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 Changes

This is the first publication of this document.

1.2 Superseded Information

There is no superseded information in this document.

2.0 LOSS PREVENTION RECOMMENDATIONS

2.1 Introduction

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 program would assist 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.

This document addresses the general requirements of a disaster recovery program in response to an identified risk at any facility. The disaster recovery program is an extension of the emergency response plan.

2.2 Mitigation

In developing an effective disaster recovery program, complete the following:

- Identify and document a Crisis/Incident Management Team (CMT/IMT) and a Disaster Recovery Team (DRT) for the facility.
- Develop detailed emergency response procedures to include:

  1. A nearby Emergency Operations Center location, suitably stocked with communications equipment and recovery materials;
  2. Actions required to restore normal operations to pre-incident levels within the shortest time possible;
  3. Maintain principles of security (personnel, physical, and information); and
  4. Implement actions for salvage, loss containment, and restoration.

- Test, exercise, and maintain the plan.

2.2.1 Staffing Recommendations

2.2.1.1 The Crisis/Incident Management Team is responsible for managing the incident. The Crisis Management Team is normally, but not necessarily, comprised of senior managers from the company. The CMT is responsible for:

- Deciding whether a disaster is to be declared
- Adapting the plan to account for prevailing circumstances
- Prioritizing the recovery of business functions so as to minimize the impact
- Initiating, controlling, and coordinating the local recovery operations

- Reviewing critical milestones during the recovery process

2.2.1.2 The Disaster Recovery Team is given responsibility for implementing the plan at the site level. The Disaster Recovery Team is comprised of assigned personnel with backup. Determine the roles and responsibilities of the DRT as follows and where applicable:

Table 1. Disaster Recovery Team (DRT) Composition and Contacts

Function	*Roles and Responsibilities*
DR Team Plan Coordinator and Backup	• Take charge of the incident. • Coordinate activity with the 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 and Facilities Personnel	• 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 DRT plan coordinator.
Hazardous Material Coordinator and Personnel	• 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 DRT 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 incident. • Report all incident information to plan coordinator. • Direct all inquiries related to the incident to the organization's media spokesperson.

2.2.2 Risk/Incident Identification

Each facility is susceptible to common threats and risks that could impact the production or service abilities of that facility. Using the table below, identify those risks the facility is most susceptible to and verify that the actions/responsibilities that can mitigate the losses associated with that risk have been reviewed and can be implemented:

Table 2. Incidents and Responsibilities

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, cell phones is 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 if so 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.

2.2.3 Strategy Development and Implementation

Establishing an effective disaster recovery plan can be complex and may require tremendous effort to implement, depending on the nature and size of the facility. It is an ongoing process that must always be kept up-to-date as operations, processes, equipment, and people change. When reviewing an established disaster recovery plan, document the following:

1. Identify alternate processes both upstream and downstream that could be implemented if critical functions or equipment are compromised or fail. Maintain critical spares for important machines.

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

• Evacuation plan • Fire protection plan • Safety and health program • Security procedures	• Employee manuals • Hazardous materials plan • Process safety assessment • Plant closing policy

3. Depending on the size of the organization, the DRT and the CMT headed by the plan coordinators meet with outside groups to discuss and plan for potential emergencies and available resources for responding. Consider the fire service, police department, electric utilities, public works, national weather service, and telephone companies.

4. The DRT and CMT must discuss and put in place internal and external resources needed for emergency recovery, such as personnel, equipment, facilities, and funding. See Table 1 for examples to consider:

Table 3. Internal and External Resources

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

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

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

2.2.4 Test, Exercise and Maintain the Program

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

2.2.4.1 Once the initial recovery plan is in place within the facility, establish regularly scheduled meetings for the DRT members.

2.2.4.2 It is the responsibility of the CMT to assess training needs for the recovery plan. If warranted, develop a training curriculum at all levels within the organization to support the program.

2.2.4.3 It is also the responsibility of the CMT to prepare representative and suitably detailed disaster scenarios. The best way to discover the inevitable deficiencies in any contingency plan is to test it. Include specifics in the exercise such as dates, time, workload, political and economic conditions, accounting period end, and concurrent activities.

2.2.4.4 Execute the disaster exercise or scenario with planned as well as non-planned drills. Consider varying the scenarios from that published, for example by substituting key players.

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

2.2.4.6 At all levels of the organization, 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 corporation are developed primarily at a corporate management level, with contribution from key location management as may be appropriate. Corporate disaster recovery and business continuity plans (DRP & BCP) take into consideration operations for all facilities and potential make-up capabilities between plants, other manufacturers, or suppliers as they 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 for that facility.

It is important to distinguish between an emergency response plan, a disaster recovery plan, and a business continuity plan. 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 1 below to identify the critical timeline for an incident management plan in general and a disaster recovery plan specifically.

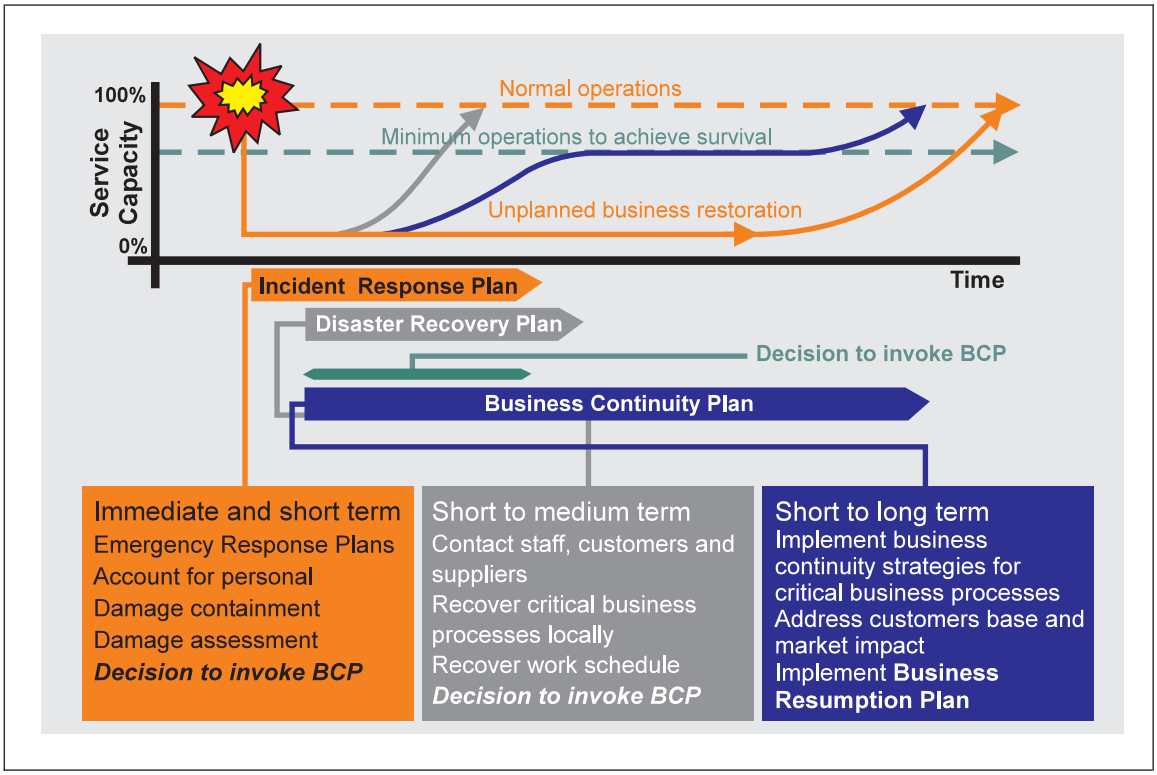

Fig. 1. Phases of Response

Although plans should be tailored to the particular facility, and no two plans are the same, there are a number of key components to incorporate 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, 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 it is a natural disaster or an unforeseen crisis, physical destruction or damage to structures, production lines, and inventory are the obvious perils. Less easy to capture is the negative impact on employee productivity, customer retention, and the confidence of vendors, partners, and customers. Every year, FM Global clients have millions of dollars in business interruption losses. While many of these losses are mitigated due to contingency planning, many of the others are more severe than they should have been because the client did not have a contingency plan. Proper disaster planning makes a big difference: A random sample of losses from FM Global clients found that, of 100 losses analyzed, 54 had some amount of disaster planning in place prior to the loss. Where planning was poor, the average cost was US$7.9 million. Where planning was developed properly, the average dropped to US$4 million a 51% cost reduction.

4.0 REFERENCES

4.1 FM Global

Data Sheet 10-0, *The Human Factor of Property Conservation*

Data Sheet 10-1, *Pre-Incident Planning with the Public Fire Service*

Data Sheet 10-2, *Emergency Response*

Understanding the Hazard publication*, Lack of Contingency Planning* (P0179)

Understanding the Hazard publication, *Lack of Emergency Response (*P0034)

Understanding the Hazard publication, *Lack of a Flood Emergency Response Plan* (P0305)

Understanding the Hazard publication, *Lack of Prefire Planning (*P0033)

4.2 Other

Federal Emergency Management Agency (FEMA). *Standard on Disaster Mitigation Guide for Business and Industry.* FEMA 190, 2004 Edition.

National Fire Protection Association (NFPA). *Standard on Disaster/Emergency Management and Business Continuity Programs.* NFPA 1600, 2004 Edition.

APPENDIX A GLOSSARY OF TERMS

Cold disaster recovery site: A disaster recovery service that provides space, but the customer provides and installs all the equipment needed to continue operations. 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 the disaster.

Emergency and Government authorities: This is 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: In the context of disaster recovery, the definition of a hot disaster recovery site is a redundant facility or a commercial disaster recovery service that allows a business or a facility 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 people take that directly affects on the probability for a property loss incident to occur and/or affects the level of severity that an incident reaches. It can be a positive or negative factor. The hazard of the human factor 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" this is, the "hotter" is the recovery site. However, this is rarely the case in manufacturing recovery activity. Warm sites are most typical.

APPENDIX B DOCUMENT REVISION HISTORY

This is the first publication of this document.

APPENDIX C BIBLIOGRAPHY

Croy, Michael & Geis, James E. "Acronym Soup, BCP, DR, EBR –What Does it All Mean?". *Disaster Recovery Journal*, (Summer 2005); 24 – 26.

Holdburg, Greg. "DR vs. BC Dueling Recovery Plans." *Disaster Recovery Journal'*, (Spring 2005): 32 -34.