the incident to allow



rapid delivery of resources to the site. There should be systems to check resources in and out at the staging area. In large facilities there may be multiple staging areas.

An assembly area is a designated location where occupants are instructed to assemble after a facility evacuation. The coordinator in charge of the area takes roll against a list of occupants assigned to that staging area and reports this information to the command center, using a runner if cell or radio communications are unavailable. An orderly assembly area is essential to verifying that all occupants can be accounted for. (In fact, ensuring that occupants are accounted for is a requirement of the U.S. law on workplace safety, the Occupational Safety and Health Act.)

There may be multiple assembly areas, since it will be useful in most emergencies to limit the number of occupants in a single area. The assembly area must also be secure—out of the way of rescue vehicles or, during a storm, under some secure shelter. When conditions are more dangerous outside the facility—for example, during a tornado or civil disturbance—occupants will shelter-in-place inside the facility. When conditions make evacuation more dangerous—for example, when an armed individual is suspected to be inside the facility—a facility lockdown will be ordered and occupants will be advised to find secure areas where they can hide until an all-clear is announced. As the next chapter discusses, occupants must be trained and drilled in these different procedures.

Topic 2: Emergency Response Plan

Emergency response plans describe an organization's continuity of operations plan (COOP)—the way in which the various functions within the organization will act together, in a coordinated fashion, to respond to an emergency from the initial report through response and recovery. Like strategic plans, the organization may require that its component functions, especially support or critical functions, prepare their own plans to describe their specific responses to the most likely emergencies.

Once approved by management, the emergency response plan becomes a guide to how the organization will:

- Prepare for incidents of different types (e.g., supplies and equipment that must be on site).
- Train and educate FM staff and facility occupants about what to do when an incident occurs.



- Respond to incidents of different types.
- Assess the incident and decide next steps.
- Audit and maintain the plan during the plan's lifetime.

The plan itself must be clear and detailed, yet simple and flexible. Designated leaders should be able to assume their roles quickly, but in their absence other individuals should be prepared to take their place. Those involved in leading an emergency response must have a clear sense of the organization's priorities and goals but enough latitude to exert authority to manage unforeseen situations. The speed of response is important in an emergency. A response plan that is complex and requires following a rigid structure of approvals may impede quick action and prevention of subsequent damage.

The plan is the result of senior management commitment to the resources required to develop and implement the plan and the collaboration of a cross-functional organizational team. An effective emergency response plan must have management support because preparation will require budgeting for prevention/mitigation and supplies and the cooperation of all occupants in periodic testing of the plan. Their support must be visible and constant.

Incident management team

An incident management team (or emergency management or response team) is assembled (or "rostered") by a designated leader. The incident management team leader can be any member of the organization but:

- Must be familiar with the facility and its processes and needs.
- Must have the ability to think strategically to solve problems.
- Must be assigned sufficient authority to make necessary business decisions.

Some organizations may adopt ICS and refer to the leader of the incident management team as the organization's incident commander. This reflects the fact that the team leader exerts command and control within the organization over incident-related issues in the same way that an incident commander from an external agency (e.g., fire department chief) would. However, the team leader transfers command to the most qualified responder during an incident. For example, during a fire, the organization's team leader transfers command to the responding fire department until the fire chief/incident commander declares that the incident is over.



The incident management team should be interdisciplinary but should minimally include, besides FM, business unit representatives, internal operations/production, finance/administration, human resources, IT, security and public relations/communication. It may be useful for the team leader to assign specific portfolios to individual team members—for example, communications planning to public relations and human resources and supply ordering and maintenance to administration and accounting. These team members can research and draft portions of the plan and assume responsibility for implementing tasks in those areas during an emergency and for maintaining those sections of the plan over time. For example, human resources could assume responsibility for compiling occupant lists and identifying occupants with disabilities who may require assistance.

The planning team may use consultants or experts in emergency response but should also involve external partners, such as police and fire departments and health, emergency management and environmental agencies. These external partners may provide technical advice, review and comment on plans and conduct or participate in training and exercises or tests of the plan.

Planning in leased facilities

Emergency response planning is still an FM responsibility in leased facilities. In a building with multiple tenants, FM must identify who is responsible for emergency response. This may be the landlord or the municipality. If the landlord is in charge of emergency response, FM should ensure that the building owner has a plan and that the plan is adequate. FM then develops appropriate prevention and mitigation controls that are synchronized and in cooperation with building management and facility neighbors. The facility manager creates and trains facility emergency response teams, ensures that equipment for emergency responses is on hand (e.g., fire extinguishers, CPR equipment) and coordinates with the building owner on drills.

In some cases, no responsible party will be designated. In such a case, FM can coordinate with other tenants and the building owners to ensure an organized and effective emergency response plan. This would include assigning responsibilities for writing the plan, defining command and organization details, developing facility-specific responses to different scenarios or managing automatic notification of occupants.

Plan components

Plans will vary according to a facility's needs, but they generally include those listed in Exhibit 1-57 and described below.



Exhibit 1-57: Emergency Plan Components

Statutes or authority
 Objectives
 Scope
 Situation and assumptions
 Emergency levels
 Command and organization
 Communication
 Drills and training
 Plan maintenance
 Restoration and recovery
 Plan version and distribution control
 Appendices:

- Contact lists for first responders, emergency teams, insurers, vendors/contractors
- Risk management policies
- Emergency scenarios
- Supply lists and supply inspection and maintenance schedule
- Physical plans
- Auditing strategy

- **Statutes or authority.** Applicable laws and regulations with which the organization must comply and which delegate authority for emergency response.
- **Objectives.** The desired outcomes of this planning process. For example:
 - Occupants will know how to recognize and report incidents.
 - Delegated team members will know their responsibilities and locations of emergency areas, such as assembly areas and incident command post.
 - Leaders will apply consistent criteria in escalating the incident.
- **Scope.** Descriptions and addresses of the buildings covered and perhaps explicitly not covered by the plan.
- **Situation and assumptions.** Identified risks to the organization and priorities in response. For example, an organization may state that its priorities are:
 1. Occupant health and safety.
 2. Infrastructure and facilities.
 3. Operations and services.
 4. Supporting local communities.



- **Emergency level designations.** Criteria for assigning different emergency levels. The criteria might use different factors:
 - The extent of the emergency's effect—how much of the facility is affected
 - The severity of impact in terms of fatalities or injuries and damage to property, mission and reputation
 - The length of disruption
 - The response needed to contain the effects of the incident
- **Organization or command structure.** Location of command centers for different levels of incidents and assignment of responsibilities (i.e., strategic, tactical, support). Current contact information should be listed for all team members in an appendix so that they can be reached at any time. This is especially important when critical personnel may be out of the country. Substitute personnel should also be included for key positions.
- **Emergency communication.** Process for reporting incidents internally and externally and notifying occupants, support teams, contractors, occupant families and facility community; emergency communication equipment and services; process to communicate serious injury or death to family members; protocol for communicating with media. Emergency communication is discussed further below.
- **Drills and training.** Training objectives at various levels of involvement, from leaders to occupants; frequency and scope of training and drills; and process for after-action analysis and learning. This topic is discussed further in the next chapter.
- **Plan maintenance.** Schedule and responsibility for reviewing and updating plan components and member contact information. Criteria for immediate review may also be defined, such as acquisition of a new building.
- **Restoration and recovery.** Responsibility and criteria for declaring the incident over and for implementing business continuity plans.
- **Version control and distribution control.** Data about plan copy itself. Plans are dated and assigned version control numbers, which will help ensure that teams are using the most current plan. Some organizations may restrict the distribution of plan copies for security reasons. In this case, the plan will include a process for controlling and tracking access.



- **Appendices.** Additional plan information could include:
 - Contact information for members of incident management teams.
 - Risk management policies related to implementing the plan, such as securing access to the building, ensuring egress from the building or any required checks/replacement of safety equipment or retraining of personnel. Retraining could include ensuring that all facility staff, including new hires, know where shutoff valves are located and what actions to take in emergencies of different types.
 - Protocols and support material for specific emergency scenarios, such as fires or power outages. These protocols are discussed in more detail below.
 - Contact information for insurers, vendors and contractors with whom arrangements have been made to provide support supplies or services, such as security guards, structural engineers, communications specialists, utilities, refuse hauling, cleaning, portable sanitation facilities and so on. Some organizations print this information on wallet-sized cards for emergency team members, so that the information is always available. They may also require that certain numbers be input into team members' mobiles.
 - Inventory lists of emergency supplies. This includes supplies that should always be on hand and should always be functional, such as flashlights and batteries, ready-to-eat food supplies, first aid equipment, tools, fuel, plastic sheeting, cameras to document damage and so on. The location of the supplies and equipment should be clearly described.
 - Schedule and plan to monitor, inspect and replenish emergency supplies. Supplies should be checked periodically and expired supplies replaced.
 - Physical facility plans, such as blueprints, critical equipment registers and BIM files. This information will be critical to first responders.
 - Strategy and schedule for auditing the plan.

A sample emergency response plan is available for learners in the online Resource Center on the Learning System Web site.

Emergency communications

Planning for rapid and effective communication is commonly recognized as an essential and complex ingredient in emergency response. Communication is especially challenging since common means of communication can be vulnerable to different types of threats. Power outages may disable telephone landlines and computer networks, while wind storms and network issues may disable cell communication. Each organization must assess its own communication vulnerabilities and plan accordingly.



Emergency communications plan

Organizations may decide to develop a separate and detailed emergency communications plan. Protocols are developed for specific incidents and describe:

- Target audiences, their information needs and priorities for communicating with these groups.
- Best strategies or channels for communicating (e.g., face-to-face meetings or briefings, phone, e-mail, Web sites, community media, social media, mailings).
- Message content and evolution of the message over time.
- Message review and approval process.
- Monitoring media for reactions.
- Responsibilities for communicating (e.g., designated spokesperson, information officer).
- Necessary supplies (e.g., equipment and services, scripts).
- After-action evaluation methods.

Notifying occupants and visitors

The first priority is in communicating with occupants both inside and away from the facility and with facility visitors. When communicating the existence of an emergency to those inside the facility, emergency team members must be aware of the need to keep occupants and visitors calm but focused on their next steps. Automatic messages sent to phones or announced over speakers should be scripted, and possibly recorded, ahead of time. Team members must also plan for how they will communicate with occupants who cannot receive emergency alerts inside the facility because of where they are working or because of hearing disabilities.

Rather than relying on manual phone calling “trees” to contact occupants outside the facility, many organizations use automated systems, called emergency notification systems (ENS), such as reverse 911 systems, which send automated voice messages (in some instances, prerecorded) to occupants’ home or mobile numbers. Systems are also available that allow emergency text messages to be sent to mobile phones of occupants who have signed on to the service. (Note that in many countries data related to individuals’ personal contact information is considered private and must be safeguarded. Communication systems should include mechanisms to maintain data privacy.) Facilities can also arrange with communication vendors for a call-in number managed off-site. Emergency team leaders can record messages with facility status updates and instructions for occupants and visitors, including information about areas to avoid when returning to the damaged location. Facility Web sites, hosted off-site, can also be used to communicate with occupants and the public.



Communication plans must also consider how to track down and communicate with employees who are temporarily away from the facility—for example, traveling for business or on temporary assignment. This was an issue in the July 7, 2005, London transit bombings, which occurred during commuting hours. How could employees be told to turn around and go home for the day?

Redundant communication systems

Given the fact that incidents can escalate in severity and scope, emergency teams should have redundant means of communicating. For example:

- A hurricane may at first leave landlines intact, allowing communication over conventional phone systems.
- However, winds may increase and power may fail, disabling facility communication systems. Emergency team members may have to turn to mobile phone systems. They must have contact information for both means of communication. If mobile phones are provided as part of an emergency preparedness effort, multiple service providers should be used. If one system goes down, at least some team members can still communicate. Some mobile providers offer push-to-talk-over-cellular phones, which operate like push-to-talk (PTT) radios (or walkie talkies) but over the cellular system. These phones allow rapid connection with a talk group by depressing only one button.
- As the storm worsens, cell towers may be damaged, taking down mobile communication. (Or call volume may increase to a level that makes communication impractical or crashes networks, as happened along the East Coast of the U.S. after the 9/11 attacks or after a small earthquake on the East Coast in 2011.) In this case, the emergency team members could be supplied with PTT radios. The range is not as great as with push-to-talk-over-cellular phones, but it will help keep team members at the incident site in contact when cellular service is down.

Communicating with media

At the same time, some organizations may choose to use the public media—especially facilities that serve the public, such as government agencies or schools. When possible, communication should be made through a brief e-mail or text message, streamed to relevant Web sites through an RSS feed or posted on a social media site.

If a spokesperson is used, it is imperative that a single spokesperson is designated and that this individual is trained in what to say and how to say it. The importance of training spokespeople for their responsibilities cannot be overemphasized. The most common mistake for untrained spokespeople is to say too much to too many



people. It then becomes difficult to correct misinterpretations and rumors. The spokesperson does not have to be the organization's top leader. In most instances, organizations choose as a spokesperson someone who is respected within the organization, familiar with working with the media and knowledgeable about the event. The Centers for Disease Control in the U.S. offers online training in crisis communication at www.bt.cdc.gov/cerc.

There should be no deception in communicating with media, but spokespeople must also not engage in speculation or blame. It is important to remember why the organization is communicating with the public. Generally this is because the organization has public stakeholders who are affected to some degree by the emergency: neighboring residents and businesses, occupant families and friends, local governments, investors, suppliers and customers. Stakeholders' needs should be considered when deciding what and how much detail to discuss in public.

Social media has become a common means of communication and miscommunication. So facility managers in charge of emergency response should assign a team member to scan social media for mention of the facility, review comments and take steps to correct misstatements as needed.

Emergency scenarios

Detailed responses to different types of emergency scenarios can be prepared on a function or area level. These scenarios include:

- What constitutes an incident.
- Whom to contact.
- Criteria for escalating the response from a local level to a tactical level.
- Response priorities (e.g., safe evacuation of all occupants and treatment of injured).
- Response roles and responsibilities (e.g., floor coordinators).
- Response directions (e.g., evacuation procedures, assembly area).
- Recovery criteria (e.g., when it is safe to reenter the building).

Role of FM in emergency response

FM's first responsibility is to prepare response plans for the FM function for different emergency scenarios as described above. The FM emergency response plan might include, for example:

- Staff responsibilities and backup assignments.
- Check-in procedures if staff are off-site.
- Contacts for suppliers and services, such as construction equipment or debris removal.
- Procedures, such as shutting down designated systems or closing fuel lines, cleaning up spills or responding to release of contaminants or hazardous materials.



- Lists of equipment needed and location of equipment.
- Necessary expertise and training and cross-training strategies.

The facility manager will also participate in emergency response and support risk management and preparedness strategies. If it can be avoided, FM should not lead the incident response, since managing this critical support function will require all of the facility manager's attention.

To ensure that the facility is always ready to respond quickly and in a coordinated manner to protect human lives and facility property, facility managers:

- Provide a liaison with management and secure management understanding and support for emergency response planning.
- Ensure that first responders and agencies have current information about buildings and systems and access to secured facility areas.
- Work with insurers to improve risk management and preparedness efforts.
- Coordinate resources and supplies that are required by the plan.
- Ensure that FM emergency team members are trained in their duties.
- Establish a chain of command within FM to ensure that decisions can be made and essential functions (e.g., contracting, payment for emergency fuel or services) can continue.
- Support evacuation drills.
- Initiate and monitor necessary preventive maintenance activities for the emergency response system, such as restocking supplies inventories and updating prerecorded messages.

✦ Topic 3: Business Continuity Concepts and Terms

One of the possible outcomes of emergency response is the activation of the organization's business continuity plans. Once immediate threats to humans and physical assets have been contained, the organization must immediately turn its attention to the future. The purpose of business continuity is to ensure that critical processes either continue during or resume quickly after an emergency so that the organization can return to normal in the shortest possible time frame. Business continuity planning is a best practice for organizations, and, for some organizations, it is required by law.

As with the emergency response process, business continuity must be aligned with the organization's strategy. Continuity efforts focus on functions that are essential to the organization's mission and/or strategy. For example, one aspect



of a bank's strategy may be to avoid fines and penalties resulting from noncompliance with local banking regulations. It therefore becomes essential for the bank to identify all those processes that could be interrupted by incidents and the conditions that would elicit regulatory actions.

Because of the strategic significance of the business continuity plan and because management must allocate budget for contingency measures, the business continuity planning process must have the commitment and support of senior management.

With management's support, the concept of business continuity can become part of the organization's culture:

- Formal statements of strategy should refer to business continuity planning and reinforce its objectives.
- Contingency operations can be transposed into formal standard operating procedures (SOPs) that are mandatory throughout the organization and that must be performed in a uniform manner.
- The roles and responsibilities described in the SOPs become part of performance expectations for the organization's members and provide the rationale for business continuity training.

Organizations can use experts in business continuity planning to consult on strategies and lead the planning process. However, managers of essential functions as well as FM, finances, legal, IT and human resources should be involved in the planning process.

This topic will focus on the concept of contingency planning and specific challenges in business continuity.

Developing contingency strategies

During the business impact analysis process, which was discussed in Chapter 2, the organization agreed about the minimal acceptable level of performance for the function and how long the function can be suspended without irreparable harm to the organization. A recovery time objective was defined. Contingency planning will help the organization accomplish that objective.

FM will be directly and indirectly involved in planning and implementing contingencies—identifying potential temporary facilities and interviewing landlords, making arrangements with suppliers of services and equipment, and arranging for storage and transportation of redundant equipment and supplies.



Continuity requirements analysis

The next task is to understand what those essential functions need to continue or to resume minimal operations by the agreed recovery time. Business continuity planners can then work with department managers and supervisors to identify specific continuity requirements, referring to the business process analysis for the essential functions as a guide. Discussions should focus on both tangible requirements, such as supplies, and intangible needs, such as authority to make certain kinds of decisions.

Requirements should be essential, not ideal. For example, it would be ideal to have a computer system in the temporary or backup office to record transactions, but if the volume of transactions is low, the process could probably be performed manually.

Primary requirements could include items such as:

- A certain number of personnel with specific knowledge and skills.
- Equipment, supplies and material required to perform the function.
- Adequate workspace for the required number of personnel and amount of equipment/material. The work space should be clean, healthful and safe.
- Financial support (e.g., payment of suppliers).
- Information and vital records.

Secondary requirements, in support of the primary requirements, could include:

- Temporary lodging for personnel and per diem living expenses.
- Providing meals and beverages.
- Transportation for employees to and from the temporary location.
- Parking arrangements.
- Arrangements with suppliers and repair vendors to include standing delivery/maintenance contracts, such as delivery of fuel for backup generators.
- Power and voice/data communication.
- Mail and shipping services to and from the temporary location, including forwarded mail from the primary facility.
- Facility management services to maintain the temporary location.

Contingency strategies

Contingent arrangements must be made for workspaces, employees, equipment and supplies, and services.

Contingent workplaces (also known as secondary sites or business continuity backup sites)

The choice of an alternative workspace will depend on a function's requirements, how essential it is to the organization, how quickly the function



must resume and how difficult it may be to find a substitute space. For example, a bank that must continue monetary transactions and will suffer compliance fines and loss of future business if it cannot continue completing, monitoring and reporting transactions may need to arrange a hot site. A hot site is a workspace that is completely ready to be occupied and used. All necessary equipment and furnishings are on-site, cabling is in place and services can be turned on immediately. If the space is never used, the expense is seen as a form of insurance against business interruption, worth the possible costs of not being able to continue the functions.

Alternatively, an organization may choose a cold site for an activity that is essential but can be resumed within a week. A cold site does not include furnishings or equipment but can be made ready in a relatively short amount of time. An empty space is leased, and contracts are created with service providers and vendors to equip the space by the required recovery point once the signal is given.

Some organizations may maintain warm sites. A warm site is partially prepared for use (e.g., cabling, lighting, phones and desks are in place) and can be brought online relatively quickly by adding specialized equipment and delivering supplies needed to perform the function. A warm site might also be a flexible space that can be quickly converted to serve the essential function. When it is not being used for an essential function, it can serve as storage or temporary office space.

Did You Know?

Large multinational corporations frequently contract with hotel chains to provide temporary workspaces utilizing rooms, meeting rooms and conference space. The hotels have food, water, emergency power and security staff—all critical elements in an emergency.

Other alternatives are possible as well, depending on the nature and needs of the function that must be continued. Employees can work from home or remotely. Employees in affected functions can be provided with mobile kits that include laptops and cellular or satellite communication devices. Some buildings offer “virtual offices” that provide different levels of service, from mail forwarding and telephone answering to conference rooms and desks.



Areas in the facility—or other buildings in a multibuilding facility or other facilities in a global organization—that are used for less essential functions may be repurposed for another, more critical function. This is an especially attractive strategy if the functions use similar equipment and numbers of employees. Another option may be to establish a memorandum of agreement (MOA) with another organization. An MOA is a reciprocal agreement to provide each other a specific amount of workspace if an emergency disables one of the facilities. Organizations may also pool their resources to establish and maintain common contingency workspaces. However, collaborating organizations must ensure that the needs of all participating organizations can be accommodated in case of a widespread emergency. The International Association of Emergency Managers offers an MOA template on its Web site, www.iaem.com.

Contingent workforce

Some emergencies may directly affect the availability of trained workers—for example, pandemic illnesses or transportation disruptions. Plans may specify the transfer of essential functions to unaffected facilities performing the same function. Or the plan may involve cross-training workers so that employees in nonessential functions can replace temporarily unavailable employees. Arrangements can also be made with available employees to work overtime or for retired employees to return to work temporarily. Temporary labor agencies can agree to provide certain numbers of workers with certain skills when notified.

Contingent equipment and services

In a similar manner, the equipment needed to perform the essential function must be purchased and stored (full redundancy) for later use or similar equipment can be reassigned to the essential function until the facility fully recovers. Facility managers can also contract with vendors to deliver necessary equipment, materials and/or supplies within a specific time frame if the business continuity plan is activated. The same approach can be taken with services, such as voice/data communication. Having the agreements fully executed before the emergency ensures that the agreements can be quickly fulfilled when needed.

Outsourcing as a contingency strategy

An organization may determine that the best strategy for continuity of a certain function may be to outsource the activity. However, outsourcing to ensure business continuity does not relieve the organization of all business continuity concerns. Function leaders must perform due diligence to ensure that suppliers



Data and document continuity

and contractors have the means to carry out the essential process within the required parameters—both the necessary equipment and trained staff. They may want to see the supplier's or contractor's own business continuity plans.

Business continuity must ensure that there is no loss of data as a result of an incident, that data is gathered and stored and continues to be available to functions during the interruption. This includes online (both Internet and intranet) database systems and applications, such as payroll and purchasing.

Off-site, continuous backup of essential data and storage of archived data is part of an organization's mitigation program. FEMA recommends a formal vital records program in which:

- Records about emergency response and business continuity are identified and protected.
- Records necessary to continued operations and to remain in compliance with laws and regulations are identified and protected.
- The process of protecting vital records is formalized as a business continuity process, with a responsible leader and approved policies and procedures.
- The organization has access to online and/or hard copies of documents and to e-mail within 12 hours.
- Redundant media are used to back up vital records.
- The inventory of vital records is kept current.
- A risk analysis is performed of records and databases.
- A vital records packet is developed and maintained. This packet includes location and access rights to stored documents, records inventory, equipment needed to access records and names of record-recovery experts.

FEMA recommends annual review and testing of the vital records program.

On a facility level, FM can work with IT to identify the most efficient ways to back up facility system data. Services are available to use the Internet to “save to the cloud,” saving data and applications to servers that may be located anywhere in the world. IT can help perform due diligence to ensure the security of these services.

It is the facility manager's job to plan what data related to facility management and operations should be backed up and on what schedule. Managers should work with staff to identify what stored data is accessed on a regular basis and must be available after an emergency—for example, baseline performance data or maintenance and repair histories. Staff can then be trained in how to access this data.



Managers involved in business continuity planning should remember that data backup, performed by the organization or through a subscription service, can be expensive. They should consider carefully the volume of data that needs to be backed up and the frequency of backup.

Facility managers must also identify documentation that must be preserved in case the facility itself is lost. Essential facility documents could include:

- Copies of insurance contracts.
- Building as-built drawings.
- Leases.
- Invoices and payments.
- Warranties and service contracts.
- Service histories that could be used to support valuation of facility equipment.
- Employee files, if files separate from human resources are maintained.
- Access card data, which will be critical in determining who was and was not in the building at the time of the event and whether occupants have been lost.
- Essential correspondence.
- Records of meetings.
- Any equipment information that could not be retrieved from the Internet.
- Copies of the master document index.

Facility managers can check with legal departments about local requirements for original document retention. Some documents might be scanned into electronic files and stored with backup data.

Reconstitution or returning to normal operations

The organization and FM must also plan for how functions will transition back to the facility when it is again operable. The following issues and tasks must be addressed:

- The conditions considered acceptable for return of the function(s). These should be mutually agreed by the function leaders, facility management and senior management.
- How the decision will be communicated to leaders and affected employees.
- How the functions will be returned: at once or in stages.
- What preparations must be made to return equipment, supplies and documents.
- What services must be terminated.



✦ Topic 4: Business Continuity Plan

The input for the business continuity process is the information contained in the business impact analysis (BIA). The BIA helps establish priorities and objectives for recovery of essential functions. The output of the process is the business continuity plan. There may be multiple plans, one for each essential function that must be continued or resumed quickly. Plans may be activated in stages if a facility continues to be inaccessible for longer than expected.

The Business Continuity Institute defines a business continuity plan as:

A document containing the recovery timeline methodology, test-validated documentation, procedures, and action instructions developed specifically for use in restoring organization operations in the event of a declared disaster. To be effective, most business continuity plans also require testing, skilled personnel, access to vital records, and alternate recovery resources including facilities.

Exhibit 1-58 lists common components of business continuity plans. The components are described in the text following the exhibit.

Exhibit 1-58: Business Continuity Plan Components

- Conditions for activating the plan
- Assumptions: priorities, discontinued activities, continuity objectives
- Requirements for continuity (workers, facilities and equipment/supplies)
- Contingency operation plans
 - Objectives
 - Roles and responsibilities
 - Communication plans
 - Activating the contingency processes
 - Return to the facility
- Process for reconstitution
- Continuity of data operations and organizational documentation
- Training
- Plan evaluation and audit

Most plans include descriptions of:

- The conditions that will trigger the activation of the plan (e.g., estimated loss of access to the facility or loss of power for more than three days).
- Priorities that dictate which functions will be resumed and the order of resumption and which functions may be temporarily suspended or performed only if possible without continuance resources (e.g., vendor delivery of



supplies, training activities not related to the emergency, activities in a building not affected by the incident). The plan should describe when discontinued processes should be resumed.

- Requirements for resuming the function, in terms of workers, facilities and equipment/supplies.
- Contingency operation plans:
 - Objectives.
 - Roles and responsibilities. An emergency that calls for business continuity plans to be activated may disrupt both the facility and normal leadership roles. The plans should indicate those responsible for implementing the transfer of the essential function to its temporary location and for making decisions during the transition and relocation period. Plans should specify alternates to whom the authority to lead and make decisions would devolve if necessary.
 - Communication plans—how the activation decision will be communicated and communication will be maintained during the relocation.
 - Roles, responsibilities, authority and procedures to activate the contingency processes.
 - Moving the processes back into the facility when the disruption is over.
- The process for reconstitution.
- Providing for continuity of data operations and organizational documentation.
- Training.
- Plan evaluation and audit.

Topic 5: Implementing Plans

Once the emergency response and business continuity plans have been drafted, they should be presented to management for review and approval. When they have been approved and signed off on by management, the teams and functions, including FM, can begin the process of integrating the plans into the organization's and functions' policies and procedures and into their culture. Copies of plans should be distributed to all members who may need access to the information. Additional copies should be kept in secure and separate locations (e.g., managers' homes, insurers' offices, local emergency responders) in case the facility is inaccessible.

Specific policies and standard procedures may have to be created, reviewed and implemented. Existing policies and procedures should be reviewed and revised to include issues related to emergency preparedness and business



continuity. Job descriptions should be reviewed and revised to include emergency response responsibilities and qualifications.

Functions must prepare to perform their own responsibilities. For example, HR must develop a way to compile lists of occupants assigned to specific staging areas that can be updated automatically. Home contact information must be entered into emergency messaging systems. FM and IT will work to improve data center resiliency by adding redundant systems. FM may begin to implement the arrangements described in the business continuity plans—e.g., working with realtors to identify contingency locations, securing redundant equipment, identifying and securing essential documents. Necessary resources and services can be procured. Review of contracts by the organization's attorney is recommended to ensure that the contract achieves its primary goal: the on-time delivery of specific services or supplies at an agreed amount and level of quality.

General features of the plan should be introduced to occupants through the variety of communication vehicles available—organization-wide and departmental meetings, newsletters, e-mails, Web sites, facility Twitter feeds. Training plans should be announced. Communication should stress the benefits the facility and its occupants will receive from this investment of time and resources.

Training and plan testing will be key activities during implementation of plans. This topic will be addressed in the next chapter.

Drive-away kits

Those responsible for continuing essential functions must also be equipped with the tools they will need if the facility is unavailable and business continuity plans are activated. These are commonly called drive-away kits. These kits contain equipment, information and supplies necessary for the performance of the essential function. This may include:

- Hard copy of the business continuity plan.
- Hard copy of the emergency response and business continuity team contacts.
- Hard copy of succession documents or delegations of authority, if used.
- A plan for the employee (i.e., where the employee is “driving away” to), which may be a condensed version of the business continuity plan, including only the key information the employee will need, such as a description of transportation options to reach the business continuity site in the event that mass transit and highways are disrupted.



- Critical internal/external contacts (e.g., finance, realtors, suppliers).
- Hard-copy phone lists of employees and vendors.
- Computer and communication equipment. (Computers should be loaded with necessary applications and files. Phones should operate in the applicable geographic regions.)
- Temporary work supplies, including items such as flash drives or wireless cards, backup computer and phone batteries, stationery, white boards.
- Emergency response supplies, such as a hard hat, a two-way radio, a flashlight/torch and high-visibility clothing.
- Personal supplies (e.g., toiletries, small amount of cash, credit card).

Organizations may also implement requirements that employees are “emergency-ready” at all times—for example, that they take laptop computers home with them if they will be working off-site as the result of an emergency or that they will have access to required supplies if the facility is inaccessible. Organizations should also encourage their members to ensure that their families have emergency plans as well—planning for locating and communicating with each other if members are away from home and for surviving at home for three days after a disaster strikes (e.g., having sufficient food and water, wind-up or battery-powered radios, batteries, flashlights, pet food).

✦ Topic 6: Emergency Preparedness/Business Continuity Case Study

This topic continues following the experiences of the fictional software development company LGH-EMS as it develops its emergency response and business continuity plans.

Emergency Preparedness and Business Continuity Case Study (continued)

LGH-EMS had an interesting situation. Although the parent organization had taken a very proactive approach to emergency preparedness and business continuity, division senior managers and line managers were not very interested in the issue. The division business manager planned a campaign to involve them more and win their active support. He invited the LGH-EMS CEO to attend a readiness exercise at another facility that was further along in the process and could offer some examples of how planning has already helped them.



The business manager succeeded in rostering an emergency response team. The members worked on their separate responsibilities:

- The facility manager developed lists of supplies to be purchased to support evacuation of the facility and assessed the emergency response equipment on hand. CPR equipment was installed in additional locations. The facility manager also invited the community's first responders to become more familiar with the facility and discussed how they could work together.
- The security manager worked up logical evacuation routes and staging areas.
- Human resources began to assemble occupancy lists and research communication systems that could be used to contact employees away from the facility. HR also assumed the tasks of leading the training effort and incorporating emergency response tasks into job descriptions and performance reviews.
- Senior management, the finance director and the facilities director negotiated decision-making powers and set an annual emergency response budget.

At the same time, LGH-EMS senior management and function leaders began a series of workshops to develop business continuity plans. The team decided that, of its functions considered essential, the most problematic were customer support and certain design/programming teams. Marketing could work from remote locations, but customer support needed to be together in order to share knowledge and experience of products. They needed to be able to access the systems and IT support people throughout the day and connect them into customer calls. They also needed to be able to access customer relations databases. Management indicated that any outage of customer service that exceeded an hour would be unacceptable. Design and programming teams for products on a tight schedule could be reassigned space with other teams, who could work from home and come into the office for team meetings, or relocated if the facility was not available. They would, however, need remote access to the function's data and applications.

These functions decided to recommend the following steps to management. In the event that the facility was unavailable, about 80 percent of customer service could be moved into the administrative offices of a nearby office building. In exchange, the office building would be able to use offices in the LGH-EMS building in an emergency. Customer support representatives would be gradually moved to laptops, and a virtual private network would be installed that would allow all employees to access data and applications remotely.

A procedure was developed and the technology tested at the partnering facility. The plan would be activated if the customer service operation area was reduced by one-third. FM would call the customer service supervisor, who would initiate an automatic calling system to employees. (Since only 80 percent of employees could report, schedules were created to rotate personnel through an abbreviated work schedule. Employees were assured that they would be paid for a full week.) FM would also contact the partnering facility. Management reviewed and approved the cost of the equipment. IT assumed responsibility for training the customer service personnel. Personnel were instructed to take their laptops home every night.



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. Which of the following best describes the role of the incident commander?
 - ☐ a. Best equipped to manage the type of incident that has occurred
 - ☐ b. Drafts the emergency response plan
 - ☐ c. Most senior in the organization serving on the incident management team
 - ☐ d. Deals directly with first responders

2. A building technician reacts to an occupant's direction to shut off a ventilation system by first confirming this action with the facility manager. This is an example of
 - ☐ a. transfer of authority.
 - ☐ b. chain of command.
 - ☐ c. span of control.
 - ☐ d. unity of command.

3. Which of the following statements about assembly areas is correct?
 - ☐ a. A coordinator must be assigned to each assembly area.
 - ☐ b. Assembly areas are necessary only when occupancy exceeds a certain level set by first responders.
 - ☐ c. Areas should be equipped with computers and communication systems.
 - ☐ d. The assembly area is the place where decisions are made about activating the business continuity plan or declaring the emergency over.

4. The continuity of operations plan is
 - ☐ a. a narrative description of how a facility will respond to a given emergency.
 - ☐ b. the goal the organization wishes to achieve in its emergency response actions.
 - ☐ c. documentation of the emergency response plan's effectiveness.
 - ☐ d. a description of the limits to which the organization will act to preserve assets.

5. Which of the following statements about the incident management team is correct?
 - ☐ a. The team leader is always from the community's first responders team.
 - ☐ b. Senior management must be included.
 - ☐ c. Teams should be interdisciplinary.
 - ☐ d. Current membership does not need to be listed in the plan, only the number of members and the leader's name.

6. List at least five components of an emergency response plan.



7. Which of the following statements about emergency communications is correct?

- ☐ a. The most effective plans use two-way radios.
- ☐ b. The spokesperson should be the incident commander.
- ☐ c. Organizations should use redundant communication equipment.
- ☐ d. Information should be released sparingly.

8. List at least three examples of information included in the FM emergency response plan.

9. List at least three ways in which a business continuity mindset can become part of an organization's culture.

10. Which of the following statements about a continuity requirements analysis is correct?

- ☐ a. Analyses should be performed by professional business continuity consultants.
- ☐ b. Lists of requirements should focus on essential, not usual, process inputs.
- ☐ c. Business continuity requirements should parallel requirements under ideal conditions.
- ☐ d. Only tangible needs should be included in planning.

11. A bank operates a parallel but unoccupied workspace with equipment identical to that in the transactions processing area and with the same network connections so that, during an emergency, the staff of this area can simply move to the alternative workspace and resume their jobs. What contingency strategy is the bank using?

- ☐ a. Cold site
- ☐ b. Warm site
- ☐ c. Hot site
- ☐ d. Memorandum of understanding

12. According to the Business Continuity Institute, a business continuity plan should include which of the following elements? (Choose two.)

- ☐ a. Contingency budgets
- ☐ b. Estimate of cost of business interruption
- ☐ c. Recovery timeline for designated function
- ☐ d. Validated procedures for resuming operations



Progress check answers

1. a. The incident commander is the person who is best equipped to handle a specific emergency—for example, a fire department chief or a manager from an emergency management agency. (p. 1-198)
2. d. Unity of command trains an organization to recognize that each person involved in responding to an incident should receive and follow orders from only one superior. (p. 1-199)
3. a. An assembly area need have only a coordinator to check that all occupants assigned to that area are accounted for, to maintain order and keep the assembled occupants safe and to provide status information to the command center (by cell phone, radio or runner). (p. 1-202)
4. a. The continuity of operations plan describes how the facility will handle an emergency from beginning to end. (p. 1-202)
5. c. Teams should be interdisciplinary, with representatives from business units, FM, HR, IT and finance. (p. 1-204)
6. Emergency response plans can include authority, objectives, scope, situation and assumptions, emergency level designations, organization or command structure, communication, drills and training, plan maintenance, restoration and recovery, version control and various appendices (contact lists, inventories, procedures for specific incidents). (p. 1-204)
7. c. Because incidents can vary and escalate, organizations should plan by having redundant communications systems for team members. (p. 1-209)
8. FM emergency response plans might include:
 - Staff responsibilities and backup assignments.
 - Check-in procedures during emergencies.
 - Contacts for suppliers and services.
 - Procedures to shut down or secure facility systems.
 - Necessary equipment and supplies to be ready.
 - Necessary expertise and training strategies. (p. 1-210)
9. Organizations can institutionalize business continuity concepts by:
 - Including business continuity planning in strategy statements.
 - Reflecting contingency operations in SOPs.
 - Incorporating responsibilities into performance reviews. (p. 1-212)
10. b. Requirements for a contingency plan should focus on essential rather than usual or ideal needs for performing the function. The needs may be intangible as well as tangible, including decision-making authority. (p. 1-213)
11. c. The bank has created a hot site that is ready for immediate occupancy and use. (p. 1-214)
12. c and d. The Business Continuity Institute definition of a plan emphasizes the need for a recovery timeline and test-validated methodology for resuming operations (e.g., essential documents, instructions, procedures). (p. 1-218)



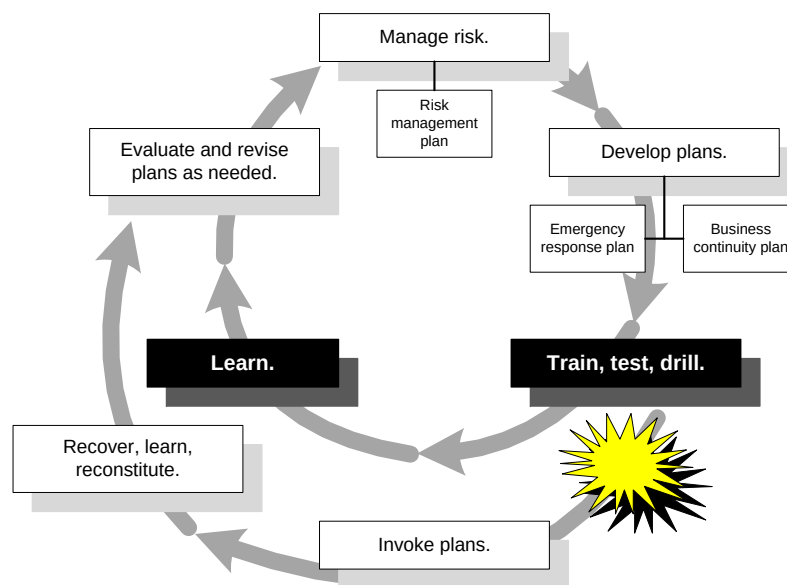
Chapter 4: Train, Test and Drill

After completing this chapter, students will be able to:

- Explain the need for emergency preparedness and business continuity training and testing.
 - Provide examples of training challenges.
 - List basic types of training and testing vehicles and their uses.
 - Explain the importance of debriefing tests.
 - Describe strategies for improving the effectiveness of drills.
-

This chapter focuses on the next phase of the emergency preparedness and business continuity model—training, testing and drilling team members and occupants in plan roles and procedures. It also includes learning from every test and drill to improve the organization’s preparedness and resiliency.

Exhibit 1-59: Emergency Preparedness and Business Continuity Model—Train, Test, Drill



Once plans have been approved, organizations must ensure that the plans are effective and that they can be implemented in the event of an emergency. This chapter focuses on:

- Training/testing strategies.
- Conducting drills.



✦ Topic 1: Training/Testing Strategies

Need for training and testing

Organizations must ensure that all occupants know how to respond in the event of an emergency—whether they are incident response team members, support team members responsible for leading evacuations or performing critical procedures, or occupants and visitors who must be able to evacuate the building in a calm and safe manner. Crisis management teams must be able to make quick but sound decisions. Those involved in business continuity plans must understand how they are expected to continue their work if the facility is inaccessible. Knowledge, however, is not sufficient. The knowledge must be tested and practiced in drills and exercises.

Plans must also be tested to ensure that they meet their objectives, which could include:

- Protection of life, assets and the environment.
- Continuation of essential processes without interruption.
- Resumption of certain processes within defined recovery times and performance levels.
- Efficient use of organizational resources.

Emergency response plans must be tested to ensure that:

- Incident team members can perform their responsibilities quickly, even under pressure.
- Incident teams can coordinate effectively with first responders and meet all their information needs.
- Procedures are clear, correct and possible.
- Procedures address all needs in a given scenario.
- Projected resources and systems are adequate.
- Required supplies are in place.
- Support teams can perform their functions in required time frames and at required levels (e.g., total evacuation of occupants within 10 minutes, rostering of occupants within 30 minutes, facility systems shutdown within 20 minutes).

Testing of business continuity plans is also essential to:

- Ensure that all interdependencies of functions have been identified and planned for. It will be of little help to the organization to provide for continuance of a customer service function if the customer service representatives cannot perform transactions.
- Verify the accuracy and completeness of the functions' list of requirements.



- Ensure that recovery time and performance level objectives can be met for essential processes.
- Validate continuity procedures, resources, and roles and responsibilities (e.g., access to the contingency site and equipment; communication with utilities, landlords, employees, customers).
- Identify potential competition by multiple functions for the same resources.
- Verify that suppliers and vendors can deliver as promised.

Training/testing programs

Emergency preparedness and business continuity training and testing can occur at all levels in an organization:

- There can be facilitywide evacuation drills and simulations.
- Incident response team leaders can test and practice planned procedures and resource availability and deployment.
- Departments or functions can review and practice contingency plans.
- Individuals may be trained in delivering first aid or operating specific types of equipment. Facility staff may be trained in how to take down and bring up building systems.

Senior management, the incident response and business continuity teams and function leaders must decide who will be trained, who will deliver training, what type of training will be most effective for the subject matter, and where training should occur to be simultaneously most effective and least disruptive to occupant productivity.

Objectives can focus on both training and testing:

- Knowledge of plans and procedures and ability to perform responsibilities
- Performance of critical plan components under simulated conditions, such as the effectiveness of communication systems or backup IT systems in an emergency

The organization must also establish a procedure to document completion of training, and the training itself must be evaluated to ensure that it is achieving its goal of increasing occupant and facility preparedness. Performance on testing objectives should be documented and discussed and a performance improvement plan developed.

Training/testing needs assessment

Training for emergency preparedness and business continuity should be designed to meet the needs of the organization and the content. It should also be viewed as a cohesive program rather than separate training events.



Those responsible for ensuring that participants and occupants are trained must therefore consider the following factors:

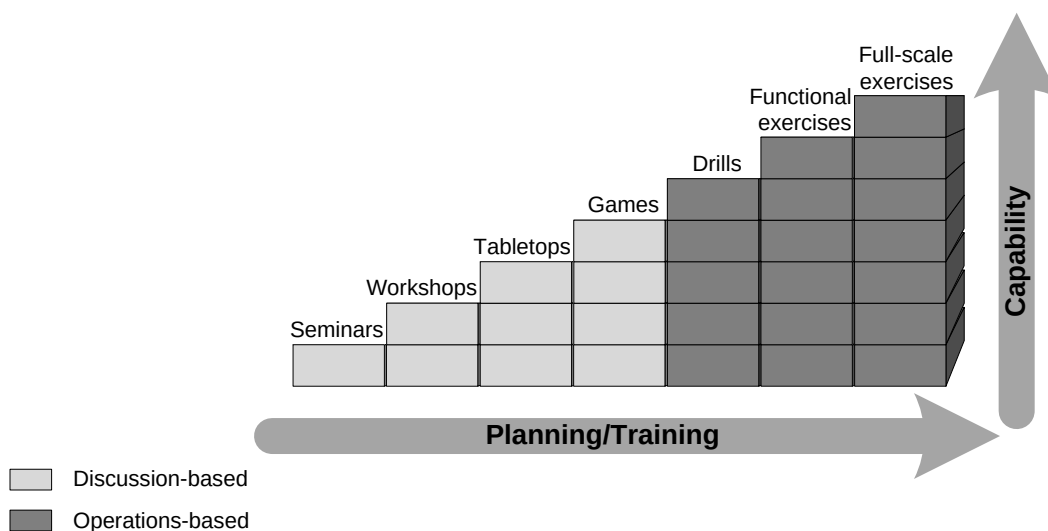
- Leaders' and occupants' familiarity with existing plans
- Rate of turnover among occupants and the average number of visitors to the facility
- Effectiveness of previous training
- Training intervals (When did the last training event occur?)
- External requirements for training (e.g., from insurers and local governments/agencies)

The training picture is complicated, and management should periodically undertake a training assessment of emergency preparedness and business continuity to establish what occupants need to know, where gaps may exist and how they should be addressed.

Training/testing design and vehicles

Training/testing vehicles range in depth and complexity, depending on the targeted learners' objectives. The U.S. Homeland Security Exercise and Evaluation Program (HSEEP) prescribes a building-block approach that matches delivery method with the complexity of learning content and the desired learner performance. This capabilities-focused approach to training is shown in Exhibit 1-60. Each method will be discussed below.

Exhibit 1-60: Capabilities-Based Learning



Source: "Homeland Security Exercise and Evaluation Program (HSEEP)." U.S. Department of Homeland Security, February 2007. hseep.dhs.gov/pages/1001_HSEEP7.aspx.



The exhibit describes training tools in terms of two essential characteristics of training:

- Planning/training—the amount of resources spent to develop and implement the training event
- Capability—the level of competency the learner will be able to demonstrate after receiving training, which can range from simple knowledge to the ability to make decisions and solve complex problems

Discussion-based learning events are focused primarily on acquiring and applying knowledge of emergency preparedness and business continuity concepts. At the end, learners can demonstrate what they know—to repeat or paraphrase key information, to recognize how the concept may apply to the real world. These vehicles include seminars or presentations, workshops, tabletop exercises and games.

Operations-based learning events require both mental and physical actions, usually in the actual environment. At the end, learners show that they understand by applying what they know in a simulated real-world setting. Training may occur on a functional or whole-facility level. This training may be more challenging, because it requires judgment and decision-making ability. These vehicles include drills, functional exercises and full-scale exercises.

Many of the training methods are also means of testing the plans, policies and procedures, and adequacy of resources. Plans can be analyzed and adjusted through workshops, tabletop exercises, drills and functional exercises without the expense of a full-scale exercise. The full-scale exercise can test the plan and the teams' and occupants' readiness and identify problems to avoid injury, fatalities and property losses before a genuine emergency arises. Some organizations require periodic plan “invocation” tests, during which plans are tested under controlled, supervised conditions.

This approach provides the training needed for different levels of involvement in emergency preparedness and business continuity:

- Seminars may be appropriate for occupants not directly involved in procedures, and visitors may receive only the initial level of training. Emergency team members can attend regular department meetings to review emergency response protocols and answer questions.
- Functions can attend workshops to develop specific procedures. For example, FM can identify shutdown needs and assign roles and responsibilities.
- Incident response or business continuity teams can exercise their individual roles and test plan components in tabletop exercises.



- Team leaders can test specific components of plans through drills, simulating the actions they would take if specific types of emergencies were announced. For example, the shelter-in-place plan can be tested to ensure that the designated space is adequate.
- Team leaders can test their own skills and their plans through team function or full-scale facility exercises. A full-scale exercise can combine occupants and first responders.

All of these vehicles are useful but with different audiences and for different purposes.

Organizations can work with local emergency management organizations or consultants to develop appropriate training and tests, including scenarios that are both realistic and challenging.

Exhibit 1-61 on the next page briefly describes these training vehicles, their approximate lengths and their particular uses.

Special training considerations

A strategy must be developed to ensure that visitors and occupants hired after a regular training session are trained. Some facilities may require contractors working on site to review and initial a summary of emergency procedures. A packet of basic emergency information may be included in new-hire packets and emergency topics included in department orientations.

In those cases in which occupants and visitors are difficult to train—for example, hotel guests, students in a university building, visitors to a museum—the emergency team must ensure that team members are trained in how to facilitate an orderly and thorough evacuation and that signage is used effectively to communicate evacuation routes and procedures.

Debriefing testing

Every testing event is an opportunity to improve performance but only if the crisis management, incident management and support teams take the time to review their experiences. A formal debriefing should be a required component of tests. Debriefing might focus on:

- Assessing what went well and what could be improved.
- Assessing command effectiveness and coordination among functions.
- Sharing team member observations of how participants responded.
- Identifying and correcting individuals' performance gaps.
- Identifying ineffectiveness and inefficiencies in response procedures and contingency plans.
- Assessing adequacy of resources (e.g., spaces, staff, supplies, equipment).



Exhibit 1-61: Learning Vehicle Characteristics

Vehicle	Length	Training Use
Seminars • Use lecture, slide presentation, panel discussion. • Feature limited learner interaction, perhaps question/answer. • Will accommodate larger groups.	One to two hours	Create awareness of concepts and benefits of emergency preparedness and business continuity. Overview concepts, plans, policies and procedures. Ensure uniform message.
Workshops • Aim at increased participant interaction. • Focused on defined output, such as new process, specific problem solution and lists of risk scenarios. • Can be larger groups with small group breakouts.	Two to four hours	Share perspectives and expertise to create consensus and/or develop solutions. Build teamwork. Test ideas.
Tabletop exercises • Leaders implement responses in a scenario according to plan. In advanced exercises, additional information and/or challenges are introduced throughout the exercise. • Smaller or breakout groups are used. • Do not occur in real time but are usually held around a conference table. • Discussion is encouraged. • No actual occupants or resources are involved.	Four to eight hours	Validate plans and specific procedures. Identify gaps, conflicts. Increase participants' understanding of concepts. Exercise decision-making skills. Motivate. Change attitudes.
Games • Competitive structure is used. • Direction of play is driven by player decisions. • Players receive immediate feedback. • Stress can be simulated by shortening decision times.	Two to five hours	Practice decision making, including group decision making. Improve understanding of complex processes and outcomes. Build teamwork.
Drills • Focus is on single operation. • Leaders and occupants perform actions in real time on site. • Feedback is provided.	Two to four hours	Validate single operation, such as facility evacuation or response to chemical spill. Assess reaction times. Familiarize participants with actual experience.
Functional exercises • Leaders respond to hypothetical incident (with complications) in real time. • Occupant involvement and use of resources is simulated.	Half day to several days	Validate capabilities and coordination of functions. Exercise leaders of emergency response functions.
Full-scale exercises • All leaders, functions, occupants participate in real time on site. • Simulated threat is presented, often with additional complications. • Participants respond as they would in actual situation. • Actual resources are used.	At least one day	Validate all elements of plans: • Interfunctional coordination • Adequacy of resources, preparation, training



✦ Topic 2: Conducting Drills

Did You Know?

Evacuation drills at the World Trade Center in the years preceding the 9/11 attacks have been credited as one of the primary reasons so many building occupants—95.2 percent—were able to evacuate the buildings in a timely fashion.

Despite management resistance to the disruption of these evacuation drills, security director Rick Rescorla would conduct unannounced mandatory evacuation drills for all employees of Morgan Stanley/Dean Witter in the World Trade Center, from secretaries to stock brokers. Twice a year, Rescorla would lead employees, two abreast, down the stairs—more than 70 floors for some occupants. On September 11, the first plane hit Tower One at 8:46 a.m. (EDT). Before the second plane hit Tower Two, at 9:02, Rescorla had managed to evacuate most of the employees and hundreds of visitors. He guided them himself, leading them in songs and cheering them on.

One of the most difficult challenges for facility managers is an evacuation drill. In a large facility, the scene can become chaotic. There may be resistance from both occupants and management to a—perhaps lengthy—interruption in their activities. Important meetings or events may be in progress. Poor weather can be punishing for occupants evacuated outside the building. Crowding can be physically and psychologically stressful for shelter-in evacuations. In tall buildings occupants may be required to use stairs, which will be difficult for some. Getting occupants back into a tall building takes time since elevator systems are not designed to transport all the occupants at the same time.

Yet evacuation drills are an essential part of emergency response. Emergency support team leaders must know routes and how to manage different situations, including the chaotic scenes at assembly areas and evacuation-related injuries. Occupants must be familiar enough with the process to perform it calmly. In addition, they must be trained in different routes, staging areas and procedures so that they can adapt quickly to evacuating under different types of scenarios.

There are also issues of compliance. Periodic fire evacuation drills may be required by local governments. For example, in the U.K., drills must be conducted every six months. A large building that practices staged evacuations—evacuating by floors or building sections—may also have to demonstrate the ability to empty the building all at once in the face of a widespread threat. Insurers may also require periodic drills, and premiums may be affected by the percentage of occupants evacuated within a defined time frame.



FM works with incident management teams to support actual evacuations and drills. Performance and participation in drills can be supported by:

- **Ensuring proper signage.** Reviewing and updating evacuation maps, staging area identification placards and mobile posters should be considered an emergency plan preventive maintenance activity.
- **Timing evacuation drills to meet compliance requirements, emergency response plan objectives and the occupants' needs.** The frequency of drills may depend on compliance or insurer requirements and on the organization's risk analysis. Incident teams should confer with first responders, with landlords or tenants in leased facilities and with management to avoid conflicts with important events. Weather forecasts should be checked before the drill is scheduled. Severe weather provides the opportunity to test shelter-in-place evacuation procedures and sites.
- **Designing staged drills if needed.** In a staged evacuation, only occupants in certain areas are ordered to evacuate at one time. By practicing evacuations in stages or facility sections, facility managers may be able to train the whole building with less disruption to the organization.
- **Keeping occupants motivated and engaged.** Familiarity breeds contempt. The more occupants practice a procedure, the less seriously they may take it. Some facility managers have motivated occupants to participate in emergency drills by turning them into contests: Which department can get all of its people out of the building and to the assigned staging area in the shortest period of time? Simple prizes and recognition in newsletters or on Web sites can support positive performance. A theater staged a free concert for guests who volunteered to participate in a drill. Staff were able to practice procedures, and guests were rewarded for their participation. Facility managers can also change the evacuation scenario by blocking the closest exit (perhaps marking it temporarily as "out of commission") and forcing the occupants to become more aware of the facility layout.
- **Planning accommodations for occupants with disabilities.** This can include warning systems that employ lights or vibration in addition to spoken messages. Facility managers must plan for how to evacuate occupants in wheelchairs—whether to install devices to assist descent in designated stairwells or perhaps to conduct training with designated team members and disabled occupants. Facilities can also construct fire-resistant



spaces as “areas of refuge” where occupants with disabilities can wait for emergency responders.

- **Winning management support.** Drills require the participation of all occupants. Neither fire departments nor insurers are sympathetic to senior managers who protest that they are too busy to participate and cannot leave their offices. In some cases, facility managers can use their powers of persuasion to show managers the impact of their behavior on the safety of first responders, occupant attitudes and insurance rates. For stubborn cases, facility managers may have to let first responders deal with the situation. Incident response teams can also enlist senior managers in emergency response by appointing them fire wardens or floor captains.

This last issue serves as a reminder to facility managers of the importance of modeling the desired attitude toward emergency preparedness and the behavior the organization’s plan requires. The incident management team must take all training events and exercises seriously and communicate this attitude to facility management staff, management and occupants.

Debriefing drills

Training of emergency team members should emphasize that, in the midst of a drill or actual response, team members must be aware of what is happening around them and document their observations as soon as possible, before memory fades. In an actual emergency, injuries and fatalities will need to be fully documented for later investigation. In drills, however, much can be learned from observing events that have not been planned for—unforeseen bottlenecks in halls or stairways, occupants who have not received the evacuation order, physical obstacles that cause occupants to trip or fall, darkened areas that are difficult to navigate, incapacitating levels of fear.

Drills can also be a valuable way to identify noncompliant occupants—occupants who refuse to participate in evacuation drills and who will, in all likelihood, refuse to evacuate during an actual emergency. “Sweep teams” assigned to ensure that occupants have been evacuated should be apprised of these individuals and their locations. Incident response teams should also consider notifying senior management about noncompliant occupants. As stated earlier, they can affect the facility’s insurance coverage, but, most importantly, they can unnecessarily risk the lives of first responders.

If necessary, follow-up drills should be scheduled to correct procedures and improve compliance with policy.



✦ Topic 3: Emergency Preparedness/Business Continuity Case Study

How will the incident management team at LGH-EMS address the issue of training, testing and drilling?

Emergency Preparedness and Business Continuity Case Study (continued)

LGH's commitment to emergency preparedness and business continuity planning began with communicating senior management's commitment to these objectives. The incident management team at LGH-EMS attended a Web conference with all the divisions and senior management. Senior management explained its commitment and encouraged the teams to ask questions. Many did, primarily about the resources planning would require. Management pledged to put budget behind its commitment.

Motivated and encouraged, members of the incident management team began attending regular department meetings to review the concepts and benefits behind these new programs and explain how they affect the employees. The team members described the rostering of support teams and encouraged volunteers, future training in first aid and CPR and periodic emergency response drills.

Workshops with essential functions began. These groups began to assemble their requirements and work with the business continuity team to develop contingency strategies for different scenarios.

The facilities manager met with her people to identify necessary procedures in different emergency scenarios.

Individual certification in first aid and CPR was offered to all occupants. As promised, evacuation drills began, led by the incident management team and employees who had volunteered to assume responsibility for evacuations of floors or departments.



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. List at least three reasons why organizations should plan for training and testing in both their emergency response and business continuity plans.
-
-
-

2. Members of an emergency team meet in a conference room to talk through how they would apply plans to a particular scenario. The group is engaged in
- () a. a seminar.
- () b. a tabletop exercise.
- () c. a drill.
- () d. a full-scale exercise.

3. Emergency team members, including floor coordinators but excluding occupants, physically reenact their actions and movements in response to an emergency. This group is engaged in
- () a. a functional exercise.
- () b. a tabletop exercise.
- () c. a drill.
- () d. a full-scale exercise.

4. Management resists allowing the incident management team to conduct more than one full-scale evacuation drill a year. How should the team respond?
- () a. Accept management's direction.
- () b. Perform tabletop exercises at greater frequency.
- () c. Plan full-scale evacuation drills as often as the incident management team finds necessary.
- () d. Plan multiple staged evacuation drills.

5. List at least three ways in which evacuation drills could be conducted more effectively.
-
-
-



Progress check answers

1. Organizations should plan for testing and training to:
 - Ensure participant performance even under pressure.
 - Improve coordination with other functions and external parties (e.g., first responders, suppliers).
 - Ensure that procedures are correct, complete and possible.
 - Check adequacy and availability of resources, spaces, supplies, staffing.
 - Ensure that response objectives can be met (e.g., evacuation time). (p. 1-227)
2. b. In a tabletop exercise, team members talk through their actions for specific objectives without using actual supplies or involving first responders or occupants. (p. 1-232)
3. a. A functional exercise allows members of the incident management team to practice and assess how well the team functions can be performed. Occupants are not involved, but team members perform necessary actions. (p. 1-232)
4. d. After informing management about the benefits and possible requirements for these drills, the team may be able to use staged drills to achieve an acceptable level of preparedness. (p. 1-234)
5. Performance in drills can be improved by:
 - Ensuring proper signage in the right places.
 - Timing evacuation drills with attention to the organization's and occupants' needs.
 - Keeping occupants motivated and engaged.
 - Planning for occupants with disabilities.
 - Winning management support.
 - Debriefing drill performance. (p. 1-234)



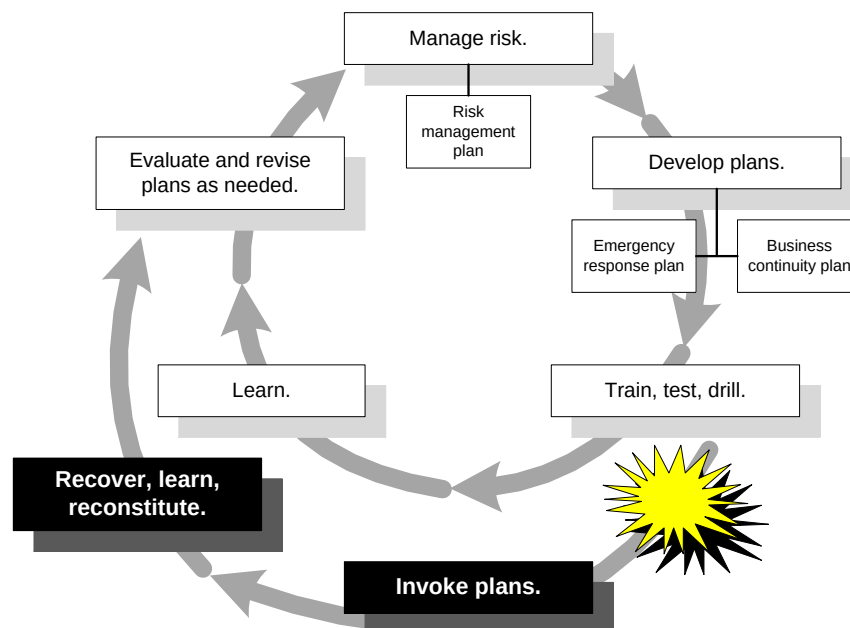
Chapter 5: Respond, Recover and Learn

After completing this chapter, students will be able to:

- Describe essential elements of an effective incident response.
 - Explain the importance of after-action debriefing and approaches to debriefing.
 - Describe FM's role during incident response.
 - Provide examples of the types of knowledge, resources and skills that may be necessary for a damage assessment team.
 - Describe the impact of insurance factors on the facility's damage assessment and recovery processes.
 - Summarize the responsibilities of incident command and FM during recovery.
-

As the emergency preparedness and business continuity model highlighted in Exhibit 1-62 indicates, this chapter focuses on how an organization and FM respond if an incident does occur.

Exhibit 1-62: Emergency Preparedness and Business Continuity Model—Respond, Recover, Learn



This chapter discusses:

- Incident response and debriefing.
- Facility damage assessment.
- Recovery and restoration or replacement of the facility.

✦ Topic 1: Incident Response

When an incident is reported, it is assessed and escalated as directed in the emergency response plan. Procedures and systems are activated, perhaps in stages as the incident unfolds. Incident team members make a series of decisions and adapt to the “circumstances on the ground.”

Coordination and control are essential to mount a unified response and to ensure that resources are quickly directed where they are needed and that authority is handed off smoothly to first responders.

First responders must be briefed on the details of the situation: what happened, where it happened, how long ago it happened, what the known effects are and what the status of response efforts is. To provide this debriefing, incident management team leaders must have received relevant and accurate information from support teams.

Throughout the incident and response, incident management and support teams must model confidence, control and calm to each other and to participants. Attention must be paid to occupants’ sense of well-being. Team members should share available information but take care not to frighten occupants. They should be patient with occupants, who may act badly out of fear. Removing occupants as quickly as possible from the scene may help minimize traumatic experiences and speed emotional recovery. Depending on the type of emergency, the incident response team (usually the HR manager) may need to provide access to counseling.

Documenting and debriefing the event and the response

Incidents and responses are documented formally, often in response to requirements by local governments and agencies and insurers. However, the organization should ensure that the incident is documented internally as well. By documenting all response events—even events that are eventually considered false alarms—the organization has a chance to test and improve its preparedness.



Team members' first responsibilities are to manage the incident and support response activity, but because of the importance of documentation, team members should also try to note and remember what is happening around them. As soon as the immediate response to the incident is over, team members should record their memories, while their impressions are still fresh and probably more accurate. Teams could even maintain a secure blog where brief reports could be recorded for later discussion and study.

These records serve many purposes:

- Providing material for discussion during team debriefing or after-action sessions
- Pointing to needed improvements in plans and training
- Expanding team members' perspective on incidents
- Potentially contributing to better understanding among those working in emergency preparedness and business continuity

As the incident recedes, the teams will have time to distribute surveys to team members, occupants and first responders. Interviews and focus groups can be conducted. The incident and the response can be reenacted through a tabletop exercise, so that it can be analyzed. In this way, debriefing can lead to a deeper understanding of why things happened the way they did and help develop more reliable solutions.

Managing business continuity efforts

If business continuity plans have been activated, this process should be debriefed as well. The evaluation can occur in stages, depending on the length of the relocation—assessing, first, the effectiveness of the relocation and continuance procedures and later, after the return to the facility, the effectiveness of the transition back into normal operations. Again, gathering feedback while memories are fresh is essential.

Debriefing should focus on issues such as:

- Effectiveness of communication at activation and during the relocation.
- Adequacy of the workspace, equipment, supplies and services.
- Ability to meet objectives for recovery time and performance level.

Affected managers should be encouraged to contact the business continuity team leader directly as issues related to the transition emerge. If larger issues in the plans emerge, meetings can be held with leaders of interdependent functions and/or suppliers.



FM role in the response

During an emergency response, FM coordinates with the incident command center and promptly provides any information that could affect the status of the incident and the response—from example, potential for explosions or release of hazardous materials. Emergencies can escalate quickly in intensity and spread in effect, and the incident commander must be ready to activate different responses.

If occupants have been evacuated, the facility manager must ensure that they are safe and sheltered and arrange for their transportation, if necessary, to their homes or temporary lodging. Medical attention must be provided. Food, water and blankets may be distributed if occupants will be outside the facility for a prolonged time.

The facility manager must also monitor the situation to be ready for subsequent actions:

- A damage assessment team may need to be activated so that the recovery process can begin as quickly as possible.
- Business continuity plans may be invoked, which will involve FM support.

*** Topic 2: Damage Assessment**

The facility manager may lead the damage assessment team, which will begin its work as soon as conditions are judged safe. Team members should have sufficient expertise to assess whether an asset is irretrievably lost or recoverable, make recommendations for replacement or repair and estimate recovery time frames.

Team composition will depend on the nature of the emergency and the problems created by the event. For example, after an earthquake, a damage assessment team will require structural, mechanical and electrical engineers as well as experts in debris removal and facility system equipment. A fire that affected computers and networks will require IT expertise. An emergency response that resulted in asbestos contamination or mold will require special mitigation teams.

The damage assessment team should be equipped with:

- Reference materials (e.g., as-built drawings where available, maintenance records, warranty information, reports of pre-existing problems).
- Tools to document observations (e.g., checklists, cameras, video and audio recorders, tablet computers).



- Tools to access areas that need to be assessed (e.g., keys and access codes, flashlights, ladders, shovels, chain saws).
- Safety equipment (e.g., respirators and dust masks, hardhats, first aid kits, exposure monitors).
- Lodging and meals.

A special concern during damage assessment has to be the safety of the assessment team. Structures may need to be checked first and reinforced before teams can enter the facility. Power, water and gas may need to be turned off. In severe cases, approval by local municipalities or emergency agencies to enter and initiate recovery efforts may be required. This may include supporting documentation from a licensed entity or a statement from an expert such as a structural engineer declaring the building foundation and structure sound.

The outcome of the damage assessment will be a damage assessment report that describes losses, determines how much of the facility is usable and estimates cost of repair/replacement. There are computer-based applications that guide damage assessment teams through all the various aspects of loss in different situations. Ideally these would be stored on a handheld, battery-powered device that would be functional even if the facility has lost power.

Insurance for damages

One of the first calls a facility manager makes after an emergency will be to the organization's insurer. The facility manager, risk manager and/or business continuity specialist and insurer will tour the facility and (ideally) reach agreement on what is recoverable. To prepare for this, FM should have a good understanding of the facility's insurance situation. FM must remember, however, that insurance practices and regulations are highly local. FM may need to consult with the organization's legal function or a local legal expert to understand the nuances of local insurance practices and requirements.

Review facility insurance

During the risk management phase, the facility manager reviewed the facility's insurance coverage and established a working relationship with the insurer(s). Senior management and facility management must understand the significance of how the organization has insured its property:

- Has essential property been insured adequately so it can be replaced or restored?
- Is insured property accurately valued? Is this value documented? Is the documentation somewhere secure so it can be retrieved after a facility emergency?



- Does the insurer agree with the property valuation? Some insurance companies may assess a penalty if property is underinsured, and the penalty will be deducted from the insurance payout. This can seriously disrupt financial planning for recovery.
- What is the deductible or insurance “excess”? Determining the right deductible level depends on the cost of insurance and the organization’s ability to absorb the cost of replacing a necessary asset. Senior management must accurately estimate what costs the organization can absorb.
- What exactly is covered? Is the cost of lost income due to business interruption included? Is equipment covered if the damage is due not to a storm but to a power outage caused by the storm? Will insurance cover costs such as lodging and food for those involved in damage assessment and recovery?
- What restrictions will apply to the recovery effort? What authorizations are required to begin recovery and salvage?
- Who has ownership of the salvage and how is value assigned to salvage? Can the insured keep all or a percentage of the value of salvage?
- Does the facility qualify for insurance discounts because of the emergency response plan it has in place and the prevention/mitigations actions it has taken?

**Document,
document,
document**

Damage assessment teams should document everything they observe, ideally with visual time-stamped proof. Material that is assessed as salvageable should be separated from debris and reviewed with an insurer before removing it from the site.

FM must track and document all expenses associated with this phase of the emergency: housing, meals, miscellaneous supplies, utility services, expert fees and so on.

*** Topic 3: Recovery and Reconstitution**

**Starting the
return to
“normal”**

The return to normal conditions and operations may begin before the incident is declared over. FM may lead those portions of recovery or reconstitution that pertain to the facility, reporting to the incident management team leader. The team leader gathers information and communicates with stakeholders. This ensures uniformity of message.



During the recovery phase, the incident management team:

- **Communicates with those affected through a designated spokesperson.** Employees should be briefed on the incident and future plans as quickly as possible to allay their concerns. For example, employees may want to know how they will be paid or how they can work remotely. Family members need to know where relatives are, their condition and how to contact them. Facility neighbors will want to know how their own health and well-being will be affected. Were hazardous materials released during the incident? Are they still present on the site? Will the facility be replaced? How quickly will the site be restored?
- **Investigates the causes of the emergency.** An investigation should be started as soon as possible, before witnesses begin to forget what occurred or become unavailable and before material evidence is disturbed during facility restoration or salvage efforts. Identifying probable causes can guide future prevention/mitigation efforts. Any interviews and findings should be shared with the crisis management team, which is responsible for strategic decisions.
- **Ensures ongoing security at the site.** Although the facility may not be operating fully, security concerns remain—and, in fact, become more challenging. Immediately after an incident, there will be a significant increase in visitors to the facility whose access must be controlled, and normal barriers to unauthorized access may not be operable. However, occupants' safety and the organization's assets must be protected. This may involve hiring additional security, constructing barriers and adding temporary lighting. Comings and goings of personnel and checking in and out of equipment should be documented.
- **Supports business continuity plans.** As described in the preceding topic, the incident commander may assist efforts to locate and support critical processes and to solve problems and provide resources as needed.
- **Supports management's decision to restore or replace.** An accurate assessment of the facility's status is essential to supporting management's decision to restore or replace the facility, establishing insurance coverage of recovery costs, estimating budgets and timelines for recovery (which will be critical information for business continuity activities), facilitating a rapid return to full function and minimizing financial losses through working with insurers and salvage companies.



- **Implements the crisis team decisions to restore or replace as efficiently as possible.** The recovery team will initiate the process of replacement by researching options and initiating rebuilding and renovation projects. Facility management will be directly involved in supervising restoration projects.

Recovery and reconstitution

The terms *recovery* and *reconstitution* refer to the fact that the return of the facility to full operation occurs in two stages:

- Recovery includes activities immediately following the emergency aimed at stabilizing the facility (e.g., repairing critical damage to the facility structure and the building envelope) and resuming building systems (e.g., water, heat, power) so that the facility can begin functioning, even if it is at a reduced level. This should occur as quickly as possible, since it will provide security and protect assets from further degradation. Business functions that have been moved to short-term temporary locations (e.g., hotels) may be moved again to more long-term interim locations (e.g., leased space).
- Reconstitution includes all those activities that are necessary to bring the facility back to pre-emergency condition. The time required for reconstitution can vary, depending on the amount of damage the facility has sustained and the organization's decision to restore or replace the facility. If an organization decides to lease a new, existing facility, reconstitution will proceed more quickly than if the organization decides to repair a heavily damaged facility.

The decision to restore or replace the facility will be made by management and possibly municipal authorities and insurers. The facility manager's assessment about what will be required for restoration (in terms of both money and time) will help inform management's position. If management chooses restoration, the facility manager must work with management and the business continuity team to establish priorities in bringing the facility fully back online.

Whether the decision is to restore or replace, the organization and facility management should decide whether the recovery process offers an opportunity to make changes to the facility that will increase the organization's productivity and ability to fulfill its mission. Damaged equipment can be replaced with more resource-efficient models. Building systems can be automated, and capabilities such as closed circuit video and wireless networks can be installed. Space can be reallocated to meet current needs. New facilities can be relocated to more promising and/or less vulnerable sites.



Before management decides on restoration or replacement of equipment or facilities, FM can help lead the organization in executing recovery projects that implement improvements identified in existing strategic plans. It may be opportune to invest in these plans following an unplanned disruption in order to avoid a planned disruption later. To do this, facility management must engage all stakeholders—including neighbors, government agencies and emergency responders—to ensure that implementing the plan at this time is prudent from a financial, timing or other perspective.

FM responsibilities

Specific facility manager responsibilities during recovery include:

- **Bringing the facility management function back online as quickly as possible.** Facility management will probably be the first function to resume its responsibilities. Facility managers must be prepared to bring staff back to work, juggle normal and recovery work assignments and track data related to both operations and recovery work. This means that facility technology and records must be brought back online as quickly as possible, especially computerized maintenance management systems (CMMS) and bidding and project management applications.
- **Managing recovery projects.** Progress and costs must be tracked, and senior management, line managers or tenants and occupants must be regularly informed about progress and possible completion dates.
- **Supporting sustainable practices.** Facility managers must consider and assess the application of sustainable practices and identify opportunities to increase the facility's sustainability. This might include reuse of materials (e.g., ceiling tile, carpeting, wall board, metals) if they pose no hazardous consequences.
- **Serving as a liaison with outside parties,** such as insurers or inspectors. FM should not, however, answer questions from the media and outside parties. This is the responsibility of the designated spokesperson, who has been trained for this task.
- **Managing salvage.** Facility managers may work with professionals and insurance adjustors to determine what assets can be kept or repaired for reuse, sold as salvage or removed as debris. When dealing with salvaged material, facility managers must be mindful of best practices concerning sanitation and mold remediation. Insurers can often recommend salvage companies.



- **Documenting recovery experiences.** In addition to documenting costs for insurance and business purposes, the facility manager should also document the recovery experience itself. This could involve photographing progress, maintaining a blog on the experience and inviting occupant input, keeping minutes or records of regular recovery-related meetings or saving media reports of the event and the recovery. Information about what went right, what went wrong or simply what happened will add to the facility management function's store of institutional knowledge.
- **Commissioning repaired and new systems and assets.** As with a new facility, the facility manager must ensure that all repaired or new systems function as promised and designed. The facility manager may be assigned the task of determining at what point the facility is fully operable again.

✦ Topic 4: Emergency Preparedness/Business Continuity Case Study

The case study of LGH-EMS resumes, examining if the organization's investment in emergency preparedness and business continuity planning have helped it weather an incident.

Emergency Preparedness and Business Continuity Case Study (continued)

An emergency occurs

Late in the evening, the LGH-EMS facility manager received a call from security. One of the workers for the cleaning service with whom LGH-EMS contracts had been using a propane-fueled floor burnisher when the machine exploded. The cleaner was burned, and there was a small fire burning in the immediate area. The fire department was on its way. Security had sounded an evacuation alarm in case there were people in the building working late.

The facility manager alerted the emergency response team leader, who is the unit's business manager. She then called the chief building engineer and they both went immediately to the facility to assess the situation. Once on site, the engineer conferred with the fire chief and began turning off power in that area and ventilation to decrease the chance of smoke spreading throughout the facility.

The facility manager was surprised at how few people were outside the facility, and when she asked the security manager about this, he explained that he had been too busy with the emergency medical team treating the contractor to sweep the building. The facility manager began a quick sweep with security and found about 20 people still working at their desks. They were told to go home immediately.



By now the team leader had arrived and had communicated directly with the fire department. Once the incident was under control, the fire department declared the incident over and the facility secured and safe to reoccupy. The facility manager had access to the damaged area blocked. She called the supervisor of the affected area at home, and they decided on a plan for the next day. The automated calling system was then used to contact employees in the affected department and instruct them to call their supervisor for further instructions. The damaged area was wet, smoky and charred in spots, but a damage assessment could wait until the morning.

Employees began arriving early the next morning, but almost immediately reports of odors and complaints of breathing difficulties started coming into the facility manager's office. Paramedics and the fire department were called, and the building was evacuated completely again. The evacuation was not as orderly as it had been in drills, since smoke had started to fill the hallways and employees were distressed and started to panic. The paramedics had trouble getting close to the building because of the crowds of employees. Employees were sent home for the rest of the day.

The fire department reported that the original fire had traveled through the walls, smoldered overnight and broken out in another area of the building. Now two areas were fire-damaged and two floors were heavily smoke-damaged. Employees in the affected areas—mostly designers and programmers—would not be able to use their work areas for at least a week.

As soon as the scope of the fire in the facility was clear, the team leader activated the business continuity plan. Employees were instructed via the automatic messaging system to report to the contingent workplace one hour before their usual start time the next day. This had been identified in tests as the time required for representatives to find their assigned workspace and set up their computers and VPN access to LGH-EMS. Customer support was able to take its first call as soon as the service lines opened up. Service was a little slower, but representatives had been trained to deal with customer frustrations, and most customers were patient as soon as the situation was explained. Since the department was working below full staffing levels, the manager was authorized to bring in lunch every day.

After the first day, the strategy seemed to be working well. There were some difficulties getting technical experts on the line quickly, however. There was also some confusion when employees in the affected area reported for work and could not find workspace. The business continuity team decided it would have to designate two technical experts to make the move with customer service to the alternate facility. In an emergency like this, in which part of the facility was inaccessible to the organization, the product development teams would have to be assigned priorities. Priority level one teams would report to work as usual. Priority level five teams would work from home. The manager of each team would be responsible for communicating with team members.



Post-event debrief and recovery

The incident management team had scheduled a debriefing meeting over breakfast, but after the second fire they decided that they should include the crisis management team. Since the conference room equipped for Web conferences was in the damaged area, it took a while for the team to decide on a good alternative. Within two hours they had arranged a teleconference with the crisis management team at headquarters, and the decision was made to invoke the business continuity plan for the affected functions.

The team leader debriefed the crisis management team. This emergency could have been handled better. There was not sufficient staff to conduct an evacuation and still maintain an acceptable level of security. Occupants' cooperation with the first call to evacuate was disappointing, and the lack of organization in the second evacuation was potentially dangerous.

The crisis management team was concerned about the flawed evacuation that morning. The incident management team proposed solutions. Obviously occupants would have to be retrained in procedures. The staging areas would have to be moved to accommodate emergency vehicles. There would need to be discussions with the cleaning vendor. Perhaps an analyst would need to be brought in to examine the building's fire detection and suppression system. The plan would appear to be weak in managing after-hour emergencies and would have to be re-examined.

Even as customer support was being transferred to the partnering facility, the facility manager was meeting with the insurer and beginning a damage assessment of the affected area. Furnishings and electronics were a complete loss. The fire had not breached the outer shell but interior walls, ceiling and floors would have to be replaced. Cabling would have to be reinstalled.

On the heels of the insurance adjustor came the local building inspector, who wanted to inspect the entire structure with the facility manager.

Other areas of the facility had suffered some smoke damage. Cleaning teams arrived every night to scrub walls and surfaces and shampoo rugs. Some soft furnishings were removed at night for professional cleaning.

Since the finance director was more experienced in this area, she worked with the insurance company on the valuation and coverage issues. The facility manager began getting bids from a series of contractors and suppliers.

There was only one misstep on the path to recovery. The facility manager had arranged for a service to demolish the burned area and for a hauler to remove debris. The demolition group had just started when an insurance adjustor appeared, furious that demolition was proceeding without the insurer's approval. The atmosphere was tense for a while, but with calm and patience, the facility manager placated the adjuster and work was resumed.



It would take two weeks to return the facility to full operation. Transitioning back was not difficult. At the end of the working day, managers contacted all affected employees (both customer support and the low priority development team) to report to work as usual. The organization and the facility had weathered the emergency well. A new wireless system was installed in the renovated area as a test. If it proved useful, there were plans to expand it throughout the facility. The relationship between customer service and their technical team had strengthened considerably, since tech people would rotate through assignments with customer service. During those rotations the teams spent most of their time together and grew closer in appreciating each other's work.

Interestingly, the incident also started an alliance with the neighboring office building. The two facility managers began a practice of sharing experiences and exchanging ideas. LGH-EMS's experience with emergency preparedness and business continuity set a good example for the other facility.



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. List at least three FM responsibilities during an actual incident response.

2. Which of the following statements about damage assessment teams are correct? (Choose two.)

- ☐ a. Teams should be created to meet the needs of the emergency.
- ☐ b. Outsiders should not be included in the team's initial damage assessment workup.
- ☐ c. Facility conditions should be secured before the team begins its work.
- ☐ d. Damage assessment should wait until essential business functions have been resumed.

3. List at least four pieces of information a facility manager should know about the facility's insurance coverage.

4. List at least four essential actions that must be taken as soon as an immediate crisis has been handled.

5. Recovery activities are distinguished from restoration activities in that

- ☐ a. the objective of recovery is stabilization and resumption of operations at reduced levels.
- ☐ b. recovery completes the return of the facility to pre-incident levels.
- ☐ c. recovery decisions are made by first responders.
- ☐ d. the restoration period is open-ended, but recovery should occur within three days.



6. List at least five responsibilities a facility manager has during the recovery/restoration period.



Progress check answers

1. During an actual incident response, FM:
 - Coordinates with incident command and provides prompt and clear status information.
 - Ensures that evacuated occupants are safe and cared for.
 - Monitors action to be ready if the situation escalates or business continuity plans are activated. (p. 1-242)
2. a and c. The damage assessment team should include, in addition to facility management, experts in the types of damage and repair issues specific to the emergency. Insurance adjusters and expert consultants are frequently included in the team and should be identified before an emergency happens. Facility management should ensure that the site is safe before beginning an assessment: that structures are sound, and power, gas and steam have been turned off. (p. 1-242)
3. Facility managers should know, before an emergency occurs, the following information about the facility's insurer, coverage and procedures:
 - Extent and accuracy of coverage
 - Insurer confirmation of facility valuation
 - Deductibles
 - Contacts and process to follow when insurance may be involved
 - Restrictions and coverage during the recovery period
 - Discounts available for emergency response measures (p. 1-243)
4. As soon as an immediate crisis is under control, incident command should turn next to:
 - Communicating with management and occupants and families.
 - Investigating the cause of the emergency.
 - Ensuring ongoing security at the facility.
 - Supporting business continuity plan activation.
 - Gathering information to support management's decision to restore or replace the damaged facility.
 - Implementing management's decision. (p. 1-245)
5. a. The object of recovery is the stabilization of the incident scene and the return of essential functions to defined levels within the defined time frame. (p. 1-246)
6. FM responsibilities during restoration/recovery include:
 - Bringing facility management functions back online as quickly as possible.
 - Managing recovery projects.
 - Serving as a point of contact with outside companies or agencies.
 - Managing salvage.
 - Documenting the recovery process to support organizational learning.
 - Commissioning recovery projects to ensure that the projects are completed and systems perform to specifications. (p. 1-247)



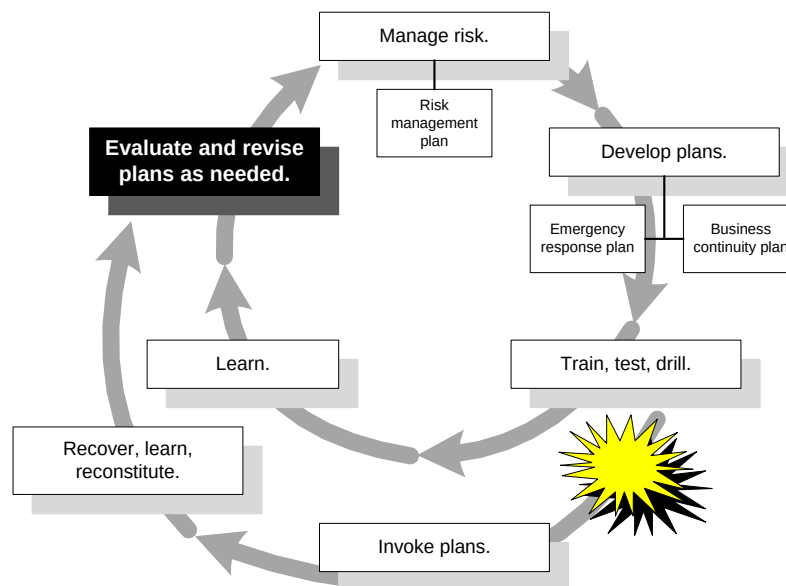
Chapter 6: Evaluate and Revise Plans

After completing this chapter, students will be able to:

- Describe the purpose of reviewing and auditing risk management, emergency preparedness and business continuity programs.
 - Provide examples of issues that might be examined during review of risk management strategies and emergency preparedness and business continuity programs.
 - List conditions that should trigger immediate review of programs.
 - Describe the purpose and focus of auditing programs and plans.
-

This chapter looks at the final phase of the emergency preparedness and business continuity model as shown in Exhibit 1-63.

Exhibit 1-63: Emergency Preparedness and Business Continuity Model—Evaluate



Throughout this process, the organization has assessed its plans' completeness and effectiveness in an ongoing manner—after tests, false alarms and incidents—but these ad hoc analyses should not take the place of an annual review and audit of the organization's risk management, emergency preparedness and business continuity programs.



Review and third-party audits are valuable tools for ensuring that the organization's programs are effective in meeting their objectives and use resources in an efficient, accountable manner. They also ensure that programs have been adjusted to respond to changes in the organization's risk profile, assets and processes or strategy.

✦ Topic 1: Evaluate and Audit Programs

Annual review	Risk management, emergency response and business continuity programs should be reviewed annually or as the organization deems necessary. The goal is to ensure that the programs' objectives are still valid, that the associated plans are valid and that all information in the plans is accurate and current. Relevant sections of plans should be sent out for review by external parties, such as first responders, insurers and consultants. In addition, those involved in the organization's programs should confer with peers in other organizations to see if the organization is using best practices and can learn from others' experiences.
Risk management program review	The following issues should be considered during review of the risk management program: • Have identified risks changed in terms of frequency or impact? Have some risks gone away? Have new risks appeared? • Has the organization's and facility's vulnerability to likely risks changed? • Have risk management strategies proven effective? Have new and possibly more effective strategies become available?
Emergency preparedness program review	The following issues should be considered during a review of the emergency preparedness program: • Level of management commitment to emergency preparedness • Fulfillment of objectives: • Are training and practice events being conducted, and are they effective in preparing team members and occupants? • Are the evacuation performance parameters being met in drills? • Have the identified prevention/mitigation measures been taken? • Are listed supplies and equipment in place, and are they operable/current? • Are contracts with vendors in place, and are these vendors still in business and able to fulfill their commitments?



- Emergency team members:
 - Are all members listed in the plan with their current contact information?
 - Have all members received copies of the plan? (And, if applicable, has each member signed the acknowledgement sheet to document his or her receipt of the copies?)
 - Have all members been trained in their responsibilities during an emergency?
- Effectiveness of procedures to manage probable risk scenarios
- Effectiveness of communication systems
- Accurate, current information about buildings and systems
- Current and complete list of occupants
- Effectiveness of training and testing processes
- Effectiveness of documentation policies and processes
- Debriefing process:
 - How are feedback and recommendations gathered during debriefing?
 - What improvements have been suggested?

Business continuity program review

In reviewing the business continuity program, organizations should consider:

- Are business continuity plans still aligned with strategy?
 - Have essential functions changed?
 - Have business processes changed?
 - Are the recovery times/levels still necessary and realistic? (In other words, is the function truly at risk if it is not resumed by the specified time and at the level described? Are the objectives possible to attain?)
 - Is the cost-benefit ratio of the contingency strategy to business continuity still favorable?
 - Have new alternative strategies been identified?
- Is the level of detail in the plan correct? Has the plan allowed flexibility in how objectives may be achieved?
- Have function leaders been involved in the development of strategies?
- Is everyone prepared to implement contingency strategies if the plan is activated?
- Have data/documentation backup procedures been tested? Are better alternatives available?
- Is the vital records program accurate? (An annual or quarterly audit of vital records is a recommended practice.)
 - Are the necessary vital records identified?
 - Are all the records identified as vital truly vital?



Immediate review triggers

Because emergency preparedness and business continuity are tied closely to the organization's mission, values and strategic objectives and to specific characteristics of the workforce and workplace, any significant change in these areas calls for prompt review of the risk management, emergency preparedness and business continuity programs. In addition, changes in the organization's risk assessment—the appearance of a new risk, the development of new vulnerabilities—will require that the organization's decisions about emergency response and business continuity be reexamined.

The need for immediate review, revision and reapproval of the emergency response plan include changes in:

- Facility vulnerabilities and emergency scenarios. (This would include changes in the facility's immediate environment, such as new neighboring facilities, natural gas pipelines or high voltage transmission lines. It might also include new internal risks, such as the new use of hazardous chemicals.)
- Level and speed of response by external responders and agencies.
- Facility size and layout.
- Numbers and location of employees in the facility.

The need for immediate review, revision and reapproval of business continuity plans could be affected by:

- Organizational restructuring, including changes in ownership, mergers, acquisition or divestitures.
- A new strategic plan that might alter essential functions.
- Reengineering of business processes—and the introduction of new technology that requires reengineering of processes.
- Changes in continuity requirements.

Annual audits

An annual review of the organization's programs could take the form of an audit. During an audit, an unbiased third party examines processes in terms of their effectiveness, efficiency and compliance with internal and external requirements. These audits may be required by insurers and government agencies.

An audit checks to see if:

- Documents are complete and current.
- All members who should have current, complete copies of documentation do in fact possess such documents. If applicable, members document receipt of the plan on a cover sheet.



- Plans comply with applicable laws and regulations and the organization's strategies, policies and standard operating procedures.
- All team members are listed with current contact information.
- Necessary delegations of authority have been made in writing.
- Emergency response plans are aligned with local emergency response strategies and systems and fulfill their requirements.
- Risk analysis and management plans seem reasonable.
- Proposed risk management strategies have been implemented and tested for effectiveness.
- Plans have clear and reasonable objectives and are constructed in such a way as to achieve their objectives.
- Procedures have objectives and are constructed in a valid manner.
- Supplies and contingencies listed in the plans are adequate and in place or accessible.
- Delivery of required training and testing is documented.
- Events are documented as required, and documents show application of correct procedures.
- Training and testing methods are valid.
- Resources have been used in an accountable and prudent manner.
- Due diligence has been used in contracting and leasing.

The incident management team should schedule a full-scale exercise in conjunction with the audit to demonstrate the program's effectiveness.

Prior to the audit, the plans should be evaluated and revised as needed, a new version number assigned and the documents redistributed.

✦ Topic 2: Emergency Preparedness/Business Continuity Case Study

The fictional organization LGH-EMS has reached the final phase of the emergency preparedness and business continuity model.

Emergency Preparedness and Business Continuity Case Study (continued)

A year after implementation of the LGH-EMS emergency response and business continuity plans, the LGH crisis management team held a Web conference with the EMS emergency response and business continuity planning teams. First, they talked through the facility's previous risk assessment. At first, they all agreed little had changed in terms of risks.



Then one member mentioned a newspaper article about a burst water main not that far from the facility. The infrastructure was aging in this area. What would happen if there was a similar mishap in the main feeding LGH-EMS? Surely that would affect facility operations, but for how long? And what if a fire occurred while the water supply was not functioning? The teams delegated analysis of these issues to team members and agreed to meet again in two weeks to discuss possible adjustments to the emergency plans. This was a process with which they had become familiar. As a result of the fire, the plans had already been extensively retested and revised.

In terms of the physical facility, LGH-EMS had expanded, acquiring a neighboring building. For now EMS occupied one-half of the facility. The organization's plans had to be revised accordingly, including its risk management, emergency response and business continuity plans. The teams began generating questions that would have to be answered:

- Had the expansion affected the designation of essential functions?
- What risks were posed by the cafeteria and leased operations?
- Had the evacuation system been affected by the new tenant?

The plans were revised, and management approved the addition of a cafeteria in the new building to serve employees in both buildings. The remaining space was leased to a small fabricating business with a warehouse and shipping area.

LGH-EMS's story has many unique elements, but the experience it describes should speak to all facility managers. FM deals with risk on a daily basis and must be prepared to manage its vulnerabilities, prepare for emergencies, continue its operation and recover from disaster.

But FM is also part of an organizational team, and its mission is to protect the organization's people, facility and assets and to provide space and services for all the other functions in the organization—while fulfilling its responsibilities to the community and the environment. Its efforts in emergency preparedness and business continuity start with FM but must extend beyond the FM function to the goals of the organization and its members.



Progress Check Questions

Directions: Read each question and respond in the space provided. Answers and page references follow the questions.

1. List at least three factors that could trigger immediate review and revision of an emergency preparedness plan.

2. List at least three factors that could trigger immediate review and revision of a business continuity plan.

3. Which of the following factors would be examined during the audit of emergency response and business continuity plans? (Choose two.)

- () a. Accuracy of name and contact information
() b. Business process requirements
() c. Occupant names and contacts
() d. Business soundness of measures taken



Progress check answers

1. Triggers for an immediate review of emergency response plans include changes in:
 - Facility vulnerabilities and risk scenario assessments.
 - Support from first responders.
 - Facility size and layout.
 - Numbers and locations of occupants.
 - Hazardous materials or equipment on site. (p. 1-258)
2. Triggers for an immediate review of business continuity plans include changes in:
 - Organizational restructuring.
 - Strategic goals.
 - Business processes.
 - Continuity requirements for essential functions. (p. 1-258)
3. a and d. An audit checks that actions are being performed as described in the plan, that information in the plan is accurate and that the measures described are sound from a business perspective. The audit would not reexamine business process requirements, although it may check that the requirements listed in the plan are accounted for in some manner (either stored for use or secured by agreement for future use). Similarly, the audit would not verify occupant names and contact information but would check that this information was being managed for currency, accuracy, completeness and compliance by human resources. (p. 1-258)

Next Steps

You have completed this competency of the IFMA Facility Management Learning System. Next, check your understanding by completing the online competency-specific chapter quizzes and case study to help you identify any concepts that need additional study. Check your understanding another way by selecting the competency-specific eFlashcards, or visit the Resource Center to download printable flashcards.

Once you have completed the chapter quizzes, reviewed the eFlashcards, completed the case study and feel confident that you have mastered the information, you can advance to the next competency.

