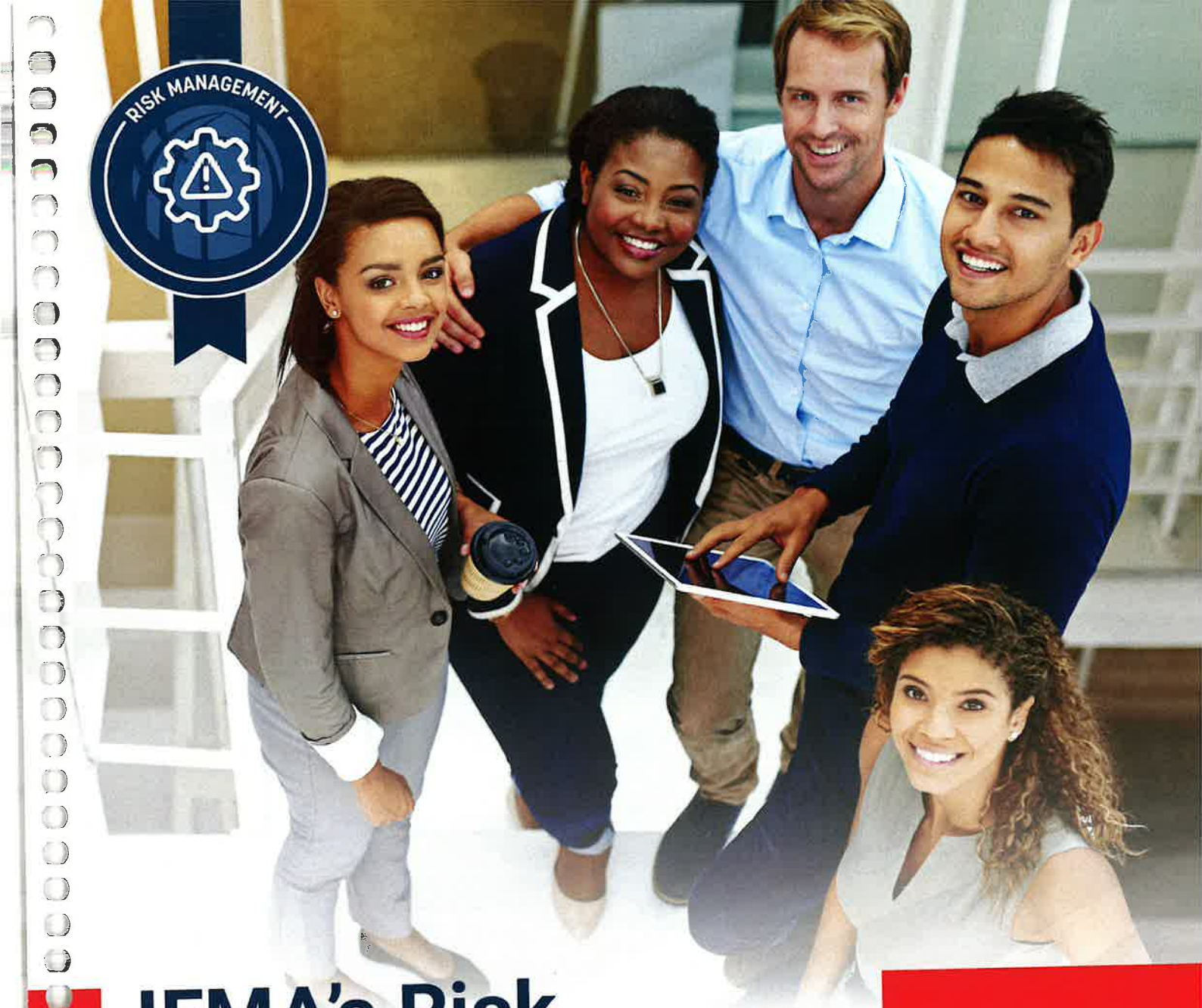


IFMA's Risk Management Course

Student Guide

IFMA™

Acknowledgments

IFMA's professional development courses – including our world-class credential programs, the FMP®, SFP® and CFM® – are the cornerstone of our industry-leading offerings for career advancement. The contribution of IFMA volunteer members is critical to the relevance and value of our educational programs. The result of their global input is learning for facility managers, by facility managers. We would like to acknowledge the cumulative hours and expertise our members have contributed to educational content development and review, from design through delivery, with special acknowledgement to Teena Shouse and Maureen Roskoski as lead contributors, ensuring that IFMA's Risk Management Course accurately reflects the body of knowledge and skills required of FMs in today's global business environment.

Teena Shouse, RCFM, FMP, SFP, IFMA Fellow

Maureen Roskoski, CFM, SFP, ISO 22301 Lead Auditor

Michael Barnes, CFM, FMP

Randy Braverman

Stephen Brown, CFM, FMP, SFP, ProFM, CPE

David Reynolds, CFM, FMP

Johnny Vinken, RCFM, FMP, SFP, M.Eng, CET, IFMA Fellow

Edition 2022, Version V2017PARM_1.0

Printed on 100% post-consumer waste recycled paper

Intellectual Property and Copyright Notice

All printed materials and information in the companion online components in IFMA's core competency courses are owned by IFMA and protected by the United States Copyright Law as well as the international treaties and protocols, including the Berne Convention. IFMA's core competency courses and companion online components are for your personal educational use only and may not be copied, reproduced, reprinted, modified, displayed, published, transmitted (electronically or otherwise), transferred, resold, distributed, leased, licensed, adapted, passed all, uploaded, downloaded or reformatted.

In addition to being illegal, distributing IFMA's course materials is in violation of copyright laws and will limit the course usefulness. IFMA invests significant resources to create quality professional development opportunities for its members and the associated FM industry. Please do not violate intellectual property rights or copyright laws.

Edition 2022, Version V2017PARM_1.0

Printed on 100% post-consumer waste recycled paper

Table of Contents

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

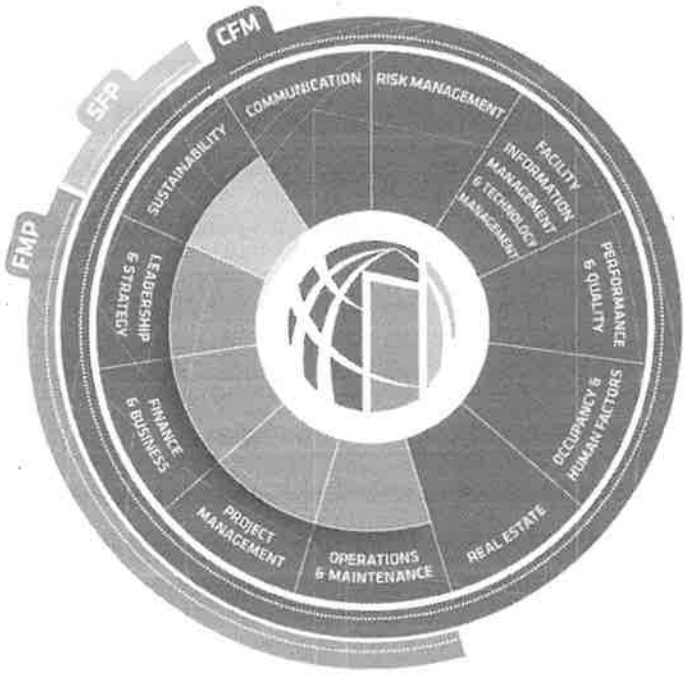
Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

IFMA Credentials

About IFMA Credentials

After analyzing the work performed by facility managers, we have defined 11 competency areas. Our three world class FM credentials, — Facility Management Professional™ (FMP®), Sustainability Facility Professional® (SFP®), and Certified Facility Manager® (CFM®) — are based on these competencies.

1. The FMP® is the foundational credential for FM professionals and industry suppliers looking to increase their depth-of-knowledge on the core FM topics deemed critical by employers.
2. The SFP® is the leading credential for all FM and like-minded professionals with an interest in the development of sustainable FM strategies.
3. The CFM® is the premier certification for experienced FM professionals. A comprehensive exam assesses knowledge, skills, and proficiency across all FM competency areas.



Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

IFMA's Core Competency Courses

IFMA's 11 core competency courses, developed from IFMA's Global Job Analysis (GJTA), comprise the body of knowledge for facility managers. IFMA continuously refreshes the courses to align with global industry standards for FM knowledge, skills, and tasks. The courses provide practical knowledge and examples to help you improve your performance.

IFMA's Core Competency Courses include the following:

Communication: develop the skills you need to be an effective liaison between external and internal stakeholders.

Participants will be able to:

- Create and deliver the right message for the intended result.
- Develop an FM communication plan.
- Identify and share relevant information to the appropriate audience.

Risk Management: address the role of the facility manager in supporting or leading risk management planning; emergency preparedness, response and recovery; facility resilience and business continuity.

Participants will understand how to:

- Respond appropriately to emergencies affecting the facility.
- Meet the organization's business continuity goals.

Facility Information Management and Technology Management: understand how to leverage modern tools and techniques for today's workplaces and occupants.

Participants will be able to:

- Understand secure, efficient data collection supports decision-making processes to meet core business objectives.
- Conduct technology needs assessments and anticipate the impact of new technologies.
- Understand decisions are made to keep, update, augment, or replace technology.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Occupancy and Human Factors: grow your ability to support organizational and individual occupant performance, while leading the FM team to develop and implement practices necessary to achieve success.

Participants will be able to:

- Create an environment where motivation, productivity, and retention are the norm.
- Blend safety and security with innovation.
- Negotiate service level agreements.

Real Estate: understand real estate principles and practices and how they contribute to achieving the core business strategy.

Participants will be able to:

- Develop and implement a real estate strategy to support the core business including assessing, acquiring, and disposing of real estate, and space management.
- Understand project management principles for managing new construction and other major projects.

Performance and Quality: define and make relevant what it means to capture fitness for the intended purpose, embrace a continuous improvement mindset, and satisfy stakeholders' needs.

Participants will be able to:

- Determine the needs and expectations of stakeholders for the facility and related service requirements.
- Understand and describe what comprises a comprehensive quality management system for FM.
- Measure the FM organization's performance to make continual improvements.

Sustainability: define the basics of five areas of sustainability and make relevant what it means to embrace sustainability.

Participants will be able to:

- Understand the management basics of:
  - Energy
  - Water
  - Materials and Consumables
  - Waste
  - Workplace and Site

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Welcome

Course Introduction

Welcome to IFMA's Risk Management Course!

Participant Introductions

- → Your name
- → Company name and/or job responsibilities
- → Reason(s) for taking this course — expected outcome(s)
- → Your experience in FM — years and work responsibilities over your career

Expectations

Learner responsibilities:

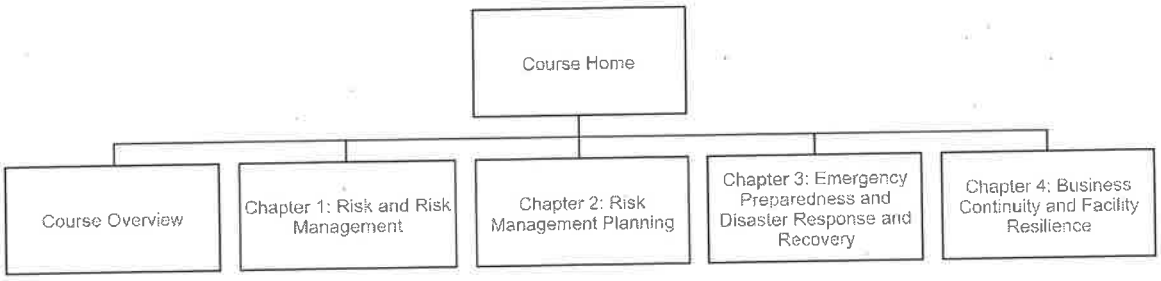
- → Be prepared – complete class pre-work
- → Take part in class discussions and activities
- → Follow the rules of common courtesy
- → Provide feedback to the instructor and IFMA

Course Audience

Welcome to IFMA's Risk Management Course! This course is designed for persons interested in developing knowledge and skills in IFMA's FM Core Competencies and who wish to gain practical knowledge to enhance FM industry professional development.

Course Chapters

There are four chapters in the Risk Management course.



Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Course Goals

The goals for this course are as follows:

- Evaluate the facility risks that could disrupt, compromise, or cause a failure of the demand organization and provide valuable input into risk management strategies to support the continuity of the business.
- Support the demand organization's need for development, testing, and maintenance of a business continuity plan.
- Develop a Risk Management plan for FM operations that align with organizational strategy.
- Train FM staff in their roles and responsibilities in the event of a business interruption.
- Detail the resources required to support the facilities aspect of business continuity and plan for the provision of those resources in an emergency.

Course Overview

Risk management is a strategic process for building a resilient organization, one that is strong and quick to recover when trouble hits. Well-managed organizations have detailed risk management strategies. These strategies shape the risk management plans for each of their functions, including facility management (FM).

> *"The destination is Resilience...the journey involves Risk Management, Emergency Preparedness, and building a strong Business Continuity Program." ~Teena Shouse, IFMA Fellow, Author*

Risk management is accepting the uncomfortable reality of risk, and it should be a critical component of strategic planning. By practicing risk management principles, organizations decrease the occurrence or impact of certain risks while being able to pursue opportunities in the face of uncertainty. Major decisions can be evaluated using a risk-benefit ratio that can help organizations more fully understand their level of risk tolerance – how much risk they are comfortable assuming. Organizations may balance the risk levels of their portfolio. For example, opening a facility in a politically unstable area may offer enough potential benefit if this risky venture is balanced by several other facilities with much lower risk profiles.

Facility managers must understand the demand organization's level of risk tolerance and its strategies for managing risk. This enables the facility manager to align the FM risk

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

management plan with that of the organization. It helps senior management more accurately understand the impact of facility risks.

Risk management is an essential first step in planning for emergency preparedness and business continuity. During the risk management planning process, FM and the demand organization gain greater awareness of the hazards they both face and how their occurrence could affect the facility and its occupants. This awareness can be used to decrease the facility's and the organization's vulnerability to hazards.

Definitions of risk management may vary, several elements are agreed on. These are:

- Identify human and physical assets that would be at risk should a threat occur.
- Assess and evaluate the level of vulnerability should a threat occur.
- Prioritize the severity of each occurrence.
- Prepare a plan to mitigate as much risk as possible.

Risk management is the first step in planning for business continuity in an emergency. During the risk management planning process, FM and the demand organization's leadership identify the threats they face. They determine how those threats could affect the facility, the occupants, and the organization's ability to compete in the marketplace.

Some countries and organizations have developed standards to define a common risk management language. For example, Australia, and New Zealand have developed the AS/NZS 4360. Through the Federation of European Risk Management Association (FERMA), risk management organizations such as AIRMIC and the Institute of Risk Management (IRM) have established standards. The International Organization of Standardization (ISO) has developed global, consensus-based standards and guidelines. How these standards apply to the different facets of risk management is covered in this course.

Risk Management Competencies in FM

Outlined below are the competencies and the performance standards that a facility manager should know regarding risk management, emergency preparedness, business continuity and facility resilience.

Given the need to manage risks to an organization, its facility, and its operations, and occupants, a competent facility manager develops and implements a risk management plan. Characteristics of the plan include that:

- The plan is developed and coordinated in cooperation with all functional representatives, critical contract service providers, and required experts.

- The plan identifies or lists physical assets, systems, and essential resources that if damaged or compromised would interrupt, disrupt, or cause failure to business operations.
- The plan is focused on facilities services for the physical space as well as the site environment, for example a flood plain.
- The plan considers potential exposures from and impacts to neighboring facilities and operations.
- The plan includes an assessment of the impact of disasters on the demand organization including people, facilities and technology in terms of the probability of continued operations.
- The plan identifies and assesses risks, as well as the methods to mitigate risk, such as preventive measures, contingency plans, redundant systems, insurance, and protocols for securing alternate resources.

Given the need to respond to emergencies affecting a facility, a competent facility manager prepares for, responds to, and recovers from emergencies such that:

- Developing emergency management plans and procedures are developed that meet the health, safety, and security needs of the facility and its occupants.
- Creating simulations or exercises to test the emergency management, disaster recovery, and business continuity plans that have been developed.
- Executing of simulations or exercises to test that the plans are monitored and evaluated. Update and correct the plans and procedures where deficiencies are observed in the simulations and tests.

Given the need to ensure the resilience of a facility and its operations, a competent facility manager develops and implements a facility resilience and business continuity by ensuring that:

- The plan is developed in cooperation with other functional representatives, critical external resources, and required experts.
- The plan clarifies the roles and responsibilities of facility staff, other functional staff, external resources, and service providers after a disaster.
- The plan includes protocols and enables necessary authorizations for when and how to access external resources, service providers, and systems.
- The plan ranks facilities, operations and systems in terms of criticality and priority based on an assessment of the potential risks identified, the likelihood of occurrence, and their impact on occupants, facilities, and the business as well as any dependent operations.
- The plan includes measures of success.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Risk management is a core FM competency. This course is based on the following competencies:

- Risk management planning.
- Emergency preparedness.
- Response and recovery.
- Facility resilience and business continuity.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Chapter 1: Risk and Risk Management

Lessons

- Objectives
- Lesson 1: What is Risk?
- Lesson 2: Risk Factors
- Lesson 3: What is Risk Management?
- Lesson 4: Building Risk Awareness

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Objectives

Chapter 1: Objectives

On completion of this chapter, you will be able to:

- Define risk as it applies to facility management.
- Identify what is required to manage risk.
- Outline the organization's risk awareness and culture.
- Understand the organization's level of risk tolerance.
- Understand how to build a culture of risk awareness.
- Demonstrate your understanding of risk management.

This chapter lays the foundation to the study of risk and risk management. It defines risk. It explains what is required to manage risk, raise the organization's risk awareness, and assess the organization's risk culture.

The objectives of this chapter are for you to be able to influence the organization's level of risk tolerance, help build a culture of risk awareness, and further develop your understanding of risk management.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 1: What is Risk?

Lesson 1: Objectives

On completion of this lesson, you will be able to:

- Influence the organization's level of risk tolerance.
- Understand the organization's level of risk tolerance.
- Demonstrate your understanding of risk management.

What is Risk?

The international standard, ISO 31000 – Risk management – Guidelines, defines risk as "the effect of uncertainty on objectives." Uncertainty is about the probability that an event might occur, what the potential damage or loss might be if it should occur and what is the organization's capacity or ability to recover from the loss.

When the probability is high that an event might occur, the risk of loss may be high or low depending on the event. For example, some people consider the sports of parasailing, bungie jumping and parachuting safe because they experience little uncertainty over the outcome, they believe the equipment to be safe and they have confidence in their personal abilities. Others may hold a different opinion and see these activities as dangerous and risky. Perhaps they have less confidence in their personal capability to recover if they make a mistake or if there is an equipment failure. People's level of uncertainty about an outcome can depend on how much confidence they have in their ability to affect the outcome and recover.

Estimating uncertainty is both personal and scientific. Actuaries who work for insurance providers, apply very scientific methods based on big data sets. Weather forecasters, rely on historic data and satellite imagery to predict weather patterns and forecast, such as the probability of rain, snow, sleet, and sunshine. Facility managers rely on the judgments of actuaries, weather forecasters and manufacturers of equipment and materials.

Risk for FM is about the level of uncertainty they have that if an event did occur, it would negatively affect the safety and viability of the demand organization, its occupants, assets, and operations. The higher the probability of being wrong in predicting an outcome, might increase or decrease the risk.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Uncertainty over an outcome can stem from a wide variety of events, such as an interrupted supply chain, lawsuits, strategic management errors, accidents, insufficient cash flow, equipment failures, natural disasters, pandemics, man-made disasters and social unrest, among others.

Uncertainty comes in many forms and exists in every aspect of a business operation:

- Financial or economic risk exists with uncertainty over the outcome of changing market conditions, sales, resource costs, and other factors.
- Legal and liability risk exists with the uncertainty over the probability of accidents or harm any time a person sets foot on an organization's site, or the outcome when a product or service is developed and released.
- Risk exists with the outcome of decisions about who to hire when staffing a function or choosing a contractor.
- In Project Management, risk exists with the decisions made about what should be done, by whom, and by when. Those decisions expose the organization to losses if they fail to bring a project in on time and within budget.
- In FM, risk exists with any action or decision that, if done improperly, threatens people or property. This includes occupant health and safety, the physical assets such as facilities and equipment of the organization and the infrastructure that enables organizational productivity including its technology.

Source of Risk

One way to analyze risk is to think of it in terms of the source. Here is a list of possible sources.

- **Human-made:** This type of risk is caused by the acts of humans, both accidental and purposeful. Examples include the probability of disgruntled employees vandalizing property or physically harming individuals. The probability of injury to people or damage to critical systems due to acts of terrorism or sabotage such as accidents during construction, disruption of fuel supplies due to labor strikes, and fires due to arson.
    - An addition to human-made risks are activities that harm living organisms and the environment through emissions, waste and resource depletion. Human-made environmental disasters include hazardous material spills during transport, careless fires, groundwater contamination, explosions, and acts of terrorism that target natural resources.
    - On a larger scale, nuclear plant meltdowns, dam failures, water main breaks, toxic spills, hazardous exposures, and groundwater contamination due to

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

inadequate preventive or corrective maintenance can also be considered human-made risks.

- A facility's aging infrastructure, including its plumbing systems, HVAC systems, roofing systems, and the like, become risks if they are neglected (human error) or if they are still in use beyond their expected lifecycle, this is caused by human error. Building systems are designed to withstand a certain level of trauma and threat, but that ability diminishes with age and use. When systems fail, they can cause harm.

- **Environmental and climate related:** These risks are the result of weather or environmental conditions, such as floods, hurricanes, drought, fires, and sandstorms. These events may have secondary or indirect impacts as well. For example, excess rain may cause a nearby levy to burst, flooding the facility. Other examples include natural disasters, such as earthquakes, volcanoes, tsunamis, and pandemics.
- **Technological:** These risks include building system failures, cyber-attacks, such as malware, trojans, or other software virus threats and FM hardware or network failures. Technology systems that are out of date have an increased risk of failure and attack. These risks can be thought of as human-made but are separate because they deal specifically with the reliance on computer technology used to support facility operations, information management, knowledge management, learning management, customer service, sales management and financial management systems.

During your efforts to identify risks, include threats that lie beyond the walls of the facility, such as potential hazards from a neighboring business operation. Consider global, regional, and local political and economic risks, such as a recession or war.

Risk Identification

The purpose of risk identification is to discover, identify and describe where and how an organization is vulnerable or at risk. The process answers the question, what might prevent us from achieving our objectives. The facility manager's role is to raise awareness of possible risks within the organization. To begin, consider identifying risks as an exploration. Possible techniques to identify risks and understand their potential impact are:

- **Gather data:** When identifying risks, having relevant and up-to-date information is vital. Interview stakeholders and conduct surveys. Use outcomes of the business process analysis in a "what if" scenario exercise. For example, "What if we lost the ability to get, use, or produce a key business element? What can we do about that?"
- **Brainstorm:** Convene team members and other business functions, perhaps with a trained facilitator to guide the discussion, generate a list of possible threats and

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

discuss the feasibility of different responses. A discussion of one risk will most likely bring others to mind. Working together, the participants might conduct a SWOT (Strengths, Weaknesses, Opportunities, and Threats) Analysis to share their assumptions about how resilient the organization is to withstand threats and what future threats might be. To provide balance in evaluating potential risks, take advantage of the group's knowledge. Have the group think beyond one facility. Consider risks that could occur at a group of facilities, or a whole portfolio of facilities operated by the demand organization.

- After an event, you can convene team members and stakeholders to do a **Plus Delta** exercise. A Plus Delta is a chart that records what the team thought went well, worked, and should be built on or repeated in the future. It highlights what did not work, why it did not work, and what to avoid repeating in the future.
- The team can also discuss and act out "**what if**" scenarios. This method clarifies people's assumptions about the resiliency of systems to withstand attacks.
- Look at historical information about the company, the region, the industry.
- Take a serious in-depth look at the **elements of continuity planning** to determine the less-evident outcomes of a particular risk event. While many organizations may have had pandemic plans in their business continuity documents, few were prepared for the total shutdown of cities, towns, states, and countries across the world and the closure of all but essential businesses as a result of the 2020 COVID-19 pandemic.
- **Model the risk**. Proven, easily understood approaches, methods and inexpensive technologies make quick, convenient, adjustable scenarios feasible for example, the @RISK add-in to Excel. If the demand organization has a strategic planning group, they may already be using risk modeling technology.

Armed with well-developed risk information an organization can position itself to manage risk well and act responsibly to protect its stakeholders.

Risk Identification Resources

To create a list of risks that might make a facility vulnerable, consider using the following sources:

- **Government bodies**, such as meteorological, economic development or emergency management agencies. Emergency management agencies or ministries of the interior may have documents that identify risks, such as flood zones or areas prone to earthquakes. They can provide more specific local guidance on the frequency and scope of different types of events.
- **First responders,** for example, fire and police, who have direct experience as well as records.

- **Insurers** who rely on a knowledge base of experiences to price their services.
- **Facility and organization records** and organizational memory of previous events. For example, records on facility damages due to weather can help identify specific facility weaknesses during hurricanes, typhoons, and high winds.
- Discussions with **other facility managers and risk management expert consultants** in the area and with comparable facilities.
- **Audits** are a valuable tool for identifying risk, use them to:
  - Evaluate risk management maturity. Determine if the plan still works. Risk maturity builds on the original risk framework and experience. It addresses new risks and places less emphasis on risks that are no longer of concern. This is a form of continual improvement, Plan, Do, Check, Act (PDCA).
  - Determine if the steps for effective risk management are being followed.
  - Assess compliance to standards that address risk.

Facility managers and individual functional leaders often address additional risks, such as those related to compliance with standards and regulations. For example:

- If a facility has a commercial kitchen, it will be subject to regulations associated with food handling and safety. Food handling and safety may not be related to a specific event but may refer to operational requirements in general.
- Most organizations are subject to occupational health and safety regulations, such as those from the Occupational Safety and Health Administration (OSHA) in the United States (U.S.) and the European Agency for Safety and Health at Work (EU-OSHA) in Europe. To protect the safety and health of occupants and workers, these organizations require specific methods of performing work. Partial or total shutdown of operations due to non-compliance with government and/or governing industry standards is part of the human-made risks category.
- In most parts of the world, the employer is responsible for the safety of employees and occupants in its facilities. This extends to contractors and visitors, and in many regions, extends to employees working outside the organization's facilities. Aside from legal responsibilities, this is vital in attracting and retaining employees, and maintaining the attraction of the brand.

Failure to understand and plan for these standards and regulations can be a significant risk to facility operations and the demand organization. Prioritize and incorporate this information into your demand organization's plan. Make it a best practice.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 2: Risk Factors

Lesson 2: Objectives

On completion of this lesson, you will be able to:

- Define risk as it applies to facility management.
- Develop your understanding of risk management.

As part of the Risk Identification Process, you should consider a variety of factors:

- **Tangible and intangible sources of risk.** A tangible source is one whose damage can be measured. For example, a labor strike or power outage that can disrupt production; a flood or power surge can jeopardize product integrity; a computer hacking can expose customer data or steal financial assets. An intangible risk is something that is not easily measured, such as an event that taints an organization's reputation or brand image. An example might be an unfavorable article in the press or customer complaints on social media.
- **Causes of issues.** Identify the root cause of an incident, such as human made, climate based, natural disasters, and technological. In the process, you will uncover more about what triggers a loss and where an organization is vulnerable.
- **Risk indicators.** Risk indicators use data to identify, assess and manage emerging risk events. For example, an increase in service calls may indicate the potential failure of critical equipment or a critical process. An economic downturn resulting in people losing jobs may signal future social unrest or acts of vandalism.
- **The nature and value of assets and resources.** FM may have critical equipment that, should it fail, the impact would be harmful to the core business. Before that happens, you must have a plan for redundancy and replacement.
- **Lack of knowledge and uncertain reliability of information.** As you gather information, make sure that it is accurate and that the sources are reliable.
- **Time-related factors.** Risks should also be considered in terms of current conditions and future conditions. Is the risk urgent, or is it outside the span of the risk management plan? Coastal flooding and clean water shortages are examples.
- **Biases, assumptions, and beliefs of those involved.** Based on their own biases or assumptions, a person or organization may identify or ignore a risk. Be sure to analyze all risks to determine their priority and how to handle them.

After considering all factors, the next step is to create a list of potential risks for your situation. These include risks specific to the region, your type of organization, your facility, your business-critical equipment and processes, and risks related to your contractors and

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

service providers. Once the risks, are identified, analyze them to determine which ones pose significant short-term and long-term threats to the organization.

You can further categorize risks as organizational, operational or environmental in nature.

Examples of Organizational Risks

Organizational risks are potential losses to the demand organization due to an event. They include material, strategic, reputational, regulatory compliance, legal, security, and operational risks (*Spacey, 2015*). Some examples of organization risks are:

- **Risk:** Noncompliance with regulatory requirements (human-made).
  - **Cause:** The organization assumes that no one would conduct an inspection. An inspector from the local regulatory body conducts a surprise inspection. He finds an open container of hazardous pesticide unattended on the grounds.
  - **Impact:** The organization is cited and fined for improper handling and storage of hazardous materials.
- **Risk:** Loss of institutional knowledge or Tribal Knowledge Transfer (human-made).
  - **Cause:** FM assumes institutional knowledge would always be available. During a critical renovation project, a long-time senior leader on the FM team retires. The position cannot be filled because the organization's goal of having minimal staff. FM must rely largely on outsourcing many of its functions.
  - **Impact:** The loss of institutional/operational knowledge creates project delays, necessitates rework on customer service requests, and causes budget increases.
- **Risk:** Loss or theft of data (technology).
  - **Cause:** The organization assumes it is not vulnerable to cyber-attacks; however, it experiences a cybersecurity breach through the building's automation system, which was unsecured and vulnerable to attacks.
  - **Impact:** Critical customer information is stolen, including credit card numbers on file, names, and addresses. The company faces lawsuits, regulatory inquiries, and decreased sales.

Risks can exist with other organizations that are part of your supply chain or aftermarket partners. Whatever the type or scope, the risk is being wrong in estimating or predicting an occurrence and its outcome.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Examples of Operational Risks

Operational risks are potential losses that result from inadequate or failed procedures, systems, or policies. They may be employee errors, systems failures, and fraud or other criminal activity. Some examples of operational risk include:

- **Risk:** Employee exposure to hazardous chemicals (human-made).
  - **Cause:** The manager assumes an employee will follow all safety procedures; however, an employee does not wear proper personal protective equipment (PPE). This may be due to employee negligence, lack of training in safety procedures, lack of proper safety equipment, or failure on the part of management to reinforce safety practices.
  - **Impact:** Could result in injury and possible loss of work time as well as higher worker's compensation costs.
- **Risk:** Active shooter (human-made).
  - **Cause:** Management assumes site security procedures are adequate. An employee who has been terminated gets past site security and begins shooting in the building. This may happen when security procedures and protocols such as terminating access cards, communicating when an employee has been terminated, are not followed.
  - **Impact:** Could result in injury or death for anyone on the property. Physical assets and data security may also be at risk.
- **Risk:** Equipment identified as critical to a business process may fail (human-made).
  - **Cause:** FM assumes equipment has been checked. During a key event hosting 70,000 attendees at a sports arena, critical equipment fails. This may be due to improper installation or a failure to respond to alerts within the electrical system.
  - **Impact:** The attendees are in the dark and panicking, which could result in physical harm to themselves and to employees of the facility. The reputation of the organization may suffer.

People are responsible for most operational risks. By establishing the proper policies and procedures, you can avoid or greatly reduce these risks. You should include a process for monitoring and evaluating the effectiveness of your policies and procedures. For operational risks, the most important elements to consider are safety, personal protective equipment (PPE), quality assurance/quality control (QA/QC) processes and procedures, and site security.

Examples of Environmental Risks

Environmental risks are potential losses due to events in nature or human actions. Some examples include:

- **Risk:** Harm to the environment (human-made).
  - **Cause:** The organization stores its heating oil in an underground storage tank. FM assumes the tank is in good order; however, the tank is old and has an undetected leak.
  - **Impact:** The groundwater is contaminated, and the organization is required to clean up the contamination.
- **Risk:** Harm to the environment (human-made).
  - **Cause:** The organization is retrofitting lighting. The contract states that the lighting contractor must recycle the old fluorescent light bulbs. FM assumes the contractor is complying with the approved disposal practices; however, to save money, the contractor disposes of the bulbs in a landfill.
  - **Impact:** Mercury from the bulbs can contaminate the soil or groundwater. The organization, who is ultimately accountable, may be cited or fined.
- **Risk:** Harm to buildings (environmental).
  - **Cause:** Tornados with high turbulent winds and air-born debris are predicted for the area. According to the safety procedures, the facility manager monitors the situation and moves building occupants to the building's interior when the threat becomes imminent. Soon after, there is a touchdown near the facility.
  - **Impact:** The facility sustains damage to the roof, windows, and building exteriors and a loss of power.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 3: What is Risk Management?

Lesson 3: Objectives

On completion of this lesson, you will be able to:

- Identify what is required to manage risk.
- Demonstrate your understanding of risk management.

Risk management

ISO 31000 also describes the Risk Management Process (RMP) as the systematic application of policies, procedures, and practices to a) the activities of communicating and consulting, b) establishing the context, and c) assessing, treating, monitoring, reviewing, recording, and reporting risk. The goal of risk management is to actively minimize and control uncertainty in an organization.

Risk management applies to:

- People – the safety of occupants, visitors, employees, and service or contracted personnel
- Supply Chains – the prevention of disruptions in the delivery of materials and services
- Products & Services – the protection of products and services that occupants, customers, and clients depend on
- Financial Assets – the protection of financial assets and systems owned by the demand organization and its occupants
- Physical Assets – the protection of facilities, equipment, grounds, and personal property
- Intellectual Assets – the protection of digital and physical stored data and records
- Brand Image – the preservation of a positive public and media opinion of the demand organization

Risk management is a basic part of management and decision-making. It is integrated into the structure, operations, and processes of the organization. The FM risk management strategy must support the demand organization's risk management plan. At the functional level, this means that you will contribute to various elements of risk management. For example, you may conduct audits to identify situations that could be a threat to the

building and occupants. In the event of a chemical spill, you may be responsible for cleaning up hazardous waste. You may even own some of the functions, such as managing an emergency response team. The FM team might handle a situation until the first-responders, or the incident-response teams arrive.

Risk Management Process

Risk management is an integrated process as shown in Process for Risk Management.

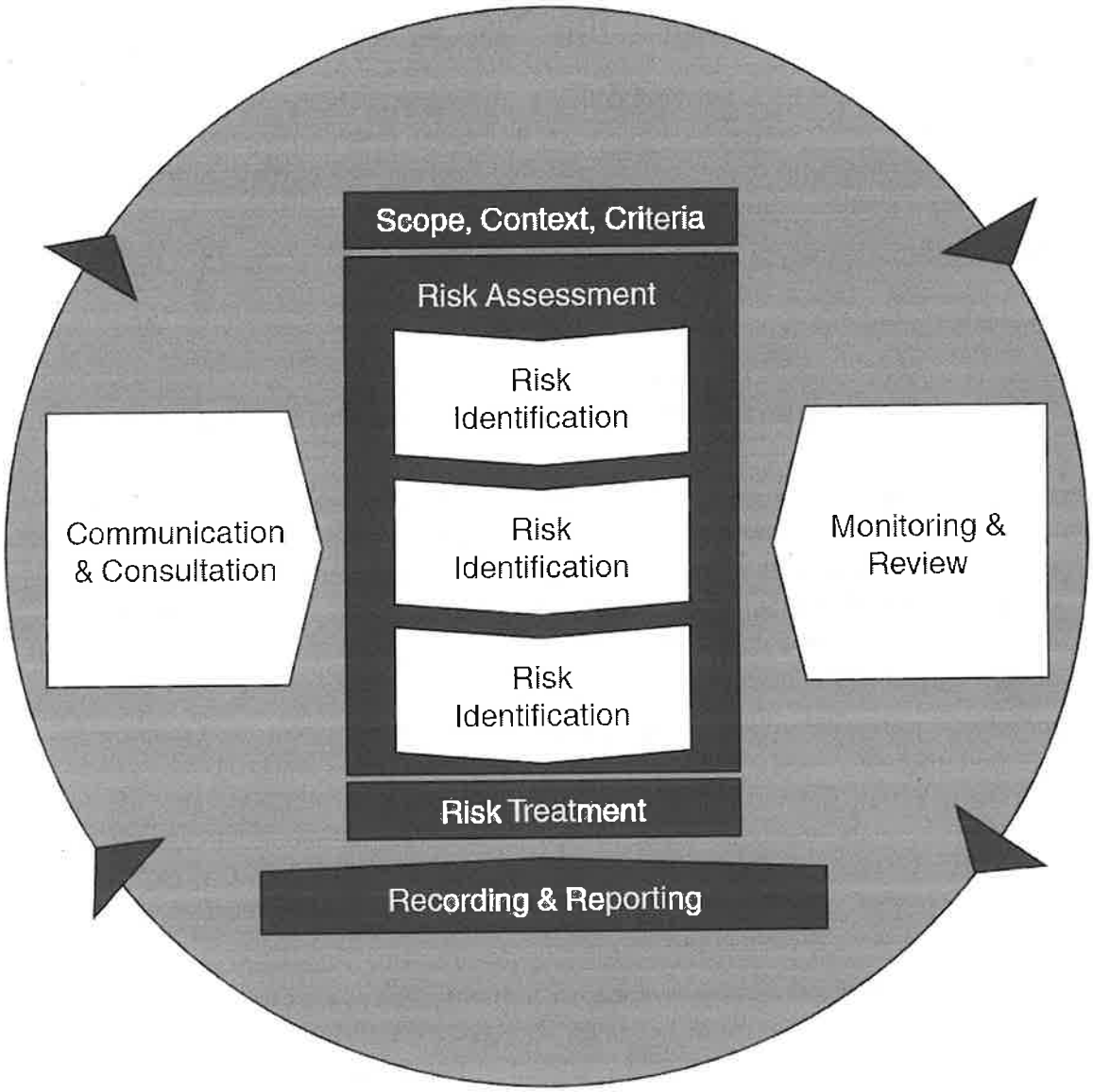


Figure 1 Process for Risk Management.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Key elements of the risk management process include:

- **Threat Identification Process.** If the FM team does a great job of identifying risks or threats to the facilities and ways to minimize or eliminate those before an incident occurs, everyone wins.
- **Risk Management Planning Process.** This is done at the strategic level of the organization. It is a high-level plan that is integrated into all organizational activities. FM may or may not be responsible for developing the strategic risk plan, but is a stakeholder in the planning process.
- **Business Process Analysis (BPA).** This is a subprocess of the overall risk management planning process. It is a step-by-step way to evaluate every element in performing a function. One key activity in risk management planning is to determine which functions are most critical to the demand organization. These are functions that cannot be paused or can only be paused briefly with a backup plan in place. The BPA captures the processes, workflows, systems, resources, controls, and personnel needed to conduct those functions.
- **Business Impact Analysis (BIA).** The BIA uses the information gathered in the BPA to predict what may happen when a disruption occurs. FM can use this to determine strategies to handle these disruptions.
- **Emergency Response.** An emergency is a situation of grave risk to health, life or the environment. It requires quick response to prevent the situation from getting worse.
- **Emergency Response Team.** At the site level, this is usually the facility manager's responsibility. You may be responsible for putting together an emergency response team (ERT). The members of the emergency response team receive specialized training, such as first aid and cardiopulmonary resuscitation (CPR). This team would address any operational issues that occur, such as a chemical spill, weather-related disaster, or a medical emergency.
- **Incident Command System.** Some emergencies require responses from multiple agencies, including local government, the private sector, and others. The Incident Command System defines the roles and responsibilities for managing such emergencies. In these situations, you may act as a first responder until the incident management team is on site, and you turn over control to them. You may also provide information, such as the layout of a building, gas or power controls, or possible hazardous chemicals on site.
- **Business Continuity Planning Process.** Disruptions to business can occur at any time, and organizations must be prepared to manage them. Business continuity plans identify the procedures to follow in the event of a disaster. The output of the planning process should include a timeline for action and instructions for restoring organization operations. To create and test these plans, you will need skilled personnel, access to vital records, and alternate recovery resources, including facilities. You should be able to adapt business continuity plans to the size and

impact of the event. For example, a tornado may blow out windows, damage part of the roof, or destroy the entire building.

Business continuity planning includes the "return to work" process. As the facility manager, you are responsible for worker and occupant safety, and for ensuring that the facility is fully operational for the organization. For that reason, you may be responsible for the requirements for resuming work. This may be a staged process, where essential functions come online first, progressing to full functionality for the entire organization.

- **Disaster Response Process.** Disaster response is a subprocess or a part of the business continuity plan. It is what happens after an event occurs. FM plays a key role. For example, immediately after the incident, to ensure occupant safety, FM may be responsible for controlling access to the site. Coordination with other departments will be necessary, such as IT, to help restore services. FM protects the organization's assets, both human and physical.

A facility manager plays an important role in risk management, particularly in the safety of occupants and the protection of assets. FM must ensure that operations go on and business continues as usual. In the demand organization, FM may or may not own the risk management process, but should participate in the development of the principles, framework and processes that the demand organization establishes.

Throughout the process, ongoing communication is important, both between leadership and the facility managers, and among individual department managers. The organization's risk position should be reevaluated regularly, and every time there is a change to the risk profile. If the risks have shifted, if the organization's strategy has changed, or if the risk strategies have proven ineffective, repeat the risk identification process.

Organization leadership should consider this information along with their attitudes about risk appetite and risk tolerance. They will assess the risk relative to the overall business plan. For example, they will have a different response when there is a high risk to a product line that is about to be discontinued as opposed to a service that is expected to grow substantially.

Governance and Policy

Many organizations have developed formal risk policy and governance frameworks to maximize the benefits of change while minimizing the outcomes of associated risks. The goal of such governance and policy is to provide a guidance structure to risk decisions to help an organization cope with risks in uncertain or complex situations. (Florin & Burkler, 2017). Risk governance is more than just risk analysis; it looks at risk through the lenses of

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

public health, the law, politics, social convention and more. It is the basis of risk decisions for the organization. (CIO Index, N.D.)

The International Risk Governance Council (IRGC) has published the IRGC Risk Governance Framework, which utilizes an iterative and cyclical model incorporating pre-assessment, appraisal, characterization/evaluation, and management integrated with communication, stakeholder engagement, and context discussions. ISO 31000 also provides guidelines, techniques, and vocabulary for risk management. Resources for making effective use of the standards in specific cases exist but not in the standards themselves.

The principle behind risk governance and policy is that systems must be in place to enable decision-making and management of risk in a way that conforms to the organization's strategy and culture. The structure enables the organization to set risk limits, understand its exposures, and make decisions for handling risk before an emergency arises. Development of risk governance and policy may already be in place within the organization or may be developed concurrent with risk management planning.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 4: Building Risk Awareness

Lesson 4: Objectives

On completion of this lesson, you will be able to:

- Outline the organization's risk awareness and culture.
- Understand the organization's level of risk tolerance.
- Understand how to build a culture of risk awareness.

The facility manager is in an ideal position to raise the awareness of the importance of risk management, including what risks are, what the potential impact might be, and what are the available treatments. Building risk awareness should begin with the FM function. To help build awareness, engage personnel from those firms that supply services to the FM function, or engage personnel from key functions within the demand organization. The goal is to create a shared understanding of what constitutes a risk, what the probabilities are of it occurring, and what are feasible treatments.

For example, one strategy for building awareness might be to combine informative briefings with "what-if" scenarios designed to facilitate discussion and get consensus on response tactics.

- The briefings might be short repeating telecasts shown in lunchrooms or public meeting spaces.
- The scenarios could be invitation only to key contractors or key demand organization personnel to meet virtually every other month. A facilitator sets up the "what if..." scenario based on one type of threat (climate or technology related for example), and then guides the discussion. Once the recommended response tactics are documented, they become the responsibility of FM to set up a project team to further refine them.

Another strategy for building awareness is to engage existing groups in identifying threats and hazards.

- The demand organization sponsors a wellness initiative that encourages a healthy lifestyle and regular exercise. Many employees participate in the walking club that "hikes" before work, during lunch, or after work. Depending on the weather, they walk either the surrounding grounds or the hallways in the buildings. There are markers at specific distances letting the walkers know how far they have walked. The FM approaches the walking club to help identify hazards that might cause falls such as broken sidewalks, and debris or water on the path. Walkers are also encouraged to notify FM or security if they see strangers or anything unusual.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- FM sponsors annual contests that engage personnel in creating posters, videos, slogans, and the like reminding people to be safe, think safe, and report concerns.
- The emergency response teams meet at pre-set intervals to conduct walkthroughs of existing disaster procedures to confirm they are complete, clear, and actionable.

Developing a Risk Acceptance Culture

Several factors contribute to shaping an organization's response to risk, including the environment in which it operates, its history and experiences, and its management style and expectations. How that organization views and handles risk is its risk management culture. Risk culture includes a demonstrated tolerance, acceptance, and even appetite for risk.

Individuals in FM and the demand organization may view risk differently. The high probability of surviving an event might encourage them to accept the risk, as in do nothing. If the risk carried extreme financial and image consequences, they might not be willing to accept it. Instead, they may want to support actions designed to avoid or mitigate the damage.

A risk acceptance culture is not binary. People are not risk-averse versus risk-accepting. Instead, their view of risk is a continuum and where they fall along that continuum depends on what they believe is at risk and their perceived level of uncertainty over the probability of loss or damage.

To better understand your organization's risk culture, think about how the demand organization and FM handled events in the past. Was leadership proactive? Did leaders take the time to identify potential risks before an event occurred? Was leadership reactive? Did it wait for events to occur before committing resources to respond? The organization's culture will determine the amount of attention, resources and tools it will make available to identify and manage risk.

Chapter 1: Progress Check

1. Why does FM need to identify risk? (Choose the best response)

   a. To discover risks and vulnerability that will impact the organization from achieving their objectives.
   b. To allow FM to put plans in place to raise awareness of the potential risks in the organization.
   c. To discover, find and describe the risks and vulnerabilities that might help or prevent an organization from achieving its objectives.
   d. To discover any vulnerabilities to the FM organization.

2. The three types of sources of risks are:

   a. Environmental and climate, bio-chemical and technological risks
   b. Human-made, environmental and climate, and technological risks
   c. Bio-chemical, organic, human-made and technological
   d. Organic, environmental and climate, and human-made

3. Answer True or False.

   Non-Compliance with government or governing industry standards is a human-made risk.

   a. True
   b. False

4. Answer True or False.

   Estimations or occurrence predictions and outcomes do not form part of tangible or intangible sources of risk.

   a. True
   b. False

5. Risk management is applied to which of the following elements:

   a. People and intellectual assets
   b. Products & services and physical assets
   c. Supply Chain and financial assets
   d. All of the above

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

6. In the event of a chemical spill:
   a. FM is always required to clean up hazardous waste
   b. FM may be responsible for cleaning up hazardous waste
   c. FM may not clean up hazardous waste ever
   d. The demand organization cleans up all hazardous waste

7. What is a high-level activity that is integrated into all organizational activities, and is done at the strategic level of the organization?
   a. Business Process Analysis
   b. Risk Management Planning Process
   c. Business Impact Analysis
   d. Threat Identification Process

8. Business Continuity planning includes:
   a. A return to work process
   b. A first responder plan
   c. An emergency response team
   d. A business impact analysis

9. Name two external resources that can help identify risk.
   a. Government bodies and first responders
   b. Employees and risk management expert consultants.
   c. Insurers and company records
   d. Other facility managers and senior management

10. Risk management is applied to which of the following elements:
    a. People and intellectual assets
    b. Products & services and physical assets
    c. Supply Chain and financial assets
    d. All of the above

Chapter 2: Risk Management Planning

Lessons

- Objectives
- Lesson 1: Risk Management Planning

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Objectives

Chapter 2: Objectives

On completion of this chapter, you will be able to:

- Determine risks in terms of their likelihood of occurring and severity.
- Understand how to prioritize the level of response.
- Select an appropriate risk treatment.

This chapter is about being proactive in your approach to managing risk. It explains the importance of aligning the FM risk management strategy with that of the demand organization. The focus is on identifying risk and deciding on how to respond before the risk occurs.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 1: Risk Management Planning

Lesson 1: Objective

On completion of this lesson, you will be able to:

- Determine risks in terms of their likelihood of occurring and severity.
- Understand how to prioritize the level of response.
- Select an appropriate risk treatment.

Well-managed organizations have high-level risk management strategies. These strategies influence risk management plans for each of their functions, including FM. To ensure that the FM risk management plan is aligned with that of the demand organization, you must understand the demand organization's risk management goals and strategies.

A facility manager should be directly involved in managing risks to the FM function. A risk assessment should be conducted and a facility risk management plan developed. The facility manager must be prepared to support requests for the funding of risk management initiatives and help senior management understand the impacts of the facility risk factors.

By understanding the infrastructure that supports the demand organization's work, the facility manager is in a unique position to help management examine the organization's risk-tolerance factor.

Strategic priorities change over time. If risk management activities do not keep up with these changes, any efforts can become less effective and end up reacting and trying to comply with regulations rather than being strategic and preparing for threats.

In addition to its 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. If the risk management program initiatives are managed independently by each function, organization-wide issues may suffer.

Communication between senior management and FM is critical. It will help keep the focus on the same goals, prioritize projects to meet those goals, and fund those projects to provide the necessary protection against the risks.

With good risk information, an organization can manage risk well and act responsibly to protect its stakeholders and assets. To create a sound risk management plan that matches the demand organization's strategy, the facility manager must:

- Identify the kinds of risks that can occur for example, power failure, bad weather, flooding, fire, failure of structural elements, how often they occur, how likely they

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

are to occur, and the severity of the impact to the demand organization and its core business functions.

- Determine where the organization's structures and infrastructure are vulnerable to these risks.
- Determine how damage to facility equipment and systems, or disruptions in FM services, would impact key organizational functions.

These decisions cannot be made in a silo. An organization's best defense against negative risk outcomes is a comprehensive approach to risk management and a recognition of how risks are interconnected. Any risks identified by the FM organization should be communicated with leadership, individual department managers and other key stakeholders. This will inform their own decisions relative to the overall business plan and ensure a successful risk management strategy.

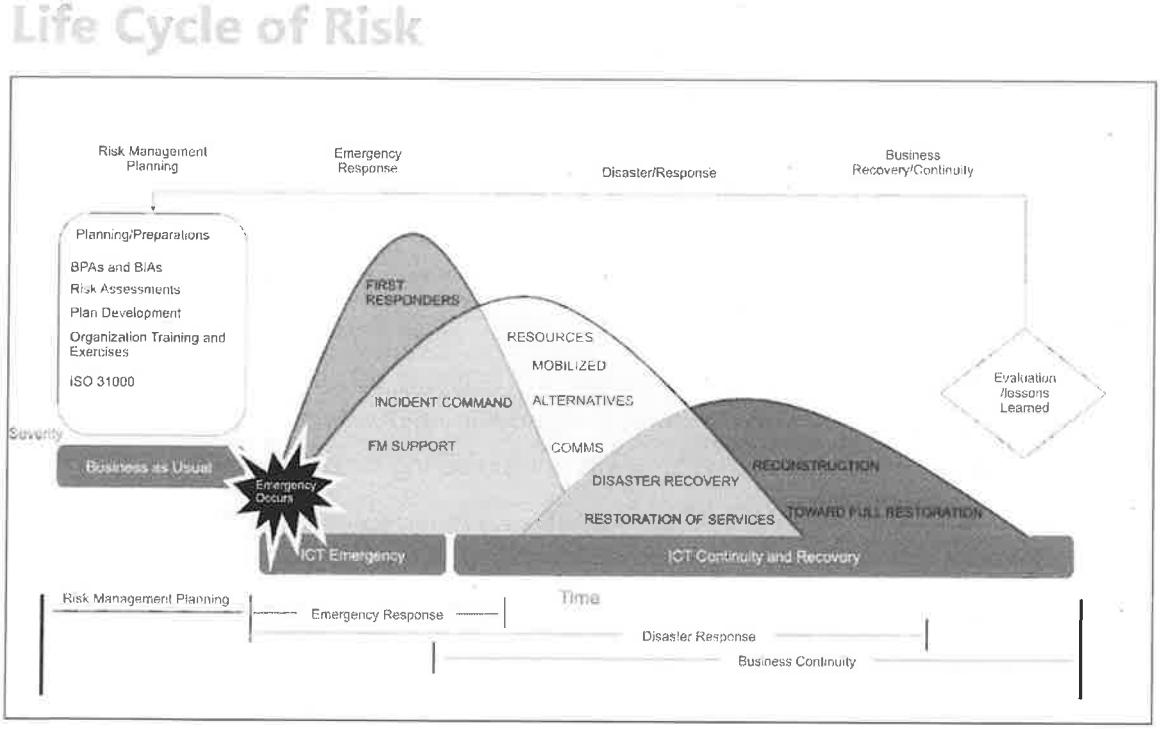


Figure 2 Life Cycle of Risk

The life cycle of a risk incident is shown in Figure 2. This life cycle has four phases that unfold over time. In each phase, and for each organization, the FM roles and responsibilities will vary. The four phases overlap and are:

- Risk Management Planning
- Emergency/Incident Response

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- Disaster Response/Recovery
- Business Recovery/Continuity

The focus of this chapter is on risk management planning. Emergency/Incident Response and Disaster Response are discussed in Chapter 3. Business Recovery/Continuity is discussed in Chapter 4.

Planning Phase

Risk management planning is the:

- Identification and prioritization of threats or risks.
- Evaluation of the probability of their occurrence and severity of the impact on the demand organization's operations, assets, occupants, and neighboring community.
- Implementation of strategies or treatments that avoid or minimize the probability of an occurrence of a threat and the impact if it should occur.

Risk management planning has two main goals:

- Identify risks
- Prevent these risks from occurring, or mitigate or minimize their impact

This phase lays the foundation for the other phases of the incident life cycle. Decisions made in the planning phase affects what happens later. Planning and preparation include:

- Physical asset and human resource risk analysis.
- Business process analysis.
- Plan development.
- Organizational training, with exercises and/or simulations.
- Planning for scenario testing and exercising the emergency response plan. This includes plans for disaster response/recovery and emergency communication.
- Planning how to sustain essential business processes during and immediately after the incident (i.e., business continuity).

During the planning phase, you will have a list of potential risks for your situation. These include risks specific to your region, your type of organization, your facility, your business-critical equipment and processes, and risks related to your contractors and service providers. Once you identify the risks, you need to analyze them to determine which ones pose significant short-term and long-term threats to the organization.

During the planning phase identify the essential processes that must continue without interruption or recover quickly. The organization then assesses how prepared it is for an

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

emergency and develops plans to meet its goals. Those plans must comply with local requirements.

To protect itself, an organization must have a thorough, in-depth approach to risk management and must understand how risks are interconnected. For example, in today's global and highly connected economy, even the most isolated business is likely to have some connection to businesses across the world. A major disruption in one country can stop or stall projects in another. Here are some examples:

- Supply chains are complex. An organization may not know all the players in that chain, or what it takes for those players to deliver a product or service.
- An organization's cloud storage may be local or could be anywhere in the world.
- A utility company may suffer a cyber-attack, causing loss of services to the organization.
- A corporation's major supplier may suffer a ransomware attack, causing the loss or violation of data privacy. This would affect the organization's reputation as well as its ability to provide essential services. (Parasuraman, Kamban. 2019, May 20)

The risk management planning process helps the organization anticipate and protect itself from risks. Even within a facility or an organization, risks are interconnected. Consider the example of a facility in a region with a heavy rainy season. During one rainy season, a membrane roof patch fails, and the damage goes undetected. Water from several minor rainstorms penetrates the multiple layers between the roof membrane and the interior ceiling. Finally, a major storm floods the roof, forcing water through the ceiling and causing it to collapse over the organization's data center. A proactive risk management strategy would prioritize frequent inspections of the exterior to check for potential failure points due to the high likelihood of water damage. It might also specify insulating or patch materials to be available.

Analyze Risks

Risk analysis is the process of identifying potential risks, determining the probability of them happening, calculating the impact of their occurrence, and determining ways to avoid, prevent, or mitigate the occurrence. The goal is to understand how the risks affect the demand organization as well as the FM function.

The facility manager can decide how detailed and complex the risk analysis needs to be. The purpose of the review, as well as the availability and reliability of the information, should guide the decision. Use techniques that focus on quality, quantity, or both. When analyzing the risks, consider these factors:

- What might cause the risk to happen?

- How likely is it that the events will occur? (Refer to history and or predictions.)
- How severe might the financial consequences be? What is the impact to core business functions? Consider both direct and indirect costs.
- How severe might the human and physical consequences be?
- How complex and interactive are the business relationships? How do the various departments within the organization, employees, visitors, other stakeholders, and area residents depend on each other?
- Which factors are time-related?
- How effective are the controls (protections and back-ups) that are currently in place?
- How might the employees react? How might it affect the brand's reputation?

When a risk is hard to evaluate, quantitative and qualitative analysis will help you better understand the potential impact. Use data from expert research and from benchmarking studies done for similar facilities to help guide your analysis. Members of the team doing the analysis may have their own biases, opinions, and perceptions of the potential risk. Data can help overcome this bias.

For each risk that is identified, a team estimates the likelihood of the threat and determines the impact that event would have on the core business. The members of this team should be subject matter experts and representatives from all related functions who would understand the severity and likelihood of the hazards. Risks that pose a threat to life, safety, or health should be assigned a high priority. For certain risks, such as those related to weather, you may find data to help determine how likely the event is to happen.

Here are two examples of risk analysis:

Example 1:

Categorize risks either by who or what is impacted (e.g., people, facilities, or technology) or by the potential cause (e.g., environment, human, or technology). Grouping risks this way, may help the team think through the likelihood and impact of all those potential threats. The group can decide on the rankings for example, 1 being low and 5 being high. They can also decide how to calculate the score, for example multiply the likelihood by the severity. The output of this process is a matrix that shows how the priority was determined, as seen in Table 1: Example of Risk Analysis Matrix below.

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority
Environmental hazard occurs during renovation or remodeling.	3	3	9	2

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Occupants have a bad reaction to odors from paint fumes and floor epoxy.	3	4	12	1
The temperature in the reconfigured space cannot be regulated.	3	1	3	3

Table 1 Example of Risk Analysis Matrix.

Example 2:

You might decide to use a four-quadrant grid to assess risk as shown in Figure 3: Example of Risk Analysis Grid using the same example as shown in Table 1.

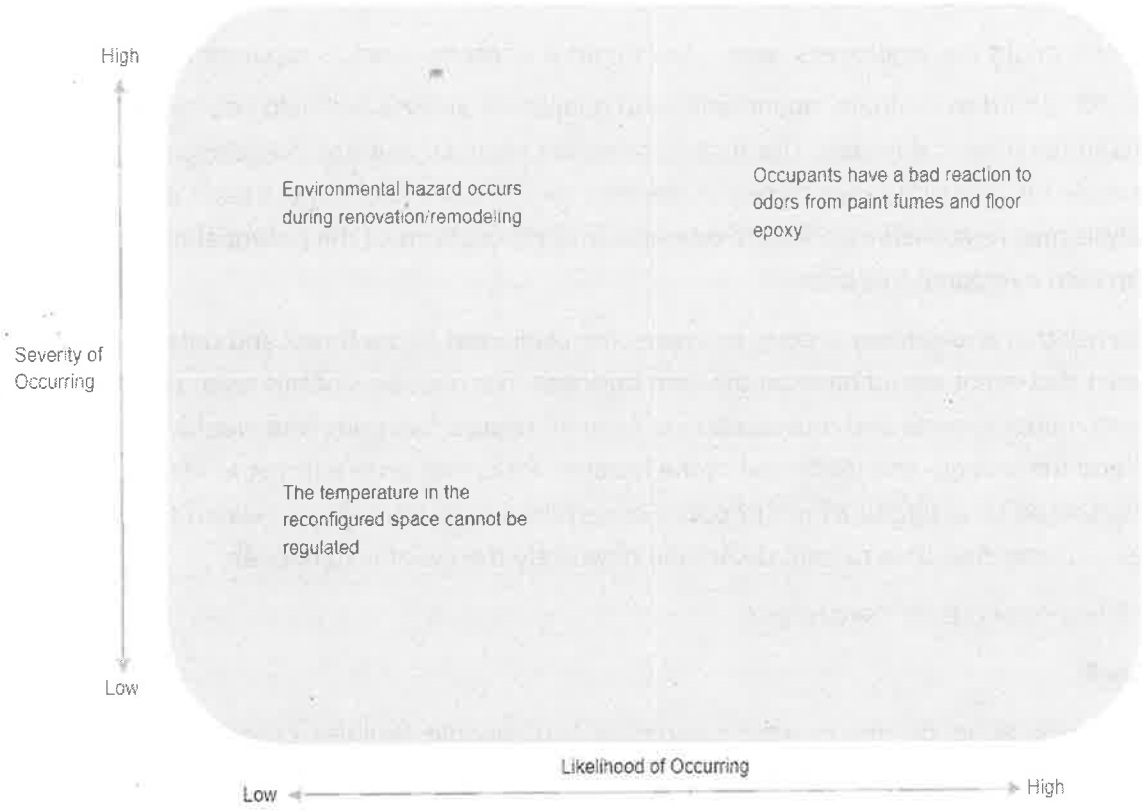


Figure 3 Example of Risk Analysis Grid

These are just two of the tools you might use to help assess risk. You can find variations by searching online or within your own company's Risk Management Department/Corporate Security. You may even create one that suits your needs. The point of all variations is the same: 1) identify risks and classify them by their level of threat – how likely they are to occur and 2) estimate the impact on the organization if they were to occur.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

While doing the risk assessment, always keep in mind the strategic objectives and business needs of the demand organization. This demonstrates your commitment and ability to protect the interests of the demand organization. It also provides support for your budget requests.

After assessing the risks, you need to evaluate them and determine the risk treatment strategy – or how to handle each risk.

Evaluate and Treat Risks

Treating risks means putting plans in place to either stop the risk from occurring or minimizing the impact of the event. The team must consider, or evaluate, the impact of the risk and the cost of the treatment. To do this, the facility manager must understand the organization's risk tolerance, or its "readiness to bear the risk after risk treatment, in order to achieve its objectives." (ISO/Guide 73:2009 Risk management – Vocabulary)

ISO 31000 uses the term "risk treatment" for the series of repeated steps used to evaluate and determine the organization's strategy for handling a risk:

- Formulate and select possible actions to take.
- Quantify the costs, process impacts, pros, cons, appropriateness, and consequences of each possible action.
- Identify the most appropriate risk treatments.
- Plan and implement the risk treatment.
- Assess the situation to determine if the treatment worked.
- Determine if the remainder of the risk is acceptable and conduct further treatment if necessary.

The goal of every risk treatment strategy is to tolerate, avoid, prevent, mitigate, or transfer risk. Here are some risk treatment strategies to consider:

- **Tolerate** the possibility that the event will occur and accept its possible impact. A do-nothing strategy when the likelihood of occurrence or the severity of the threat is low can be selected. For example, in the risk matrix, the facility rated the overall risk associated with not being able to regulate the temperature in the reconfigured space as low because an audit of the building showed this location as having proper airflow.
- **Avoid** the risk. Choose this strategy when the risk is highly likely, and its impact is higher than any off-setting benefits. The risk is avoided by taking actions so that the threat goes away. For example, due to the number of employees working from home, an organization plans to reduce the size of its data center. This change will reduce HVAC load and return open workspace to the IT Division. The data center is

mission-critical; however, the cabling complex and the equipment is sensitive to dust contamination. The organization wants to avoid contamination; therefore, the organization decides to build and fully mobilize a new data center in a different space within the unit. Once the old data center is vacant, the space can be renovated for reuse.

- **Prevent.** The goal is to greatly reduce the likelihood of an event occurring. Tactics include preventive maintenance to reduce the likelihood of equipment failure and redundancy. For example, backup power systems (power generators) or placing equipment with the same capabilities in multiple locations. Locating electrical panels on higher floors to reduce the water damage when you are in a flood-prone area is an example.
- **Mitigate.** This strategy can lessen a threat when a risk cannot be avoided or tolerated, or when the benefits outweigh the risk. The goal is to lessen the impact or severity of an occurrence. For example, an organization can have compelling business reasons for its presence in a high-crime area. They may take steps to mitigate or lessen the risk:
  - Provide high-security fencing with card-reader access for staff vehicles.
  - Install closed-circuit cameras with live monitoring around the perimeter and install signs warning of the surveillance.
  - Install an alarm system in the facility that would notify an approaching employee of a breach.
  - Provide staff at the front desk with a panic alarm.

  High-level strategies for risk mitigation include alignment with standards, proper planning, emergency preparedness, and following best practices. Consider tactical steps, such as facility audits, critical system identification, and cyberspace management.
- **Transfer/share** the risk. Choose this strategy when the risk cannot be avoided and the impact is significant. Risk transfer strategies may include:
  - **Insurance**, in which an insurer accepts potential losses in exchange for a fee. Insurance does not get rid of the business risk. For example, fire insurance will replace or rebuild the facility, but the time interruption (construction period) is a loss the organization must still bear. Consult with an asset-liability expert to ensure an understanding of the possible restrictions for each type of occurrence.
  - **Contracting**. For example, by installing a community floodwater diversion system, the contractor and the organization share risks associated with increased costs to prevent or mitigate flooding.

After the risk treatment strategy is determined, another risk analysis is done. To provide data to support the strategy chosen, additional columns can be added to the matrix. See Table 2 Risk Analysis Matrix.

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority	Risk Strategy	Assigned to:
Environmental hazard occurs during renovation or remodeling.	3	3	9	2	Prevent	FM
Occupants have a bad reaction to odors from paint fumes and floor epoxy.	3	4	12	1	Mitigate	FM
The temperature in the reconfigured space cannot be regulated.	3	1	3	3	Tolerate	NA

Table 2 Risk Analysis Matrix

Once the strategy is determined, document it, communicate it, and validate it with the appropriate functions and stakeholders in the organization. Distribute the data so that the entire group can analyze the risk strategies. The results are critical in supporting decisions about how to allocate limited risk prevention and mitigation resources

As a facility manager, you must consider risks related to the facilities and grounds, and how they will impact the demand organization, the occupants of the facilities, the relative stakeholders, and the surrounding environments.

Case Study #1: Talent Management or Bench Strength – Treatments are Mitigate and Prevent

The facility manager was told that one of his long-time employees is about to retire. This caused the facility manager to reach out to HR to ask for a report on all facility staff tenure. The manager discovered that two-thirds of his staff were eligible to retire within the next 36 months. The manager began to consider the implications of those positions becoming vacant – How long before a replacement can be hired? Are there people currently in the company who are ready to step into these roles?

HR reported that it would take a long time to fill the positions as few people had the required skills. FM then collaborated with HR and Training to develop a talent management plan. The plan included formal training, rotating job assignments, and mentoring. Next, FM and HR identified talent within the organization to participate in the talent management initiative. The analysis might look like Table 3: Risk Analysis Matrix.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority	Risk Strategy	Assigned to:
Loss of key personnel	5	4	20	1	Mitigate	HR

Table 3 Risk Analysis Matrix

More to the Story

The facility manager decided to apply the same thinking to service contractors. He identified those contractors the organization most depended on and whose absence would put the organization at risk. He asked what would happen if a contractor was unable to fulfill a commitment? Did the contractor have a succession plan in place? Were there other contractors who could step in when required? He discussed the importance of having a succession plan in place and talent development with key contractors. He also began to build relationships with other contractors. See Table 4 Risk Analysis Matrix.

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority	Risk Strategy	Assigned to:
Loss of key contractors	3	5	15	1	Prevent	FM

Table 4 Risk Analysis Matrix

Case Study #2: Autoclaves – Treatments are Tolerate, Prevent, and Avoid

The organization manufactures composite materials. One building houses two large autoclaves that are adjacent to each other. The autoclaves are used to cure the composite materials. Run times can be up to 14 hours. Both autoclaves have hundreds of tubes that pump gas into them. There are valves that maintain the density of that gas. Engineering sets the formula specific to the material being cured. The formula specifies the internal temperature, the pressure in pounds per square inch, and the length of time the materials are enclosed in the autoclave. If the autoclaves do not sustain the required temperature and gas density, the composite materials may be ruined. FM is responsible for maintaining the autoclaves and the building where they are located.

After a while, the tubes can develop small leaks due to wear. When this happens, the autoclave cannot be operated at its full potential. The cost to reseal the tubes and replace the gas is high because 1) the repairs must be done by specially trained craftsmen, 2) the work can only be done when the autoclaves are not in use, and 3) the time required to do the repairs is often longer than one eight-hour shift resulting in overtime.

Nonetheless, the risk treatment strategy was decided to tolerate the loss because of the high material and labor costs. Also, this decision was supported by the reality that the autoclaves are rarely run at full capacity, but only to the level sufficient for the job. It is like owning a racing car that does not run on all its cylinders. However, missing a few cylinders does not matter because the car is only driven to the grocery store. Therefore, this risk strategy of toleration only works if the autoclaves do not have to run at full capacity.

In time, due to wear, the autoclaves will need to be serviced. When this happens, they are either temporarily put out of commission allowing the craftsmen access or they are decommissioned.

More to the Story

Because of the size of the autoclaves, a person can get inside them. If a person were to get trapped inside, they could die. The risk strategy for safety was to avoid the risk by requiring emergency latches inside each autoclave to prevent a person from getting locked in. This safety feature was tested frequently.

More of the Story

The facility is located on a fault and is prone to earthquakes. Having two autoclaves provides some redundancy should one fail or be damaged. However, having them adjacent in the same building diminishes the effectiveness of a redundancy risk treatment strategy. FM worked with engineering to identify other locations outside of the fault area that had autoclaves and could satisfy this location's requirements if needed. See Table 5: Risk Analysis Matrix.

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority	Risk Strategy	Assigned to:
Equipment failure	2	5	10	3	Tolerate	FM
Safety of personnel trapped	3	5	15	1	Prevent	FM
Earthquake	3	5	15	2	Avoid	FM

Table 5 Risk Analysis Matrix

Case Study #3: Nuclear Pumps – Risk Avoidance

The nuclear plant has hydraulic pumps that emit a signal when they are about to fail or require service. The alarm only goes off every 9 to12 months. The labor contract specifies that repairs and service can only be performed by an engineer. When the pump emits the signal, the engineer has three hours to do the repair. After that, the pump begins to release nuclear contaminants. The process of repairing the pump is very prescriptive. The engineer

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

must execute the steps precisely. Doing the steps in the wrong order or forgetting a step would subject the engineer and possibly others to nuclear contamination. The engineer must also use tools designed specifically for the task. The engineers are trained in how to do the work. However, because the application of the training is infrequent, those who were trained do not accurately recall the procedure.

In the past when an alarm went off, the plant manager asked who was trained. If no trained engineer was on site, she called engineers who were at home. At the same time, engineers on site began searching for the tools. Who used them last? Where are they kept?

The plant manager reached out to FM and Training to come up with a solution. Training developed a short video that demonstrated each step of the process. Training also created a diagram showing every part and step in the process. The diagram was laminated to prevent tears and smudges. FM built boxes that were attached to a wall near each pump. FM arranged for redundant power sources to the box. The boxes housed the video, the diagram, and a complete set of tools. FM also worked with IT to secure the boxes so only authorized personnel could access the contents. See Table 6: Risk Analysis Matrix

Risk	Likelihood (1-5)	Severity (1-5)	Risk Score	Priority	Risk Strategy	Assigned to:
Nuclear contamination	2	5	10	1	Avoid	Tema

Table 6 Risk Analysis Matrix

KPIs and KRIs as Predictors

Both **key risk indicators (KRIs)** and **key performance indicators (KPIs)** support the organization's risk management strategy. Both indicators provide metrics for the demand organization's risk management strategy as well as for the FM department. **KPIs** measure the performance of key processes and systems - how well something is being done or functioning. They measure what has already happened and are often considered **lagging** indicators, because they are after the fact. However, the information generated can be used to predict future performance because they may signal an emerging problem, thus making the information a **leading** indicator or a **KRI**.

For example, an organization may use the volume of service calls (a KPI) to measure the performance of its equipment. An unexpected 20 percent increase in service calls for a specific piece of equipment may signal a potential failure of a critical part. An FM organization that recognizes the service trend as a risk indicator can take steps to prevent the failure of that piece of equipment or prepare to replace the equipment before it fails.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Another example is using the number of occupant complaints as both a measure of customer service (a KPI) and as a risk indicator (a KRI) of poor customer service. If occupant complaints increase, there is some likelihood of a larger problem. Organizations use KRIs to get an early signal of increasing risk exposure in various areas of the enterprise.

The same concept applies to evaluating risk exposure related to an operational or environmental hazard, a technological threat or any other organizational risk. KRIs can be identified, measured and tracked to guide the organization's response to risk. You can also use them to identify necessary changes before these changes become critical. This will enable actions that will prevent or minimize the material loss caused by the risk factor.

When a process is measured, it will affect another process which is also being measured. This provides insight into future performance. KPIs must be actionable; responses to KPIs can be corrective actions. More detail regarding KPIs can be found in the ***IFMA's Performance and Quality Core Competency Course***.

Planning: Asset and Human Analysis

The first step to planning is to inventory the physical and human assets FM is expected to manage and protect. The inventory can be as simple as a list of building systems (HVAC, plumbing), equipment (boilers, chillers, trucks, forklifts), and FM personnel (craftsmen, maintenance, administration, computer techs). Next is to collect information that helps you identify possible risks as in equipment failures.

One approach when inventorying equipment, systems, and buildings is to ask your craftsmen and maintenance personnel to rate each item on a scale of A, B, and C. A means all is good, do nothing. B means things are okay but pay attention. C means act, as in repair, replace, or do a major overhaul by a given date. You can verify the ratings and budget for the suggested actions. A side benefit is this strategy engages your staff. Maintenance and craftsmen are closest to the work. It also gives you a picture of future risks if not acted on in a timely fashion. See Table 7: Sample Inventory and Rating.

1. Create a chart in Excel or some other data base system to list key equipment, systems and buildings.
2. Ask maintenance personnel to rate the equipment, system or building on a scale of A, B or C. They must put in a plan to correct anything rated as a C.

Equipment	Make &Model	Age	Size	Location	What is most important to be aware of	Rating* if C, add your plan
Boiler 1				Bldg 1	Leaks	C. Do a

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

			major overhaul by _____date)
Boiler 2	Bldg 4	Hard to find replacement parts	C. Replace by ____(date)
Chiller 1	Bldg 3	Vibration	C. Shorten the preventive maintenance cycle to once a month

Table 7 Sample Inventory and Rating

You can take a similar approach to assessing your personnel. Your goal is to have an adequate number of qualified personnel to 1) maintain your current buildings, systems and equipment and 2) be able to respond in case of an emergency. See Table 8: Sample Talent Management Plan.

People	Work site Shift	Skill set or special expertise	Risk management strategy
Joe			Cross-train
Jose			Certify
Joey			Ask to be a mentor

Table 8 Sample Talent Management Plan

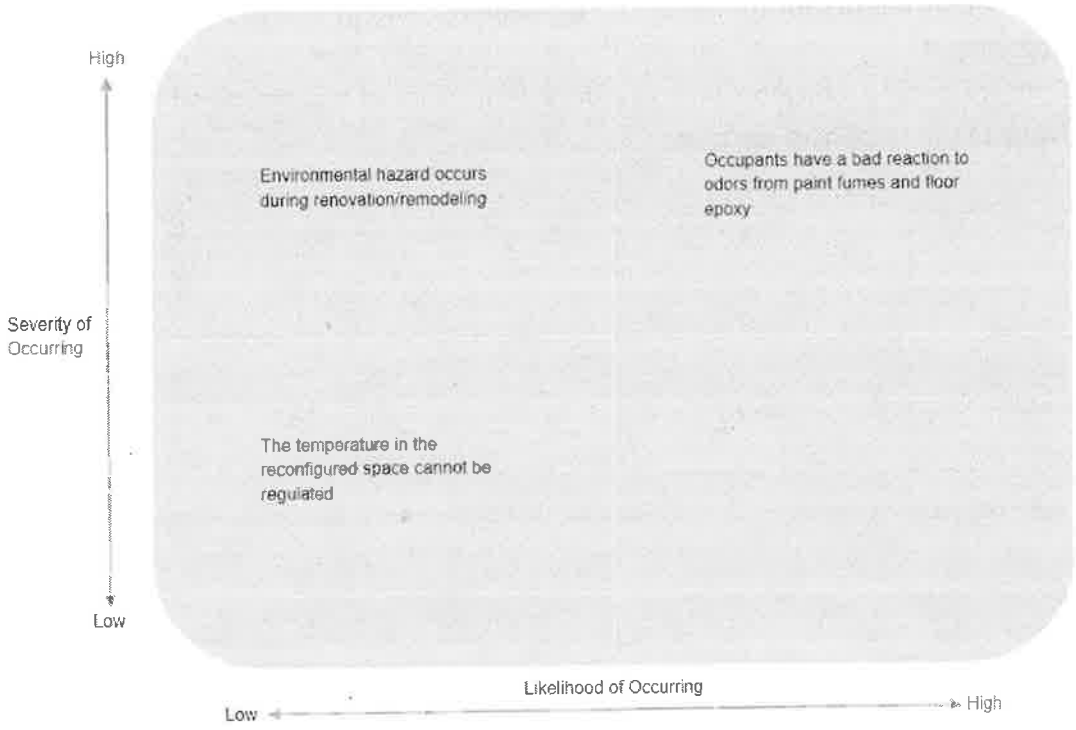
Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Chapter 2: Progress Check

1. What is one of the popular tools used to analyze risk?

   a. Risk analysis matrix
   b. Pareto chart
   c. Cause and effect diagram
   d. Scatter plot

2. What is the name of this tool?



   a. Risk analysis grid
   b. Risk analysis matrix
   c. Risk analysis image
   d. Picture graph

3. Name potential treatment strategies.

   a. Tolerate, avoid, mitigate, leave it alone, contract
   b. Avoid, tolerate, mitigate, prevent, and transfer
   c. Accept it, prevent it, insure it, ignore it, and contract it.
   d. Document, tolerate, share, avoid, and eliminate

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

4. Is the following example a KPI, KRI or another key indicator? Identifying the number of occupant complaints, and adjusting the process based on the results.

   a. KPI
   b. KRI
   c. KRI and KPI
   d. Neither

5. Which of the responses is a true statement about KPIs and KRIs?

   a. Both are lagging indicators
   b. Both supply metrics for the demand organizations strategy as well as the FM department
   c. Both are leading indicators that measure performance of organizational functions
   d. None of the responses are true

Chapter 3: Emergency Preparedness and Disaster Response and Recovery

Lessons

- Objectives
- Lesson 1: Emergency Preparedness
- Lesson 2: Emergency Response Plans
- Lesson 3: Disaster Response and Recovery

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Objectives

Chapter 3: Objectives

On completion of this chapter, you will be able to:

- Determine your current emergency response knowledge and plans.
- Determine what improvements to emergency response are necessary to ensure employee and client safety.

This chapter is about the roles and responsibilities of FM prior to, during and after an emergency. It begins with emergency concepts and terms that facility managers are expected to know when collaborating with first responders. It explains the importance of having a well-designed command structure and the importance of organizing resources (people, equipment, and services) prior to an emergency so you can respond quickly and appropriately. It lists the training you and your staff should get. It provides guidelines about how to build your own emergency response plan. It concludes with information about how to develop your disaster response and recovery plan.

Case Study

This case study will be used throughout this chapter.
When Training Kicked In – Meredith's story

In 2016, over 6,954 fires burned an area of over 669,000 acres across California in the U.S. 1,274 structures were damaged or destroyed and six people lost their lives.

Meredith's organization is located in northern California U.S. The organization developed an incident response plan and business continuity plan as part of the certification for ISO 22301 – Security and resilience – Business continuity management systems – Requirements.

This plan includes:

- Guidelines on when to evacuate and where to assemble.
- Guidelines on when to shelter-in-place.
- Addresses of alternative facilities for work.
- Guidelines on when and how to return to normal.

Meredith never imagined the extent to which this would be tested, but in October 2017, the organization's plans were put to the test when the area experienced unprecedented fires that raged for 100 days.

Sunday

9:45 p.m.: The fire started about 18 miles (29 kms) northeast of the organization's main facility.

Monday

1:00 a.m.: High winds carried the fire southwest to the city limits.

1:30 a.m.: Officials began evacuating neighborhoods.

2:00 a.m.: High winds allowed the fire to jump across a six-lane highway that runs north-south through the city.

3:48 a.m.: Meredith received a call from an employee who said that his spouse needed to evacuate. They had a small child and did not know where to go. Meredith began contacting other employees local to the fire area.

4:45 a.m.: Meredith notified leadership of the situation, and the company's incident response and business continuity plan kicked in. The office affected was officially closed. The organization's communication plan was enacted, where the designated person sent out official communication to the entire organization.

Mid-morning: A large neighborhood northwest of the city had burned.
12:00 p.m.: Two medical centers were evacuated.

End of day: A senior living complex, a winery, a school, and another neighborhood were lost. Other properties sustained substantial damage, and the fire continued to spread.

Power and natural gas were shut off. Neighbors set up watch in the neighborhood and proactively began wetting down roofs. The air quality was so poor that people were advised to stay indoors unless wearing a mask.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Tuesday

The fire was zero percent contained. The organization's official communications coordinator alerted the other offices of the situation.

The fires continued to burn, and people continued to evacuate and shelter. The organization had planned on using two nearby hotels as alternative space for its command center, work areas and possible housing. Both hotels were destroyed.

Wednesday

A neighboring town was evacuated, and the area north of the city was put on evacuation notice.

Meredith returned to the office to find that natural gas was still shut off so there was no hot water.

Thursday

By morning, the fire had burned 34,270 acres (138.685 kms) and was 10 percent contained. The City estimated 2,834 homes and 400,000 square feet (37161 sm) of commercial space had been destroyed.

As the organization's plan dictated, Meredith and other local employees continued to work from home.

Friday

The fire was 25 percent contained.

Saturday

The fire was 44 percent contained.

Natural gas was turned back on in some areas, including Meredith's home.

Damage to residential area

Return to normal

- The fire continued to burn for more than 100 days before it was finally "contained".
- The office was closed for two weeks; however, employees were able to continue to work from home as indicated in the organization's business continuity plan. Employees across the organization were notified by the designated person that the office was open and all employees were returning to the office.
- The office building sustained only smoke-related damage. The landscaping, however, had been singed, and several trees on the property were severely burned. The fire came within feet of the office building's front door.
- The fire event was tough, and it was scary, but the organization's planning helped everyone deal with it in a proactive way. The employees were able to keep going forward and barely missed a beat.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 1: Emergency Preparedness

Lesson 1: Objective

On completion of this lesson, you will be able to:

- Determine your current emergency response knowledge and plans.

As facility manager, you should be familiar with some of the methodology and terminology of the emergency management discipline. First responders and emergency management agencies developed these processes and terms to enable better coordination across agencies. They cover planning, responding and post-incident debriefing. Having a standard methodology and language makes coordination and communication between facilities and first responders easier, faster, and more precise.

Emergency Preparedness Concepts and Terms

One source of emergency preparedness and management terminology is the Incident Command System (ICS), now part of NIMS in the United States. The ICS is a standardized approach to incident management that:

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

Table 9 Emergency Preparedness/Management Terminology lists vital terms often used in discussions of emergency preparedness. Many of these terms reflect formal structures. However, they are meaningful at a facility or organizational level.

Term	Definition
After-action report	Generally stated as a "lessons learned", this document describes the incident response and findings related to system response performance.
Chain of command	The chain of command is a series of management positions in order of authority.
Check-in	Process whereby resources first report to an incident. Some include incident command posts, camps, or staging areas.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

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 evacuate, where building occupants can be counted, receive essential services, and await directions from first responders and emergency response teams.
Emergency operations center	Physical location where the coordination of information and resources to support incident management activities usually takes place. This location may be a temporary facility or may be in a more central or permanently established facility.
Functions	An incident command system (ICS) includes: • **Command** – Setting objectives for the response, creating strategies, defining priorities, and assuming overall responsibility for the incident. • **Operations** – Leading activities 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. **Intelligence**, a sixth function, may be established if required to meet management needs. Intelligence ensures that information is handled in a way that not only safeguards the data but also ensures that it gets to those who need access to it to perform their missions effectively and safely. The incident commander performs these management functions.
Incident Command System	The Incident Command System is used to: • Enable a coordinated response among jurisdictions and agencies. • Establish standard processes for planning and

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

managing resources.

- Allow for the integration of facilities, equipment, personnel, procedures, and communications operating within a typical organizational structure.

National, regional, and organization type variations of this system may exist, e.g., **Hospital Emergency Incident Command System** (HEICS)

Incident Command Post (ICP)

The incident command post is a field location where the primary tactical level, on-scene incident command functions are performed. The ICP will be located close enough to allow the incident commander to observe operations but far enough away to ensure their safety. It may be co-located with the incident base or other incident facilities.

There is only one incident command post per incident. It can be relocated if necessary.

Incident management team

An incident management team, also known as an emergency management or response team, should be interdisciplinary. At a minimum, it should include business unit representatives from internal operations/production, finance/administration, FM, HR, IT, security, and public relations/communications as assembled by a designated leader.
The incident management team leader can be any member of the organization. However, the leader must be:

- Familiar with the facility and its processes and needs.
- Able to think strategically to solve problems.
- Assigned sufficient authority to make necessary business decisions.

The team leader may want to assign specific portfolios to individual team members. For example, Public Relations and HR might handle communications planning, and Administration and Accounting might be responsible for ordering supplies and for maintenance. These team members could research and draft portions of the plan. They would then assume responsibility for implementing tasks in those areas during an emergency and for maintaining those sections of the plan over time. For example, HR could assume responsibility for compiling

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

	occupant lists and identifying occupants with disabilities who may require assistance.
Incident Commander	The incident commander is the person 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. The facility manager may very well be the incident commander if first on the scene of an emergency. The facility manager would relinquish incident command to the delegated emergency responder in control once that agency takes charge of the situation.
Lockdown	Situation in which occupants are directed to lock or barricade themselves into a secure area without glass doors or significant glass in the walls, turn off lights, and maintain silence until first responders provide further directions.
Memorandum of Understanding (MOU)	Document that describes broad concepts of mutual understanding of goals and plans shared by parties. An MOU may precede a more detailed Memorandum of Agreement (MOA) that explains in detail the specific responsibilities and actions to be taken by each of the parties to accomplish their goals.
Shelter in place	Situation in which occupants are directed to stay inside the facility due to unsafe conditions outside the building.
Span of control	The number of individuals reporting to a supervisor, usually expressed as a ratio of supervisors to individuals. NIMS recommends a span of control between 1:3 and 1:7.
Staging areas	Designated location for resources to be placed while awaiting a tactical assignment.
Unity of command	The 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.

Table 9 Emergency Preparedness/Management Terminology

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Additionally, **ISO 22300 Security and resilience – Vocabulary**, offers a global, consensus-based standard with terminology language for emergency management and business continuity.

Command and Coordination

One of the fundamental concepts of emergency management is the command structure. By defining and delegating authority for different decisions, effective emergency plans address the potential for chaos and disorganization during an emergency.

Coordination and control are essential to:

- Mount a unified response.
- Ensure that resources are quickly directed where they are needed.
- Ensure a smooth transfer of authority from first responders to the incident management team.

The purpose of a hierarchical chain-of-command is to remove confusion and conflict from the activities of order-issuing and order-taking. Each participant reports to and takes orders from only one supervisor. A transparent chain-of-command ensures that responders will not receive conflicting orders from two different supervisors. Having a seamless chain-of-command is especially important because, during an emergency, a responder may report to someone other than their usual supervisor. It also provides a more controlled communication channel so that commanders do not waste time interpreting 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. The system design should ensure that the right information is provided to the right person when it is needed, regardless of whether the request comes from inside or outside one's chain-of-command.

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

- The **Crisis Management Team** or senior management may be responsible for strategic decisions on issues that affect the entire organization.
- The **Incident/Emergency Management Team** will make the necessary tactical decisions on the operational aspects of how the strategy will be implemented at the facility level.
- The **Building Emergency Coordinators**, also known as support function leaders or floor wardens, may be responsible for the deployment of functional or local tactics.

Case Study

Meredith knew that to coordinate effectively she needed to gather all the information she could. She contacted the other employees to find out:

- if everyone was accounted for
- if everyone was safe
- if there were any immediate or special needs to address
- what message needed to be communicated to staff the following day

An oversight in the response plan was that "off hours" were not included and staff were unsure of what they should do.

Lesson Learned:
The organization's evacuation plan did not include an action plan for "off hours". Employees should be encouraged to create their own plans to protect their families when evacuations occur outside work hours. After the event was over, the organization facilitated a town hall event so the affected employees could share their experience including what to be prepared for and what to pack in your go bag.

Organizing Resources

The emergency management process includes organizing available resources to respond to an incident by defining certain spaces and assigning them specific functions. Resources include people and their expertise as well as materials and equipment.

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 should only be one incident command post per incident. However, that post may move if the original location is compromised or cannot accommodate the number of people likely to be involved. Some organizations also identify other command rooms/assembly stations in case the primary location is compromised and inaccessible.

The incident command post is equipped with the information that emergency leaders will need, including communication resources and useful documentation, such as building plans, manuals, catalogs and lists of occupants with disabilities. All information about the ongoing event should funnel to the command center. The centers should be large enough to accommodate the number of people likely to be involved in the response and immediate recovery. In global organizations, command centers can incorporate virtual meeting platforms and/or chat rooms to facilitate discussion. In fact, in global

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

organizations, the incident command post itself may be virtual, with communication and coordination handled through a web conference platform or on a web site.

A **staging area** is a designated 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. Systems should be in place to check resources in and out at the staging area. Large facilities may have multiple staging areas.

An **assembly area** is a designated location where occupants are instructed to gather 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 via walkie-talkie or cell phone. A runner can also be used to take information to the command center if no other communication tools are available. An orderly assembly area is essential for verifying that all occupants can be accounted for.

In most emergencies, the number of occupants in a single space should be limited, so there may be multiple assembly areas. An assembly area must also be secure – out of the way of rescue vehicles or, during a storm, in a safe 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.

Some circumstances make evacuation more dangerous. For example, if an armed individual is suspected to be inside the facility, a facility lockdown would be ordered. Occupants would be advised to find secure areas where they could hide until an all-clear is announced.

Case Study

Meredith notified leadership of the situation and the business continuity plan began.

The incident command center was set up and staffed. A designated individual sent out official communication to the entire organization.

The office was closed.

Emergency Preparedness/Response Training

The training required of emergency response team members will be specific to the type of business(es) that operate in the facility. For instance, if hazardous materials are used,

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

specialized hazmat training must be provided. For mining operations, customized training related to rescue and mine safety is required. On a cruise ship, the training relates to emergency evacuation and water rescue, as well as firefighting.

For general operations, the training will likely consist of the following:

- How to develop and implement response and emergency evacuation plans.
- How to operate fire extinguishers. In some situations, the use of fire extinguishers can worsen the hazard; therefore, staff not trained in their proper use should not operate them. Note: In the U.S., **OSHA 29 CFR 1910.157** states that education must be provided specific to any equipment that employees are expected to use as a part of an emergency action plan.
- How to perform cardiopulmonary resuscitation (CPR), how to operate an automated external defibrillator (AED), and first aid training.
- Proper handling of hazardous materials, basic fire training, and search and emergency rescue.
- The language used by public agencies and first responders during an emergency, especially members of the incident management team. In the U.S. it is NIMS (**NIMS course 100.c**).
- Any specific procedures required for the operation being performed in the facility by safety regulations, such as the occupational safety and health agency for the jurisdiction.

Incident management teams may seek training or advice from consultants who specialize in emergency response planning. First responder agencies will likely want to participate in the development and implementation of the training and can give a lot of experience-based advice. Additional training may be recommended, and plans can be checked or potentially supplemented.

Incident management teams may also want to reach out to **volunteer organizations active in disaster (VOAD)** or **community emergency response teams (CERT)** in their immediate area. A VOAD is an agency that works to assist communities impacted by disasters. A CERT is trained in responding to the hazards that may affect their geographic area, so they may appreciate an opportunity to cross-train with the organization.

Beyond the training required for incident management team members, call on the local first responders to provide training as well. First responders can provide training materials as well as guidance. The organization should also expect the incident management team to conduct regular training for all occupants of the facility so they are prepared should an emergency response be necessary.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Beyond those industry-specific requirements, incident management team members must:

- Be confident and able to act in an emergency as trained.
- Have the physical and mental capacity to learn and perform the duties for which they are volunteering.
- Be willing to commit the time required to develop, train, and implement the emergency response plans.
- Possess and demonstrate leadership skills such that occupants would have confidence in their abilities and follow their lead in an emergency.
- Be willing and able to hold confidential certain sensitive information that they learn in the conduct of their duties.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 2: Emergency Response Plans

Lesson 2: Objective

On completion of this lesson, you will be able to:

- Determine your current emergency response knowledge and plans.

Emergency Response Plans

Emergency response plans describe the initial actions that an organization will take when responding to an incident. As with strategic plans, the organization may require its component functions, especially support or critical functions, to prepare their own plans describing how they will respond to the more likely emergencies.

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

- Prepare for different types of incidents (e.g., what supplies, and equipment must be on-site).
- Train and educate FM staff and facility occupants about what to do when an incident occurs.
- Respond to different types of incidents.
- Assess an incident and decide on the next steps.
- Audit and maintain the plan throughout the plan's lifetime.

The plan itself must be clear and detailed, yet flexible and straightforward. Designated leaders should be able to assume their roles quickly. 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 and the authority to manage unforeseen situations. Speed of response is critical in an emergency. A response plan that is complex and requires following a rigid structure of approvals may hinder action and lead to subsequent damage.

Information that can be found in the plan might include:

- What constitutes an incident
- Whom to contact
- Criteria for escalating the response from a local level to a tactical level

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- 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)

The plan requires senior management commitment to a) the resources required to develop and implement the plan and b) the collaboration of cross-functional organizational team members. Because its preparation and execution will require budgetary approval, an effective emergency response plan must have management support. It will also require management endorsement of occupants participating in periodic testing of the plan. Senior management's support must be visible and constant.

Case Study

Power and natural gas were shut off and officials began evacuating people to shelters.

The organization had planned on using two nearby hotels as alternative space for its command center, work areas and possible housing but both these hotels were destroyed.

Generally, the organization's employees were able to continue working from home, but productivity decreased as some employees needed to move around, when additional areas had to be evacuated. Some employees were without power.

Lesson Learned. It is important to think through options of alternate spaces for many scenarios, including looking at locations in other counties or states.

Components of an Emergency Response Plan

Plans will vary according to a facility's needs. Common components and descriptions are listed in Table 10.

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 the locations of emergency areas, such as assembly areas and incident

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

command post.
- Leaders will apply consistent criteria in escalating the incident.

Scope	Descriptions and addresses of the buildings covered and perhaps not explicitly 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: • Occupant health and safety. • Infrastructure and facilities. • Operations and services. • Supporting local communities.
Emergency level designations	Criteria for assigning different emergency levels. The requirements might use various 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), so that they can be reached at any time, current contact information for all team members should be listed in an appendix. When critical personnel may be out of the country, contact information is especially important. Substitute personnel should also be included for key positions.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

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 to family members severe injury or death; protocol for communicating with media.
Drills and training	Training objectives applicable to building occupants – from leaders and staff to visitors – and for equipment and protocols; frequency and scope of the training and drills; and a process for after-action analysis and lessons learned.
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 an acquisition of a new building.
Version control and distribution control	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 that all facility staff and new hires know where shutoff valves are located and what actions to take in emergencies of different types.
- Protocols and support materials for specific emergency scenarios, such as fires or power outages.
- Contact information for insurers, suppliers, and contractors with whom arrangements are made to provide support supplies or services, such as security guards, structural engineers, communications specialists, utilities, refuse hauling, cleaning, portable sanitation facilities, etc. While this information may be kept on a smart device, organizations should plan for offline access as well. The information might be printed on wallet-sized cards for emergency team members so that the data is always available. They may also require that specific numbers be input into team members' mobile devices.
- Inventory lists of emergency supplies, including:
  - Supplies that should always be on hand and should always be functional, such as flashlights and batteries, tools, fuel, plastic sheeting, cameras to document damage, etc.
  - Supplies to support people, such as ready-to-eat food supplies, potable water, first aid equipment, and toiletries, etc. These supplies and facilities should be for both emergency responders and those sheltering-in-place before the emergency responders arrive. Supplies may also be needed for those in nearby buildings who might seek shelter in this facility.
  - The location of the supplies and equipment on the list.
- Schedule and plan to monitor, inspect, and replenish emergency supplies. Periodically check the supplies for expiration dates and replace expired supplies.
- Facility blueprints, critical equipment registers, and Business Continuity Management System (BCMS) files should be readily available. This information will be critical to first responders.
- Also include the audit strategy and schedule for auditing.

Table 10 Emergency Response Plan Components

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Planning in Leased Facilities

Not all facility managers operate owned facilities. But even in leased properties, emergency response planning is still an FM responsibility. For example, in a building with multiple tenants, the facility manager must identify who is responsible for emergency response. The designated person may be the landlord/property management company designee or an entity within the local municipality. If the landlord oversees emergency response, the facility manager should ensure that the building owner has a plan, and that the plan is adequate to fully protect occupants and key physical assets. Working jointly, the facility manager can develop the appropriate prevention and mitigation controls that can be synchronized with all parties, including the facilities' neighbors. The facility manager can then set up and train members of the facility emergency response teams, ensure that equipment for emergency responses is on hand (e.g., fire extinguishers, CPR equipment), and coordinate drills with the building owner.

If no responsible party has been identified, the facility manager can coordinate with other tenants and the building owners to ensure that an organized and effective emergency response plan is in place. This would include assigning responsibilities for writing the plan, defining command center responsibilities, organizing details, developing facility-specific responses for different scenarios, and managing the automatic notification of occupants.

Role of FM in Emergency Preparedness & Response

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

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

To ensure everyone understands their responsibilities should a risk event occur, and to ensure that gaps in the plan are identified, scenario testing and drills should be done regularly. This also promotes continuous improvement of the plan and builds resilience.

Either as a team leader or team member, the facility manager should support risk management and preparedness strategies. The facility manager's role is based on experience and specialized expertise. Other capable and trained specialists within the demand organization may also make up the team.

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

- Serve as a liaison with management to ensure management's understanding and support for emergency response planning.
- Ensure that first responders and agencies have timely access to 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 the FM emergency team members are trained in their duties.
- Establish a chain-of-command within the FM department 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 renewing and restocking supplies/inventories and updating prerecorded messages.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 3: Disaster Response and Recovery

Lesson 3: Objective

On completion of this lesson, you will be able to:

- Determine what improvements to emergency response are necessary to ensure employee and client safety.

When responding to a disaster, senior management acts to preserve the organization's value. They manage its impact, support recovery, and take advantage of opportunities, such as available aid or strategic improvements during recovery. Disaster response planning includes a communication strategy aimed at preserving the organization's reputation, prioritizing recovery goals and funding programs. Once immediate threats to humans and physical assets have been contained, the organization must immediately turn its attention to the future. This step leads to initiating the Business Continuity Plan (to be discussed in detail in Chapter 4).

The focus of disaster response is to get the organization operational while fully restoring services. Its goal is to stabilize the facility (e.g., repair critical damage to the facility structure and the building envelope), resume building systems (e.g., water, heat, power) so that the facility can begin to function, and mitigate against further loss. While full recovery may take place over an extended period, the organization will benefit if operations can continue while the recovery work is underway. This will require close coordination with departments such as HR and IT.

For any organization, recovery includes more than restoring physical operations. It is also ensuring the physical and mental well-being of occupants and the integrity of the organization's financial structure. This can only be accomplished by the response team calmly and expertly executing a well-developed plan.

Even as the official first responders arrive and begin working, the site must activate its response and recovery plan. This plan defines the structure of critical elements. It establishes who is in charge to make crucial decisions to protect people and business interests, secure the site, assure controlled communications, and take first steps toward recovery. Communication-planning is often ignored. Clearly defined protocols are necessary to advise employees, create media releases, contact the insurance company, ease concerns of customers and vendors, and protect the reputation of the business. In the timeline of activities, this should occur well before the team begins cleanup and restorative actions.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Here are five steps to keep recovery efforts on track:

1. Contact and coordinate with key stakeholders.
2. Evaluate the loss.
3. Connect with local agencies in your country.
4. Begin demolition and clean up.
5. Rebuild for the future.

While coordinating with key stakeholders, consistent communication is imperative during rebuilding. All communications should be managed through a designated spokesperson.

Remember that everyone will be dealing with the event personally as well as professionally. Exercise patience, in the early days after the event and beyond. Rebuilding takes time. Be prepared to communicate on the state of the facility and provide an estimate of how long the building will remain closed to the appropriate parties. Decide whether a temporary location is needed, and schedule temporary facilities or mobile offices as early as possible. These should already be identified in the recovery plan, with agreements ready to execute.

It may take weeks to evaluate the damage, especially if there is a shortage of available contractors, service providers, materials resources, and claims adjusters. Take the appropriate time to evaluate the loss. Many business owners want to jump right into rebuilding, but most insurance claims require a thorough evaluation of the loss. This information is most helpful for future planning. Which areas took on the most damage? Why? How could the damage have been prevented or mitigated?

Take the time to go through the facility and evaluate any systems failures or areas for improvement. While documenting the damage, include plenty of pictures. During this process, involve all key stakeholders in evaluating and documenting losses to ensure everyone's concerns and thoughts are considered. Loss goes beyond the physical damage to the facility. Are there damaged data banks containing sensitive business information? Were any research and development projects lost? Gathering feedback from all departments leads to better evaluation and future planning.

Check with your insurance company to find out what documentation is needed for your claim. Several inspectors and adjusters will likely be required to evaluate the facility. The damage will need to be observed and cataloged before gutting and demolition begins. Use this time to start brainstorming improvements to the facility and the emergency preparedness/business continuity plans.

Connect with local agencies in your country. Federal, state, province, county, and sometimes even local municipalities can aid businesses after a catastrophic event. Available

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

programs will vary locally and internationally, but you should familiarize yourself with the process of applying and the required documentation.

For federal resources, program information is available year-round online. Reviewing available programs should be part of any recovery planning process, and the time to start exploring applications is before an event happens.

Disaster response and recovery also includes demolition and cleanup. Once the new plans are in place, mandated permits are issued and the required inspections are done, it is time to start. After an area or regional catastrophic event, necessary labor and supplies, such as contractors, construction workers, outside trash/rubbish receptacles, portable toilets, and temporary site services will be in short supply. Secure these quickly and as soon as possible after the event.

Before demolition begins, schedule outside trash/rubbish receptacles, fencing, and other services. By the time crews are ready to work, these need to be in place. If the contractor is scheduling site services, ensure that they are delivered by the time demolition starts. After major catastrophic events, it is common to have to wait for local dumpsters for weeks or months. If necessary, outside trash/rubbish receptacles and other site services could be brought in from other regions, so be aware of the logistics of any city-wide demolition after a disaster. Experienced contractors and national waste service companies will have the experience and connections to find and deliver solutions. To avoid weeks or months of waiting for local services to be available, reach out as early as possible.

Rebuild for the future. When rebuilding the facility, incorporate the lessons learned from the after-actions report. Waiting to rebuild until after a debriefing may seem obvious, but sometimes business owners will want to restore what they had before as quickly as possible. Also, take the time to ensure any updates to your risk treatment strategies have been incorporated into the new, more current document.

Find out if building codes have changed because of the event. City inspectors will often notify facility managers and construction managers in advance, but it is the facility manager's responsibility to confirm what the codes are.

Disaster recovery events may happen only once or twice in a facility's lifetime. But when they do, it helps to be prepared beforehand to ensure that everyone can return to normalcy as soon as possible. One of the outcomes of disaster response and recovery is the activation of the organization's business continuity plan. Once immediate threats to life and property have been contained, the organization must immediately turn its attention to the future.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

The next chapter will reveal how your emergency response and disaster recovery plans will be incorporated into your facility's business continuity plan to finally establish the ultimate – Facility Resilience.

Case Study

Meredith returned to the office to find that the natural gas was still shut off so there was no hot water. Meredith and other local employees continued to work from home as the organization's plan dictated.

The office was closed for two weeks; employees were able to continue to work from home as indicated in the organization's business continuity plan. When they could return to the office, employees across the organization were notified by the designated person that the office was open.

With the organization's planning everyone could deal with the situation proactively and there was business continuity.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Chapter 3: Progress Check

1. Which functions are included in an incident command system?

   a. Command, logistics, and finance
   b. Operations, planning and logistics
   c. Logistics, finance, and administration
   d. All the responses are elements of an incident command system.

2. What decisions are the incident/emergency team likely to make?

   a. Strategic decisions that will affect the entire organization.
   b. Tactical decisions on operational strategies, such as how the strategies will be implemented.
   c. The commander will make all the decisions. The incident team only gives input.
   d. Strategic and tactical decisions.

3. What is a staging area?

   a. A designated area where building occupants are instructed to assemble.
   b. A designated area for people who do not know what to do and are waiting for instructions.
   c. A designated space where resources are waiting for deployment.
   d. A designated area where materials are put for use.

4. What are the most common training topics for emergency response training?

   a. CPR and First Aid.
   b. Hazardous material and evacuation procedures.
   c. Common language training and specific procedures.
   d. All the topics listed are common training topics for and emergency response team.

5. The emergency response plan (ERP) becomes a how-to guideline for the organization. Name two of the components within an ERP.

   a. Identify training needed and the certification dates.
   b. Prepare supplies and equipment that must be on-site and conduct training on how to respond to different types of incidents.
   c. Record the names of the people who approved the plan and share their contact information.
   d. Historical events examples and contact information of auditors and insurers.

6. Who is responsible for emergency response planning in a leased building?

   a. The landlord.
   b. The CEO of the building.
   c. The facility manager.
   d. HR.

7. An effective facility manager performs which of the following tasks?

   a. Ensure that first responders have timely access to current information about building and systems.
   b. Coordinate resources and supplies that are required by the Emergency Response Plan.
   c. Ensure that the emergency team members are trained in their duties.
   d. All the answers are correct.

8. When do you need to record the damage?

   a. During the emergency response.
   b. Before gutting and demolition begins.
   c. After starting the cleanup.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Chapter 4: Business Continuity and Facility Resilience

Lessons

- Objectives
- Lesson 1: Business Continuity
- Lesson 2: Business Continuity Concepts and Terms
- Lesson 3: Business Continuity Plan
- Lesson 4: Professional Practices for Business Continuity
- Lesson 5: Facility Resilience

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Objectives

Chapter 4: Objectives

On completion of this chapter, you will be able to:

- Guide Facility Management and other functions in developing and implementing a business continuity plan.
- Understand the requirements for an effective business continuity plan.
- Determine what improvements to emergency response are necessary to ensure employee and client safety.

This chapter is about how the FM function can be a valuable contributor and resource to the demand organization by providing expertise in the creation of business continuity plans. While many facilities are fortunate to avoid disruptive events, there has been an increase in catastrophic incidents, such as fires, hurricanes, floods and extreme snowfalls. There have also been lengthy utility outages, workplace violence, and terrorist threats. As stated before, few organizations were prepared for the total shutdown of cities, towns, states, and countries across the world and the closure of all, but essential businesses caused by the novel corona virus pandemic in 2020. These events have reinforced the advantages of having systems in play to quickly respond to disruptive events and reduce the time for business recovery.

As described by the **Disaster Recovery Institute (DRI)**, a business continuity management system (BCMS) integrates the disciplines of emergency response, crisis management, disaster recovery, technology continuity, and business continuity.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 1: Business Continuity

Lesson 1: Objective

On completion of this lesson, you will be able to

- Guide Facility Management and other functions in developing and implementing a business continuity plan.

Business Continuity is defined by the Business Continuity Institute (BCI) as the strategic and tactical capability to plan for and respond to business disruptions so the organization can continue business operations at an acceptable level. Business continuity programs are most successful when they are aligned with the organization's mission, values and strategic goals.

Business continuity consultant Robert Hall listed the priorities for any organization responding to a crisis as:

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

ISO 22301 Societal Security – Business continuity management systems – Requirements (ISO 22301) states that a business continuity management system (BCMS) emphasizes the importance of:

- Understanding the organization's needs and the necessity for establishing business continuity policies and objectives.
- Operating and maintaining processes, capabilities, and response structures to ensure the organization will survive disruptions.
- Monitoring and reviewing the performance and effectiveness of the BCMS for continual improvement based on qualitative and quantitative measures.

A business continuity plan helps ensure that critical processes either continue to function 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. For some organizations, such as defense-related industries, it is mandated by regulatory or legal requirements.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

As with the emergency response process, business continuity must be aligned with the demand organization's strategy. Continuity efforts focus on functions and systems that are essential to the organization's mission, strategy and core business activities. For example, if FM oversees a cold storage facility, there must be a way to record actual temperature settings and maintain those settings at an acceptable level. Otherwise, the contents (e.g., perishable food, plant life, laboratory research samples, bio-pharmaceutical products, etc.) may be damaged and need to be discarded. The facility manager must identify all supporting systems and processes and the impact to the core business activities if interrupted by incidents.

Because senior management approves the budget for contingency efforts, the business continuity planning process must have their commitment and support. Senior management will also have a say in how services and functions will be prioritized. They will approve the funds necessary to acquire and maintain the human and physical resources needed to provide those services.

The relative importance of these priorities may vary depending on the organization's culture, values and strategy. Before developing a business continuity program, those involved – including facility managers – should 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.
- Are emergency preparedness and business continuity priorities aligned with the organization's strategic priorities? This will affect management's allocation of resources to mitigation efforts and business continuity. For example, a strategy dependent on continuous production to achieve market dominance will require a greater focus on protecting production assets and a speedy recovery from events.
- How committed is senior management to the concepts of risk management? For risk management strategies to succeed, including emergency preparedness and business continuity programs, management must be fully engaged. Facility managers may have to make a business case for these programs and form alliances with other functional leaders to champion them.
- How familiar are occupants and other functioning departments with the principles and benefits of emergency preparedness and business continuity? Their participation in developing, testing, and implementing plans is critical.
- How do the priorities of the demand organization's management align with FM's priorities during an emergency? Will the facility manager meet resistance from other senior management on plans related to activities, such as evacuation drills? Is management placing enough emphasis on continuing essential business processes? If FM believes the organization's priorities are not right, the facility manager may have an ethical responsibility to educate senior management about the possible negative outcomes.

- Does the demand organization have a realistic level of risk tolerance? Is the amount of uncertainty that senior leaders accept based on reality or is it too optimistic? The facility manager may need to educate management about costs that can be avoided through mitigation. They must also understand the financial risk of doing nothing.
- How will the demand organization's decision-making structure affect emergency preparedness programs? What decisions is management comfortable delegating to temporary emergency managers, who will perhaps reside within the FM department?
- Will the culture of the demand organization support the level of collaboration and trust required to develop and implement plans? Steps may have to be taken to demonstrate an understanding of the needs and perspectives of other functions and to cultivate alliances.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 2: Business Continuity Concepts and Terms

Lesson 2: Objective

On completion of this lesson, you will be able to:

- Guide Facility Management and other functions in developing and implementing a business continuity plan.

With management's support, business continuity planning can become part of the organization's culture as reflected in:

- Formal statements of the organization's 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 must be performed in a uniform manner.
- The roles and responsibilities described in the SOPs become part of performance expectations for the organization's employees 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 (e.g., FM, finances, legal, IT and HR, etc.) should be involved in the planning process as well.

Following are some key concepts and terms used regarding the contingency planning process:

- **Minimal level of performance analysis.** When analyzing the business impact of an event, the demand organization agrees to the minimal acceptable level of performance for each business function and how long that function can be suspended without irreparable harm to the organization. A recovery time objective is defined. Contingency planning will help the organization accomplish that objective. The facility manager will be directly and indirectly involved in planning and implementing contingencies. For instance, identifying potential temporary facilities and interviewing landlords, contracting with suppliers for services and equipment, and arranging for storage and transportation of redundant equipment and supplies are responsibilities that may fall on the facility manager.
- **Continuity requirements analysis.** The next task is to understand what those essential functions require 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 a temporary or backup office to record transactions, but if the volume of transactions is low, the process could probably be performed manually. Primary requirements should 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 their equipment and materials. The workspace 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 and maintenance contracts, such as delivery of fuel for backup generators.
- Power and voice/data communication.
- Mailing/shipping services to and from the temporary location, including forwarded mail from the primary facility.
- FM services to maintain the temporary location.

- **Contingency strategies.** This step includes arranging for contingent workplaces (also known as alternate sites or business continuity backup sites), employees, equipment, supplies and services. The choice of an alternative workspace will depend on a function's minimal level of performance requirements that define how essential a function or task is to the demand organization, how quickly the function must resume, and how difficult it may be to find a substitute space.

  For example, a bank must continue monetary transactions and could suffer non-compliance fines and possibly face losses of future business if it cannot continue completing, monitoring, and reporting transactions. The bank 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 cost of not being able to continue functions.

Alternatively, an organization may choose a cold site for an activity that is essential but can withstand a delay in coming online. 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, or swing space that can be easily reconfigured.

Other alternatives are possible as well, depending on the nature and needs of the function that must be continued. Some affected employees can work remotely. These employees 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. These were especially critical during the 2020 novel corona virus pandemic when virtual meetings became a necessity as businesses worldwide shut down. The support of Internet-based meeting platforms became a daily reality.

Repurpose areas in the facility – or other buildings in a multi-building facility or other facilities in a global organization – so that they can be used for a 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 website, www.iaem.org.

- **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 workers 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 with 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 (to establish redundancy) for later use, or similar equipment can be assigned 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 communications. Having the agreements fully executed before the emergency ensures that the service 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 the suppliers and contractors have the means to carry out the essential processes within the required parameters with both the necessary equipment and trained staff. They should review the supplier's or contractor's own business continuity plans.
- **Data and document continuity.** Business continuity planning, in coordination with IT processes, can minimize the loss of data due to an incident. Disaster recovery plans, developed by IT, include specific requirements and mitigation strategies to ensure the protection of and access to data. This includes online (both Internet and intranet) database systems and applications, such as payroll and purchasing.
- **Offsite, continuous backup of essential data and storage.**

  Protection of and access to archived data is part of an organization's mitigation program. The U.S.-based FEMA offers a broad set of guidelines for such a program that include recommendations for an annual review and testing of the vital records program in which:

  - Records about emergency response and business continuity are identified and protected.
  - Records necessary to continue operations and to remain in compliance with laws and regulations are identified and protected.
  - The process of protecting vital records is formalized with a designated responsible leader and approved policies and procedures.
  - The organization has access to online and/or hard copies of documents and to email within 12 hours.
  - Redundant media are used to backup vital records.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- The inventory of vital records is kept current.
- A risk analysis is performed of records and databases.
- The vital records packet is developed and maintained. This packet includes the location and access rights to stored documents, a records inventory, the equipment needed to access records, and names of record-recovery experts.

At the facility level, the FM Team can work with IT to identify the most efficient ways to backup facility system data. For example, there are services that use the Internet to store data and applications "in the cloud" – that is, on servers that may be located anywhere in the world. They 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 FM operations should be backed up and on what schedule. Managers should work with staff to identify what stored data are accessed on a regular basis and must be available after an emergency – for example, baseline performance data or maintenance and repair histories. The FM 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 carefully consider 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 past payments
- Warranties and service contracts
- Service histories that could be used to support valuation of facility equipment
- Employee files when separate files from HR are maintained
- Access card data, which will be critical in determining who was and who was not in the building at the time of the event and whether occupants have been lost
- Essential correspondence
- Records of important meetings
- Any equipment information that could not be retrieved from the Internet cloud-based system
- Copies of the master inventory index

Facility managers can check with the legal department regarding local requirements for original document retention. Some documents may 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, FM, and senior management.
  - How the decision will be communicated to leaders and affected employees.
  - How the functions will be returned, for example, all at once or in stages.
  - What preparations must be made to return equipment, supplies and documents.
  - What services must be terminated.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 3: Business Continuity Plan

Lesson 3: Objective

On completion of this lesson, you will be able to:

- Guide Facility Management and other functions in developing and implementing a business continuity plan.

Business Continuity Plan

A great deal of the input for the Business Continuity Plan (BCP) is the information contained in the business risk analysis discussed earlier. This information helps establish priorities and objectives for recovery of essential functions. The goal of risk identification, risk analysis, and determining treatment strategies is to develop the BCP. There may be multiple sub-plans, one for each essential function that must be continued or resumed quickly. Depending on the severity of the incident and damage sustained, these plans may be activated in stages.

Most plans include descriptions of:

- The conditions that will trigger the activation of the plan, such as loss of access to the facility or loss of power for more than three days.
- The priorities that dictate which functions will be resumed and the order of resumption.
- The functions that are to be suspended or performed only if no continuance resources are needed, such as vendor delivery of supplies, training activities not related to the emergency, or activities in a building not affected by the incident.
- What is required to resume the function, in terms of workers, facilities, equipment and supplies.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- Contingency operation plans that further describe:
  - **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 who is responsible for implementing the transfer of the essential function to its temporary location and for making decisions during the transition and relocation. Plans should specify leadership alternates if necessary.
  - **Communication plans.** How the activation decision will be communicated and how communication will be maintained during the relocation.
- The processes for moving back to the facility when the disruption is over.
- How to maintain the continuity of data operations and organizational documentation.
- What training is required of staff and first responders prior to an incident.
- The continuity plan evaluation and audits.

Implementing the Business Continuity Plan

Once the emergency preparedness and business continuity plans have been drafted, they should be presented to management for review and approval. When they have been approved by management, the team and other business functions, including FM, the process of integrating the plans into the organization's policies and procedures and, ultimately, into their culture can begin. 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 (for example: managers' home, insurers' offices, with local emergency responders) in case the facility is inaccessible.

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.

Business functions should also prepare to perform their own responsibilities. For example, HR can compile lists of occupants assigned to specific staging areas that are updated automatically. Home contact information is entered into the emergency messaging system. The legal department or corporate attorney reviews contracts to ensure there are provisions in case of an event for continued on-time delivery of specific services or supplies. The FM team and IT collaborate on how to improve data center resiliency, such as by adding redundant systems.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Once functional plans are completed and approved, the FM and functional leads may begin to implement some of the provisions. These provisions may include working with realtors to identify contingency locations, securing redundant equipment, and storing essential documents to the cloud or off-site.

General features of the plan should be introduced to occupants through the variety of communication vehicles available, including organization-wide and departmental meetings, intranet, newsletters, e-mails, websites and facility social media feeds.

Drive-away kits

The people responsible for continuing essential functions will require the equipment, tools, information and supplies they will need if the facility is unavailable. These are commonly called **drive-away kits**. The kits may include:

- A hard copy of:
  - The business continuity plan or a condensed version containing only that information the employee will need, such as a description of transportation options to reach the business continuity site should mass transit and highways be unavailable or unsafe.
  - The emergency response and business continuity team contacts.
  - Succession documents or delegations of authority.
  - Phone lists of employees and vendors.
  - Critical internal/external contacts (e.g., finance, realtors, suppliers).
- Computer and communication equipment already loaded with the 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, whiteboards.
- Emergency response supplies, such as a hard hat, two-way radio, flashlight/torch, and high-visibility clothing.
- Personal supplies, such as toiletries, and a small amount of cash or a credit card.

Organizations may also implement requirements that employees are "emergency-ready" at all times. This may mean, 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 have emergency plans for their families. Those plans might include how to communicate with each other if members are away from home, and a checklist of supplies for surviving at home for three days after a

disaster strikes (food and water, wind-up or battery-powered radios, batteries, flashlights, pet food, and the like).

It will be important to be able to substantiate your processes. Consider referencing ISO 22301, an ISO management system standard that specifies requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. The standard is intended to be applicable to all organizations, or parts thereof, regardless of type, size, and nature of the organization.

Business continuity is about maintaining or restoring critical functions during an event and until recovery is complete. If a well-designed BCP is expertly executed, the demand organization will sustain only the expected loss and will resume functionality in the planned time-frame.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 4: Professional Practices for Business Continuity

Lesson 4: Objective

On completion of this lesson, you will be able to:

- Understand the requirements for an effective business continuity plan.

Practices for Business Continuity

According to global insurance statistics, 40 percent of businesses that experience a catastrophic event do not re-open. Of those that do re-open:

- Within one year, 25 percent fail (FEMA).
- If the operations of the business are impacted for five days or more, up to 90 percent fail within one year (U.S. Small Business Association).
- Within two years, over 75 percent are out of business.

You may not be able to prepare a contingency for every scenario. You should, however, have documented plans in place to deal with circumstances that are most likely to happen and are within your sphere of control or perhaps not far removed from it. This may give you an opportunity to collaborate with other business units. Together, you can take a serious and in-depth look at what is required. For example, you can develop continuity plans based on what was learned during the risk analysis. There is valuable experience in developing plans for risks that are less severe but are more likely to occur before taking on a large-scale event with far-reaching consequences. In the process, the FM staff will become skilled at planning and gain valuable experience should a risk become an event.

The facility manager needs to be acutely aware of how the FM operations can participate and contribute to helping the demand organization be proactive in creating its continuity plans. This is a key area where the FM team can add real value to the organization.

Best practice includes:

- Identifying and documenting the systems critical to sustaining operations during and after a disaster.
- Developing responses that ensure reliable and consistent performance of the facility.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

- Periodically initiating reviews of potential risks with stakeholders and establishing programs designed to sustain operations or reduce the time to recovery.
- Communicating the plan within the FM organization, testing the components of the plan, and adjusting it accordingly.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Lesson 5: Facility Resilience

Lesson 5: Objective

On completion of this lesson, you will be able to:

- Determine what improvements to emergency response are necessary to ensure employee and client safety.

Resilience is not a plan or an operating procedure, but an organizational strategy. Business continuity relies on:

- Understanding which of the essential functions need to continue or resume operations within a stated time frame.
- The ability to immediately implement the necessary steps required to meet that goal. Resilience is the result of a well-developed Risk Management Program that includes Emergency Preparedness and Disaster Response and Recovery plans that are incorporated into the Business Continuity Program.

When an emergency or disaster occurs, an organization must act promptly to fulfill its obligations to multiple stakeholders. While the scope, severity and timing of an incident affect an organization, its impact also affects the time for recovery. Recovery depends on an organization's state of preparedness for incidents. Emergency preparedness and business continuity programs are the outputs of a risk management mitigation strategy. They are also key to building facility resilience. Developing and implementing these programs require organizations to invest time and money and to occasionally sacrifice convenience. This investment is insurance against possible threats that could jeopardize the organization's mission, assets and people. Facility managers must be able to define the specific costs of emergency response and business continuity activities and justify them to management using both economic and noneconomic benefits.

Emergency preparedness coupled with business continuity plans positively affect the organization's level of resiliency by:

- Protecting organizational capital assets.
- Protecting the organization's inventory.
- Protecting the organization's employees, service providers and visitors.
- Being able to continue mission-essential processes.
- Improving compliance with laws and regulations.
- Lowering insurance rates.

- Increasing stakeholder satisfaction.
- Improving communication and fostering teamwork.
- Increasing efficiency.
- Fostering a proactive (rather than reactive) culture.
- Decreasing the organization's vulnerability to litigation.

Careful attention to planning for business resilience can mitigate the impacts of a disruption and allow your business to continue to function or recover more quickly. A business continuity management system (BCMS), such as ISO 22301, can help the organization build its business continuity program in clear and tangible ways. The BCMS is the framework for business resilience. It consists of the strategy, procedures, solutions and education. This framework can build a strong, effective business resilience strategy that will allow the organization to be prepared to avoid, mitigate, and recover from adverse events.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Chapter 4: Progress Check

1. What is the purpose of a business continuity plan?
    a. The purpose of the business continuity plan is to understand the organizations needs
    b. The purpose of the business continuity plan is to ensure critical processes continue or resume quickly after an emergency
    c. The purpose of the business continuity plan is to safeguard people and their families
    d. The purpose of the business continuity plan is to put monitoring plans in place

2. What function(s) does a business continuity plan focus on?
    a. Operations and Finance
    b. HR and Finance
    c. Essential functions to the organizations mission and/or strategy
    d. FM and Risk

3. What arrangements can be made for contingency strategies?
    a. Arrangements can be made for workspaces
    b. Arrangements can be made for employees
    c. Arrangements can be made for workspaces, employees, equipment, supplies and services
    d. Arrangements can be made for equipment, suppliers, and services

4. What is a drive-away kit? (Choose the best response)
    a. A kit that sits in a vehicle until it is needed for use and has work supplies
    b. A kit that has equipment, supplies and information necessary for the performance of an essential work function
    c. A kit that has temporary work supplies
    d. A kit that has a hard hat, two-way radio, a flashlight, and a glow in the dark safety vest.

5. According to the global insurance statistics, what % of businesses do not reopen after a catastrophic event?

   a. 50%
   b. 30%
   c. 40%
   d. 75%

6. What is facility resilience?

   a. Facility resilience is an operational plan to continue essential functions
   b. Facility resilience is a plan to address how a business can keep operating after a hazardous event
   c. Facility resilience is an operating procedure
   d. Facility resilience is an organizational strategy that allows business to mitigate the impacts of a disruption, and allows business to continue to function or recover more quickly

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

Progress Check Question Answer Key

Chapter 1: Risk and Risk Management

Objectives

1. c
2. b
3. a
4. b
5. d
6. b
7. b
8. a
9. a
10. d

Chapter 2: Risk Management Planning

Objectives

1. a
2. a
3. b
4. c
5. b

Chapter 3: Emergency Preparedness and Disaster Response and Recovery

Objectives

1. d
2. b
3. c

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

4. d
5. b
6. c
7. d
8. b

Chapter 4: Business Continuity and Facility Resilience

Objectives

1. b
2. c
3. c
4. b
5. c
6. d

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper

References

In alphabetical order:

Contributor, When Training Kicked in, Meredith's story, Fire in northern California, U.S. 2017

Council Regulation (EC) No 2062/94, of 18 July 1994 *Establishing a European Agency for Safety and Health at Work*, OJ L 216, 20.8.1994, p. 1.

Florin, M. Bürkler, M. I*ntroduction to the IRGC Risk Governance Framework*, Geneva. 2017.

In the U.S., OSHA 29 CFR 1910.157 NIMS (NIMS course 100.c). As described by the Disaster Recovery Institute (DRI), (U.S. Small Business Association).

Parasuraman, K. *The Rise of Interconnected Risk*, 2019. URL:https://www.air-worldwide.com/blog/posts/2019/5/the-rise-of-interconnected-risk/. [Last Accessed: 2020]

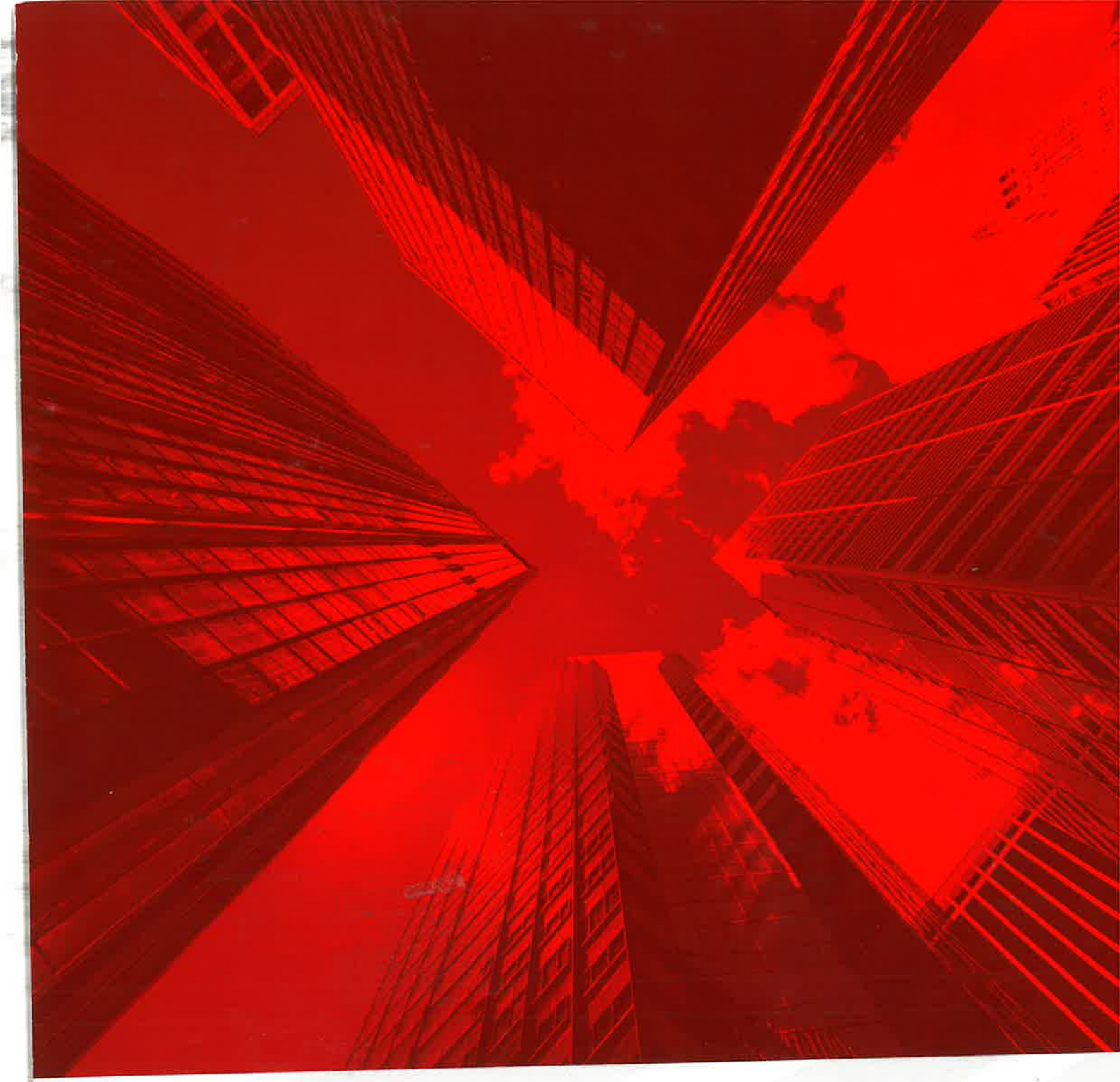
Public Law 91-596 84 STAT. 1590 91st Congress, S.2193 December 29, 1970, as amended through January 1, 2004.

ISO 22300 Security and resilience – Vocabulary, 2018-02.

ISO 22301 Societal Security – Business continuity management systems, 2012-05.

ISO 31000 – Risk management – Guidelines. (ISO/Guide 73:2009 Risk management – Vocabulary) 2009-11.

Edition 2022, Version V2017PARM_1.0
Printed on 100% post-consumer waste recycled paper



www.ifma.org
T: +1-713-623-4362 | F: +1-713-623-6124
800 Gessner, Suite 900 | Houston, Texas 77024 USA

IFMA