DISASTER RECOVERY PLANNING

Table of Contents

Page

List of Figures

List of Tables

1.0 SCOPE

This data sheet provides guidance for the development of disaster recovery plans to ensure that viable recovery strategies are in place when disaster strikes. The intent of a disaster recovery program is to document the process for restoring critical business functions to a state of normal operations following a crisis or a declared disaster.

1.1 Hazard

The main goal of the disaster recovery plan is to establish guidelines to resume or recover specific essential operations, functions or processes. In addition, the plan assists corporate management to focus on their established, yet separate, business continuity plans for the uninterrupted provision of the company's overall strategically important business operations and services.

The focus of an effective disaster recovery plan will be on expediting the following actions:

- Assessing the damage incurred to the facility
- Implementing damage control activities
- Recovering business operations

These actions address the general requirements of a disaster recovery plan in response to an identified risk at any facility. The disaster recovery plan is an extension of the emergency response plan.

Without a documented and well-practiced disaster recovery plan to follow in the aftermath of emergency situations such as natural disasters, fire/explosions, terrorism/sabotage, mechanical breakdown and service interruption, a company's ability to recover from an emergency would be significantly reduced.

A disaster recovery plan cannot be considered reliable until it is exercised and has been proven workable, especially since false confidence may be placed in its integrity. Exercising the plan has a number of benefits:

- It verifies the plan is practical by modeling recovery from disaster conditions.
- It provides training for the staff through operation of the plan.
- It provides a feedback process to ensure procedures are appropriate.
- It improves confidence for those taking part.

Do not underestimate the work required for testing, exercising and maintaining the plan. This process can be labor intensive and affects a large variety of different people within the organization and its facilities. In many cases, full testing is not practical due to the need to maintain normal business operations.

For more information, refer to Understanding the Hazard publications *Lack of Equipment Contingency Planning* (P0179), *Lack of Emergency Response* (P0034), and *Lack of Pre-Incident Planning* (P0033).

1.2 Changes

April 2025. This document has been reorganized to provide a consistent format. Minor editorial changes were also made.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

2.1.1 Identify essential operations, functions or processes that would need to resume or recover quickly after a disaster.

2.1.2 Establish guidelines to resume or recover each activity identified in 2.1.1.

2.2 Human Factor

2.2.1 General

2.2.1.1 Identify and document a Crisis/Incident Management Team (CMT/IMT) for the facility.

2.2.1.2 Identify and document a Disaster Recovery Team (DRT) for the facility.

2.2.1.3 Develop detailed emergency response procedures to include:

A. A nearby Emergency Operations Center location, suitably stocked with communications equipment and recovery materials

B. Actions required to restore normal operations to pre-incident levels within the shortest time possible

C. Actions to maintain principles of security (personnel, physical and information) and

D. Actions for salvage, loss containment, and restoration.

2.2.1.4 Test, exercise, and maintain the plan.

2.2.2 Crisis/Incident Management Team (CMT/IMT)

2.2.2.1 Establish a Crisis/Incident Management Team that is responsible for managing the incident, including the following:

A. Deciding whether a disaster should be declared

B. Adapting the plan to account for prevailing circumstances

C. Prioritizing the recovery of business functions to minimize the impact

D. Initiating, controlling and coordinating the local recovery operations

E. Reviewing critical milestones during the recovery process

2.2.3 Disaster Recovery Team (DRT)

2.2.3.1 Establish a Disaster Recovery Team (DRT)responsible for implementing the plan at the site level.

2.2.3.2 Determine what DRT positions and responsibilities are needed based on the facility. Typical DRT positions and responsibilities are described in Table 2.2.3.2.

Table 2.2.3.2. Disaster Recovery Team (DRT) Positions and Responsibilities

Positions	*Responsibilities*
Plan Coordinator	• Take charge of the incident. • Coordinate activity with emergency services. • Support the CMT in the management of the incident. • Report the following items to the CMT, who is primarily responsible for the Organization's Business Continuity Plan: incident details, non-operating processes/ equipment, safety concerns, and emergency efforts taken since the onset of the disruption.
Fire Protection System Coordinator	• Ensure the fire protection sprinkler systems (control valves, pumps, etc.) are fully functional and in good working order. • Verify that control valves remain open until authorized to be closed by a responsible incident officer. • Verify that all suppression systems are functional and have not been compromised. • Report any system malfunctions to the plan coordinator.
Hazardous Material Coordinator	• Ensure all hazardous materials and ignitable liquids are safely secured and do not pose any threats to facility. • Ensure all safety combustion guards on critical operations are functional and have operated as designed. • Report any safety malfunctions of operation processes to the plan coordinator immediately.
Facilities Coordinator	• Retrieve building as-built plans and documentation to assist emergency personnel with disaster mitigation. • Coordinate pre-planned hot, warm or cold disaster recovery sites to maintain operation of facility as needed.
Media, Marketing, and Public Relations Coordinator	• Collect damage information and details of the incident. • Report all incident information to the plan coordinator. • Direct all inquiries related to the incident to the organization's media spokesperson.

2.2.4 Risk/Incident Identification

2.2.4.1 Identify risks to which the facility is most susceptible. See Table 2.2.4.1 for a list of possible incidents and mitigation actions.

Table 2.2.4.1. Possible Incidents and Mitigation Actions

Incidents	*Mitigation Actions*
Fire and explosion risks (including arson)	• Employee evacuation plan is in place. • Emergency Response Team is active and on call. • Communication equipment, such as radios, alarm transmission equipment, and cell phones, are fully functional. • Sprinkler system protection is not impaired. • Fire walls are not compromised.
Natural hazards, such as flood, windstorm, earthquakes and roof collapse	• A flood emergency response plan (FERP) and basic emergency response plans have been established. • Flood protection barriers are available. • Building construction reinforcement material for roofs and windows is available.
Service interruption, such as gas or electric power outages	• Backup power sources, such as batteries, UPS systems and generators are functional.
Hazardous material incidents	• First aid stations are fully stocked. • Decontamination equipment is functional and available. • Ventilation systems are functional and ready to shut down as directed by emergency personnel.
Vandalism, burglary and terrorist attack	• First aid stations are stocked. • Security system logs are secured. • Fire and burglary alarm systems remain operable.

2.2.4.2 Verify that the actions to mitigate the losses associated with each risk identified in Section 2.2.4.1 have been reviewed and can be implemented.

2.2.5 Plan Development

2.2.5.1 Identify alternate processes both upstream and downstream that could be implemented if critical functions or equipment are compromised or fail.

2.2.5.2 Maintain critical spares for important machines.

2.2.5.3 Review internal emergency response plans and policies as they pertain to the following:

A. Evacuation plan

B. Fire protection plan

C. Safety and health program

D. Security procedures

E. Employee manuals

F. Hazardous materials plan

G. Process safety assessment

H. Plant closing policy

2.2.5.4 Collaborate with outside groups to discuss and plan for potential emergencies and available resources. Consider the fire service, police department, electric utilities, public works, national weather service and telephone companies.

2.2.5.5 Provide internal and external resources needed for emergency recovery, such as personnel, equipment, facilities and funding. See Table 2.2.5.5 for example resources.

Table 2.2.5.5. Examples of Internal and External Resources

Type of Resource	*Sources*
Personnel	• Hazardous materials response team • Fire emergency response team • Security • Public information officer
Equipment	• Automatic sprinkler system • Suppression system • Communication equipment • First aid supplies • Emergency power equipment • Decontamination equipment
Facilities	• Emergency operating center • Shelter area • First aid stations • Media briefing areas
Funding	• Cost and liability connected with using the involved resources

2.2.5.6 Identify the physical protection in place for key processes (e.g., automatic sprinkler protection, gaseous protection, interlock systems, etc.)

2.2.5.7 Identify where specialist help and other alternatives can be considered to get the operation running, such as hot, warm or cold disaster sites, share-loading, new facilities, warehouses, equipment, people, etc.

2.2.6 Test, Exercise and Maintain the Program

2.2.6.1 Establish a test, exercise and maintenance routine for the disaster recovery plan.

2.2.6.2 Establish regularly scheduled meetings for the DRT members.

2.2.6.3 Assess training needs for the recovery plan. If warranted, develop a training curriculum at all levels within the organization to support the program.

2.2.6.4 Prepare representative and suitably detailed disaster scenarios. Include specifics in the exercise such as dates, time, workload, political and economic conditions, accounting period end and concurrent activities.

2.2.6.5 Perform the disaster exercise or scenario with both planned and unplanned, drills. Consider varying the scenarios from that published, for example, by substituting key players.

2.2.6.6 Document and evaluate exercise results, adjusting the plan where necessary.

2.2.6.7 Establish a process whereby the CMT is informed of changes in people, manufacturing process and equipment.

3.0 SUPPORT FOR RECOMMENDATIONS

3.1 Plan Development

Comprehensive disaster recovery and business continuity plans for an entire organization are developed primarily at a corporate management level, with contribution from key location management as appropriate. Corporate disaster recovery and business continuity plans (DRP and BCP) take into consideration operations for all facilities and potential make-up capabilities between plants, other manufacturers, or suppliers since the plans relate to the strategic objectives of the organization. Depending on the size of the organization, it can be difficult for every facility to know the specifics regarding the disaster recovery plans for that facility. If a disaster recovery plan has not been developed, the guidelines provided within this document can be followed to help develop a comprehensive plan.

Distinguishing between an emergency response plan, a disaster recovery plan, and a business continuity plan is important. Emergency response is normally the initial part of the disaster recovery plan (how the local personnel respond to an event in the minutes to hours following an incident). A disaster recovery program is an ongoing process for short-term disaster mitigation that is more than a ′reaction’ to an incident. A business continuity plan is a comprehensive program to respond to an enterprise-level risk and address business disruption to normal operations in the weeks to months that follow an incident. See Figure 3.1 below to identify the critical timeline for an incident management plan in general and a disaster recovery plan specifically.

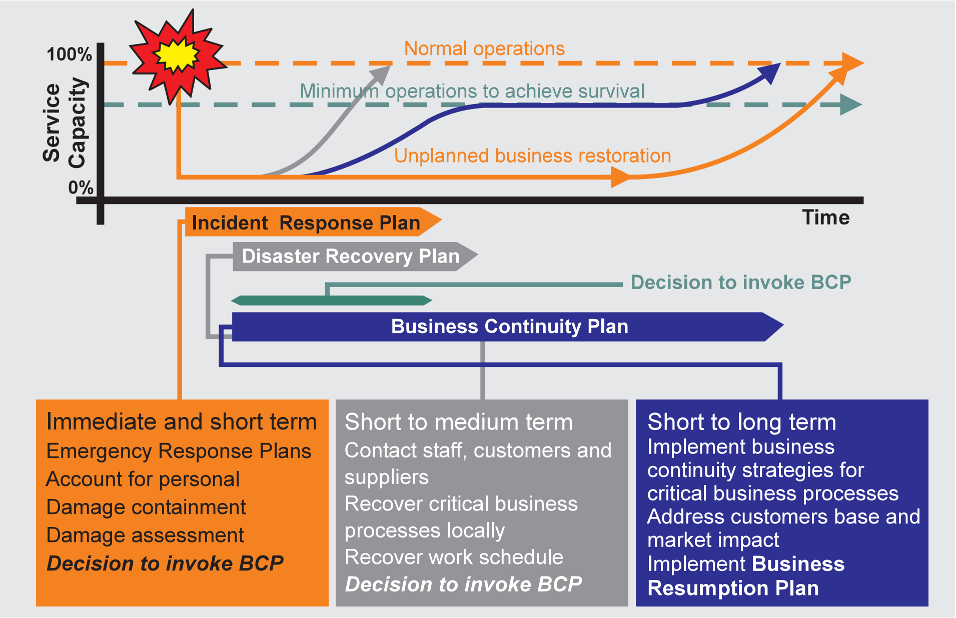

Fig. 1. Phases of Response

Although plans should be tailored to the particular facility, and no two plans are the same, a number of key components should be incorporated into all plans. Among the more important include:

- A crisis or incident management team (CMT or IMT) responsible for providing the strategic decision-making direction and appropriate notification to internal management, and for expediting recovery of operations to pre-incident conditions.
- A site disaster recovery team responsible for providing early assessments on the incident and advising the CMT/IMT on necessary damage control actions, expediting recovery and liaising with emergency authorities.
- A media spokesperson who, along with the CMT/IMT, will ensure a positive commentary is delivered to the public, company staff, customers and other interested parties.
- An initial response plan that will ensure appropriate notification and action by first responders. The plan will need to include contact details in a “Call-Out Tree” for key staff.

3.2 Loss History

In the aftermath of an emergency—whether a natural disaster or an unforeseen crisis—physical destruction or damage to structures, production lines and inventory are the obvious perils. Less easy to identify is the negative impact on employee productivity, customer retention, and the confidence of vendors, partners and customers. Every year, FM clients have millions of dollars in business interruption losses. While many of these losses are mitigated due to contingency planning, many others are more severe than necessary, because the client did not have a contingency plan. Proper disaster planning makes a big difference.

4.0 REFERENCES

4.1 FM

Data Sheet 10-1, *Pre-Incident and Emergency ResponsePlanning*

Understanding the Hazard, *Lack of Equipment Contingency Planning* (P0179)
Understanding the Hazard, *Lack of Emergency Response* (P0034)
Understanding the Hazard, *Lack of Pre-Incident Planning* (P0033)

APPENDIX A GLOSSARY OF TERMS

Cold disaster recovery site: An infrastructure only backup facility where all the equipment needed to continue operations will need to be provided and installed. A cold site is less expensive than a hot or a warm site, but it takes longer to get an enterprise in full operation after a disaster.

Emergency and government authorities: A global term that represents public firefighters, water, police, hospital personnel and local government officials in any area of the world.

Hot disaster recovery site: A redundant facility that allows a business or a location to continue its operations in the event of a disaster. For example, if an enterprise’s data processing center becomes inoperable, that enterprise can move all data processing operations to a hot site. A hot site has all the equipment and operations needed for the enterprise to continue its operation, including equipment, machinery, storage space, office space and furniture, telephone jacks and computer equipment.

Human factor: Action or inaction that directly affects the probability for a property loss incident to occur and/or that affects the level of severity that an incident reaches. It can be a positive or negative factor. The human factor hazard is directly proportional to the physical hazards and processes present within a facility and inversely proportional to the level of preplanning, education and training provided for individuals in advance of the incident.

Mitigation: Actions taken or provisions made to eliminate or reduce the likelihood or consequences of an event, either prior to or following a disaster/emergency.

Recovery: Activities and programs designed to return operations at a site to pre-incident levels as quickly as possible.

Response: In disaster/emergency management applications, activities designed to address the immediate and short-term effects of the incident.

Warm disaster recovery site: In the context of disaster recovery, a warm site can provide partial capabilities with equipment, operation, storage, computer equipment such as servers, mainframes and network connectivity. The key concept to consider is the time required to restore a level of service. The closer to “real time”, the “hotter” the recovery site. However, “real time” is rarely the case in manufacturing recovery activity. Warm sites are most typical.

APPENDIX B DOCUMENT REVISION HISTORY

The purpose of this appendix is to capture the changes that were made to this document each time it was published. Please note that section numbers refer specifically to those in the version published on the date shown (i.e., the section numbers are not always the same from version to version).

April 2025. This document has been reorganized to provide a consistent format. Minor editorial changes were also made.

May 2007. This is the first publication of this document.