Business Continuity Management Program

Disaster Recovery Plan
Development Guide

Project ID: FSEP / E&Y BCM Audit Response

Prepared by: W. Regensburger

Project ID: EY/BCP/DR Audit Response
Version: 1.1
Version Date: 02/8/16

Confidentiality Notice
The information contained in this document was prepared by the University of Southern California Fire Safety & Emergency Planning Office (FSEP). This document and the information contained in it are considered private and confidential to FSEP. No part of this document may be reproduced, reused, or distributed to other parties without the express consent of USC FSEP. If you are in possession of this document and you are not sure whether or not you should be, call the Fire Safety & Emergency Planning department at (213) 740-6197 for information on how to return or dispose of the document.
1 DOCUMENT REVISION HISTORY

This section describes the changes that have been made to this document following its initial development.

<table>
<thead>
<tr>
<th>Date</th>
<th>Ver.</th>
<th>Description of Change</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/3/2016</td>
<td>1.00</td>
<td>Initial Draft</td>
<td>W. Regensburger</td>
</tr>
<tr>
<td>2/8/2016</td>
<td>1.1</td>
<td>Fine-tuned content and formatting</td>
<td>J. Frater</td>
</tr>
</tbody>
</table>

2 PROJECT CHANGE SUMMARY

This section describes the changes that have been made to this project following its initial acceptance by the stakeholders and approval for implementation.

<table>
<thead>
<tr>
<th>Date</th>
<th>Ver.</th>
<th>Description of Change</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

1. **DOCUMENT REVISION HISTORY** .................................................................................................................. 2
2. **PROJECT CHANGE SUMMARY** .................................................................................................................. 2

1. **INTRODUCTION** ........................................................................................................................................ 4
   1.1  PURPOSE ........................................................................................................................................... 4
   1.2  SCOPE AND KEY DEFINITIONS ...................................................................................................... 4
   1.3  GOAL ............................................................................................................................................. 4
   1.4  DOCUMENT MAINTENANCE ............................................................................................................. 4

2. **KEY STAKEHOLDERS** ............................................................................................................................... 4
   2.1  COMMUNICATION RESPONSIBILITIES ............................................................................................. 5

3. **DRP DEVELOPMENT PHASES** ................................................................................................................ 6
   3.1  ASSESSMENT PHASE ....................................................................................................................... 6
   3.2  RECOVERY STRATEGY DEVELOPMENT ........................................................................................... 6
   3.3  DEVELOP DISASTER RECOVERY PLAN ............................................................................................ 6
1. **INTRODUCTION**

1.1 **Purpose**

This program document provides a guide to the IT disaster recovery planning process and the key steps involved in development of the plan.

1.2 **Scope and Key Definitions**

   **Disaster Recovery Plan (DRP):** The technical (e.g., application, network, platform, storage, dependency, etc.) component of business continuity planning to recover a data center, service, component, or application.

   **Recovery Time Objective (RTO):** The maximum amount of time that an organization can withstand the loss of a critical process, function or resource before a serious adverse business impact would result. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

   **Recovery Point Objective (RPO):** From a time perspective, the maximum amount of data loss an organization can sustain during an event.

1.3 **Goal**

To provide clear guidance to university information technology staff on the process of creating an effective disaster recovery plan, and the steps generally necessary in that development process.

1.4 **Document Maintenance**

This document will be reviewed annually and updated as needed, as the project proceeds through each phase of the Business Continuity Management Project life cycle.

This document contains a revision history log. When changes occur, the document’s revision history log will reflect an updated version number as well as the date, the owner making the change, and change description will be recorded in the revision history log of the document.

2. **KEY STAKEHOLDERS**

This section describes the roles and responsibilities of the Business Continuity Management stakeholders with regard to the disaster recovery plan. Listed below are the key stakeholders:

- Crisis Management Team
- BCM Steering Committee
- Executive business sponsor (Dave Wright)
- Program Administrator (FSEP)
- School/Department Coordinator (Team Planner)
- Program owner (Team Leader)
- IT Disaster Recovery Program Coordinator (School/Dept. IT Admin)
- USC Medical Enterprise Program Coordinator (Robert Vance)
- USC Medical Enterprise Program Owner (Paul Craig)
- USC Central ITS CIO (Doug Shook)
2.1 Communication Responsibilities

Crisis Management Team
- The team will communicate and provide direction through the Executive Business Sponsor.

BCM Steering Committee
- The BCS will provide recommendations about communications and serve as a liaison between the Program Administrators and Crisis Management Team.

Executive Business Sponsor
- Communicate BCM expectations and accountabilities relating to plan development, maintenance, training and testing of Business Continuity and Disaster Recovery plans.

Program Administrator
- Ensure the executive business sponsor is informed of the status of planning and other deliverables.
- Communicate the need to perform plan maintenance, training, and exercise to the recovery team planners and team leaders.
- Provide regular training to ensure that all stakeholders are aware of the BCM program and their responsibilities. See training policy document for details.
- Provide informational content for steering committee and crisis management team meetings.
- Stay apprised of and communicate BCM industry trends and best practices.

IT Disaster Recovery Program Planner/Coordinator
- Communicate with the Program Administrator and central Information Technology Services to ensure compliance with plan updates and testing.
- Communicate issues relating to the recoverability of IT systems that do not align with business needs.

School/Department Program Leader/Owner & USC Medical Enterprise Program Leader/Owner
- Communicate with the recovery team planner and recovery team members to ensure program compliance, expectations and accountabilities for business continuity and disaster recovery deliverables, including the BIA, plan development, maintenance, testing and training.

School/Department Program Planner/Coordinator & USC Medical Enterprise Program Planner/Coordinator
- Communicate with recovery teams and the team leader to ensure key deadlines are met. Other communications will include the scheduling of meetings, training and exercises.
- Communicate plan development, maintenance and status to the recovery leader, program administrator, and other internal stakeholders.
- Ensure recovery team members are aware of their roles and responsibilities and that staff and faculty members are aware of the business continuity plan.

USC Central ITS CIO
- Communicate with recovery team planners, leaders, and recovery team members to ensure program compliance, expectations and accountabilities for business continuity/disaster recovery plans.
- Communicate with the decentralized school/department IT administrators relative to IT Disaster Recovery inquiries and guidelines.
- Serve as a subject matter expert to approve or recommend IT disaster recovery strategies that meet university standards.
- Ensure executive level support by communicating with key staff faculty staff and researchers to ensure cooperation and collaborations with all aspects of the BCM program.
- Communicate with schools and departments the information gathering and review protocols for reviewing third party vendors.
3. DRP DEVELOPMENT PHASES

3.1 Assessment Phase

This phase involves process criticality prioritization for each school or department function in order to identify technical recovery requirements. This is accomplished through the following activities:

- **Business Impact Analysis (BIA):** A process designed to prioritize processes by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if the function were absent for a period of time. The same BIA utilized for the BCP should be used for the DRP.
- **Dependency Analysis:** This process identifies both internal and external interdependencies (upstream and downstream processes) required in order for critical IT systems to function. In addition, this process identifies the technical components that constitute IT infrastructure service dependencies.
- **Gap Analysis:** This analysis results in a detailed examination of the identified risks associated with the differences between function (RTO/RPO) requirements and the current available recovery capabilities.
- **Site Risk Assessment:** This task involves collecting site risk data from various sources, and includes technical infrastructure Single Point of Failure (SPoF) analysis to determine design and/or deployment issues that may interrupt production services.
- **Recovery Strategy Development:** Recovery strategy development involves formulating options for closing gaps identified in the Gap Analysis phase of the lifecycle. Each option identified should consider cost versus benefit in filling any gaps.

3.2 Recovery Strategy Development

Once requirements have been determined during the BIA and Dependency Analysis, IT will identify alternate strategies for technology in order to close the gap between Recovery Time Objectives, Recovery Point Objectives, and Recovery Time Capabilities.

**Activities**
- Brainstorm strategies that would meet business needs.
- Consulting with other involved groups, formulate recommended strategy options for presentation to school or department leadership, discussing options and costs.

**Work Products**
- Recovery Strategy Recommendations

3.3 Develop Disaster Recovery Plan

3.3.1 Overview

All information for continuity of critical systems is integrated into the DRP. The DRP should be easy to follow and implement.

This plan development process involves establishing responsibilities by breaking down the function into units or teams to implement both immediate procedures to continue critical processing (i.e., those procedures which must be performed within the first 72 hours or less from a disaster declaration) as well as longer-term recovery and restoration procedures (i.e., those procedures implemented to restore operations to its status prior to the disaster).
The DR plan also documents all internal and external support resources required, such as applications, processes for archival of data and records, off-site storage facilities, hardware spares inventories, redundant or diverse communications access for voice and data lines, procedure manuals and critical documentation, supplies and forms, third-party vendors, suppliers and partners.

The development of the plan also includes documenting all tasks to be performed including notification of team personnel and third parties and off-line processing procedures and recovery procedures for each recovery team. These tasks are identified according to recovery time frames, detailing when each element must be completed in order to ensure optimal recovery.

SEE: Disaster Recovery Plan Template

3.3.2 Activities
Determine plan development participants. Identify individuals to represent each IT resource and to participate in the plan development activity.

- Schedule DRP development workshop to discuss plan requirements and parameters.
- Complete the plan template, customizing it where necessary.
- Provide plan development support to plan developers, as necessary.
- Review draft plans
- Receive additional revisions and correct in the template.
- Present draft plans to unit leadership for approval.
- Provide annual attestation to USC Information Security Office (usc-ciso@usc.edu).