

1.0 Purpose

The purpose of the Contingency Plan Procedures is to support the restoration of operations, computing resources, and critical data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

The HIPAA Security Rule that governs this procedure is: *164.308(a)(7)(i) Contingency Plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Procedures defined in this document include:

- Application and Data Criticality Assessment (section 3.2)
- Data Backup Plan (section 3.3)
- Disaster Recovery Plan (section 3.4)
- Emergency Mode Operations Plan (section 3.5)
- Contingency Plan Testing and Revision (section 3.6)

2.0 Definitions

2.1 Contingency plan: Management policy and procedures designed to maintain and restore business operations, including computer operations, possibly at an alternate location, in the event of system failures, emergencies, or disaster.

2.2 Workforce: All faculty, staff, students, trainees, volunteers, and business associate who access restricted or confidential information during the course of their duties.

3.0 Procedures & Responsibilities

3.1 Contingency Operations Plan: Computer system managers, system owners, and unit and department managers must implement procedures for developing a plan to allow physical access to facilities in which restricted or confidential information is housed in the event of an emergency. Refer to the Facility Access Controls Procedures for further details.

3.2 Application and Data Criticality Assessment: System managers and owners must implement procedures for assessing the criticality of applications and data files.

3.2.1 Define Preliminary System Information: Define the organization name, system name and system manager point of contact. Provide a description of the system including purpose,

architecture and any supporting system diagrams.

3.2.2 Identify System Points of Contact: Identify and coordinate with internal and external points of contact associated with the system to characterize the ways that they depend on or support the IT system. When identifying the points of contact, it is important to include organizations that provide or receive data from the system as well as contacts supporting any interconnected systems. This coordination should enable you to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

3.2.3 Identify System Resources: Identify the applications, data files, and IT resources critical to the objectives listed in the emergency mode operations plan.

3.2.4 Identify critical roles: List the critical roles of the individuals identified in the Emergency Mode Operations Plan and the Disaster Recovery Plan.

3.2.5 Develop recovery priorities: Based on the results of the criticality assessment, categorize applications by order of criticality based on contingency resource allocations and expenditures, time, effort and costs.

3.3 Data Backup Plan: System managers and owners must implement procedures for developing a data backup plan to ensure the availability, integrity, and security of data.

3.3.1 Identify critical data files to backup: List critical files identified from the application and data criticality assessment.

3.3.2 Define backup frequency: Define the frequency of full and incremental backups respective to each application and operating system.

3.3.3 Define retention period: Define the retention period respective to each application, operating system, taking into consideration the frequency of full and incremental backups for each one.

3.3.4 Identify offsite storage: If offsite storage is required, identify a secured facility in which backups will be stored.

3.3.5 Define backup retrieval process: Identify the individuals who are authorized to request a retrieval of backup from the secured facility. Identify the method of transporting

retrieved backups from the secured facility.

3.4 Disaster Recovery Plan: System managers and owners and unit and department managers must implement procedures for developing a disaster recovery plan.

3.4.1 Define Notification process. Include a list of the affected teams and decision-makers involved in the disaster recovery effort.

3.4.2 Identify Activation team: Identify the team members responsible for performing contingency plan activation.

3.4.3 Define Damage Assessment procedures: List procedures utilized to perform damage assessment.

3.4.4 Define procedures for Restoring Applications and Data using backup copies in sequence relative to the application criticality assessment.

3.4.5 Identify Deactivation team: Identify team to perform contingency plan deactivation.

3.5 Emergency Mode Operations Plan: System managers, system owners and unit and department managers must identify critical business processes, implement reasonable security procedures for critical business processes consistent with procedures employed during normal mode of operations, and ensure the protection of ePHI while operating in emergency mode.

3.6 Contingency Plan Testing and Revision: System managers, system owners and unit and department managers must implement procedures for testing and revising contingency plans:

3.6.1 Identify contingency plan elements to test: List the selected elements identified within the contingency plan that must be tested and periodically revised to ensure that all of the elements of the contingency plan remain current and are effective.

3.6.2 Define test objectives: List the specific objective for each test element and the overall test plan.

3.6.3 Identify test participants and roles: List each test participant and the specific roles they are to perform within the test.

3.6.4 Define test scenario: List the specific scenario that will be utilized for the test. In determining the scenarios consider both the worst-case incident and those incidents that are most

likely to occur. Test scenarios should mimic reality as closely as possible. List the time frames associated with each test element and for each of the test participants.

3.6.5 Execute test and document results of test: Test results and lessons learned should be documented and reviewed with the test participants and other personnel as appropriate.

3.6.6 Revision of Contingency Plan: To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Periodic reviews of the plan must be conducted in addition to reviews whenever there are changes affecting:

- Operational requirements
- Security requirements
- Technical procedures
- Changes of hardware, software, and other equipment
- Changes with alternate facility requirements
- Changes with team members and team members contact information

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

A copy of the Contingency Plan must be stored offsite, remote from the systems for which contingencies have been developed.

6.0 Related Documents

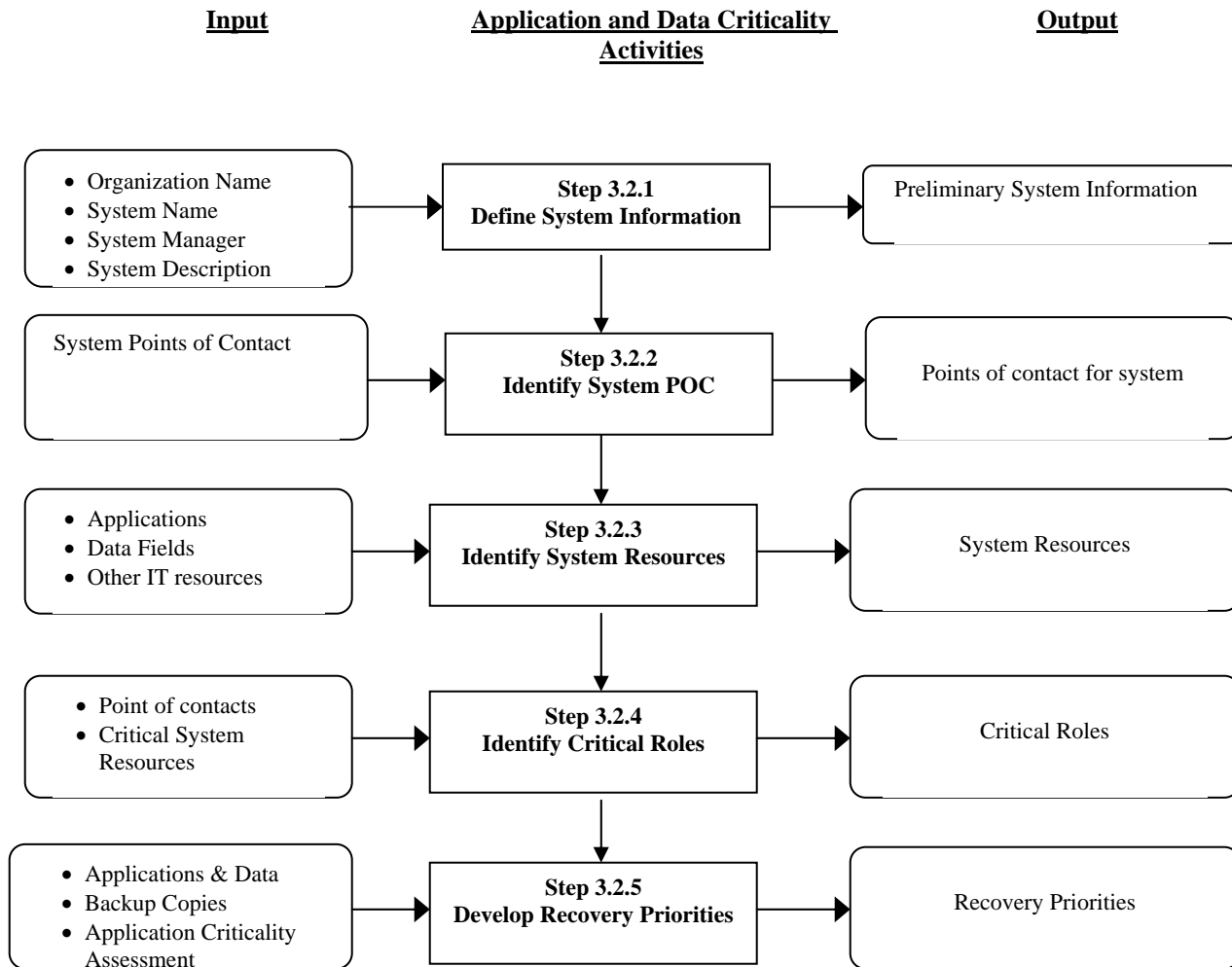
Document Name	Procedure No.
HIPAA Security Rule: Contingency Plan	164.308(a)(7) http://www.ucsf.edu/hipaa/d/ept_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	BFB IS-3 http://www.ucsf.edu/hipaa/d/ept_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
UCSF Information Security and Confidentiality Policy	650-XX http://www.ucsf.edu/hipaa/d/ept_compliance/
UCSF Medical Center Administrative Policy - Information Security and Confidentiality Policy	5.01.04 http://www.ucsf.edu/hipaa/d/ept_compliance/
Special Publication: Contingency Planning Guide for Information Technology Systems - National Institute of Standards and Technology (NIST)	SP 800-34 http://www.ucsf.edu/hipaa/d/ept_compliance/
Presentation at January 22, 2004 CSC Workshop #3 on Contingency Planning	http://www.ucsf.edu/hipaa/d/ept_compliance/
System Management Procedures	60-001 http://www.ucsf.edu/hipaa/d/ept_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	12/17/04	Mark Monaghan and Jim Grubb	Initial Release, modified to match SOM template.

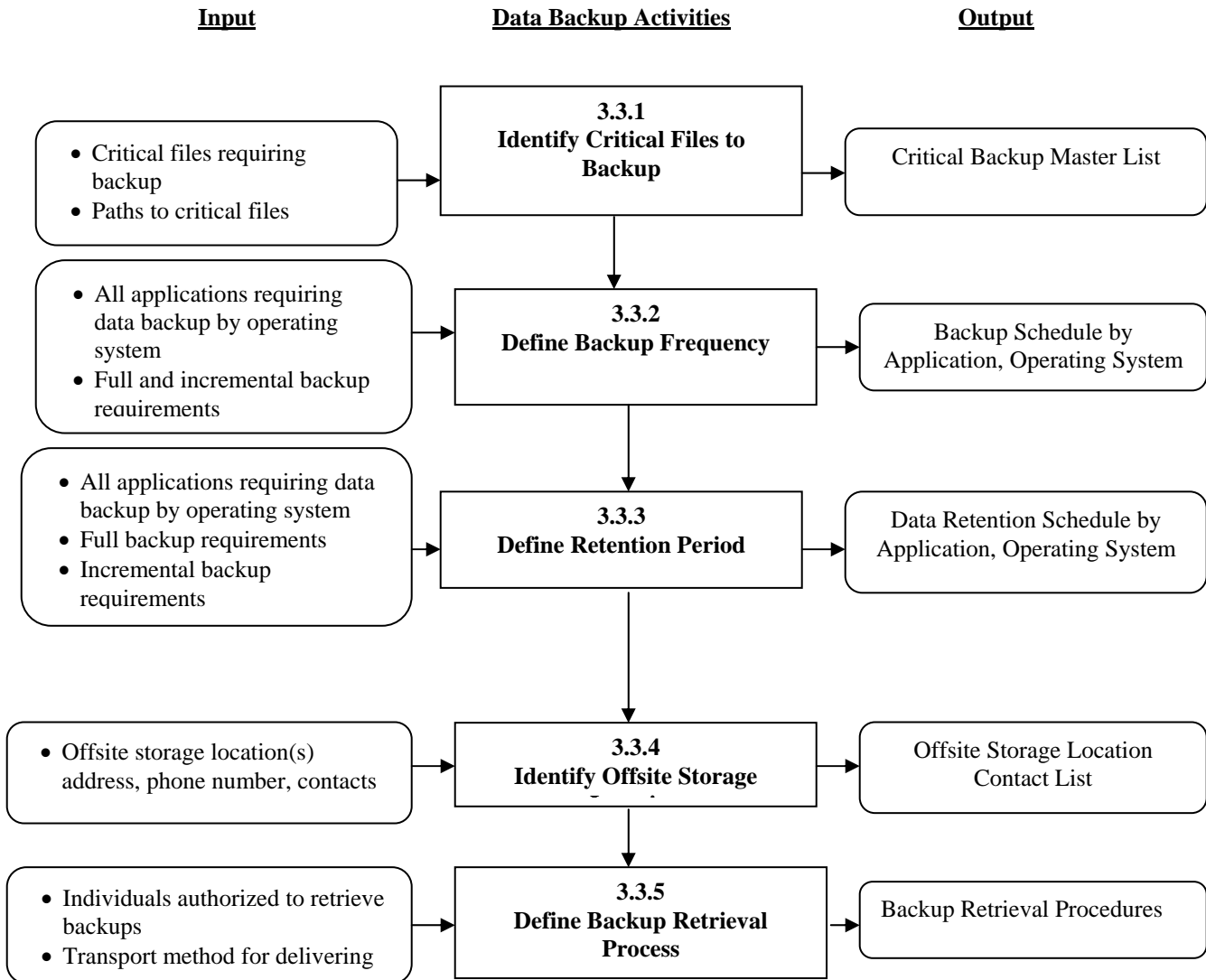
If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Appendix A: Application and Data Criticality



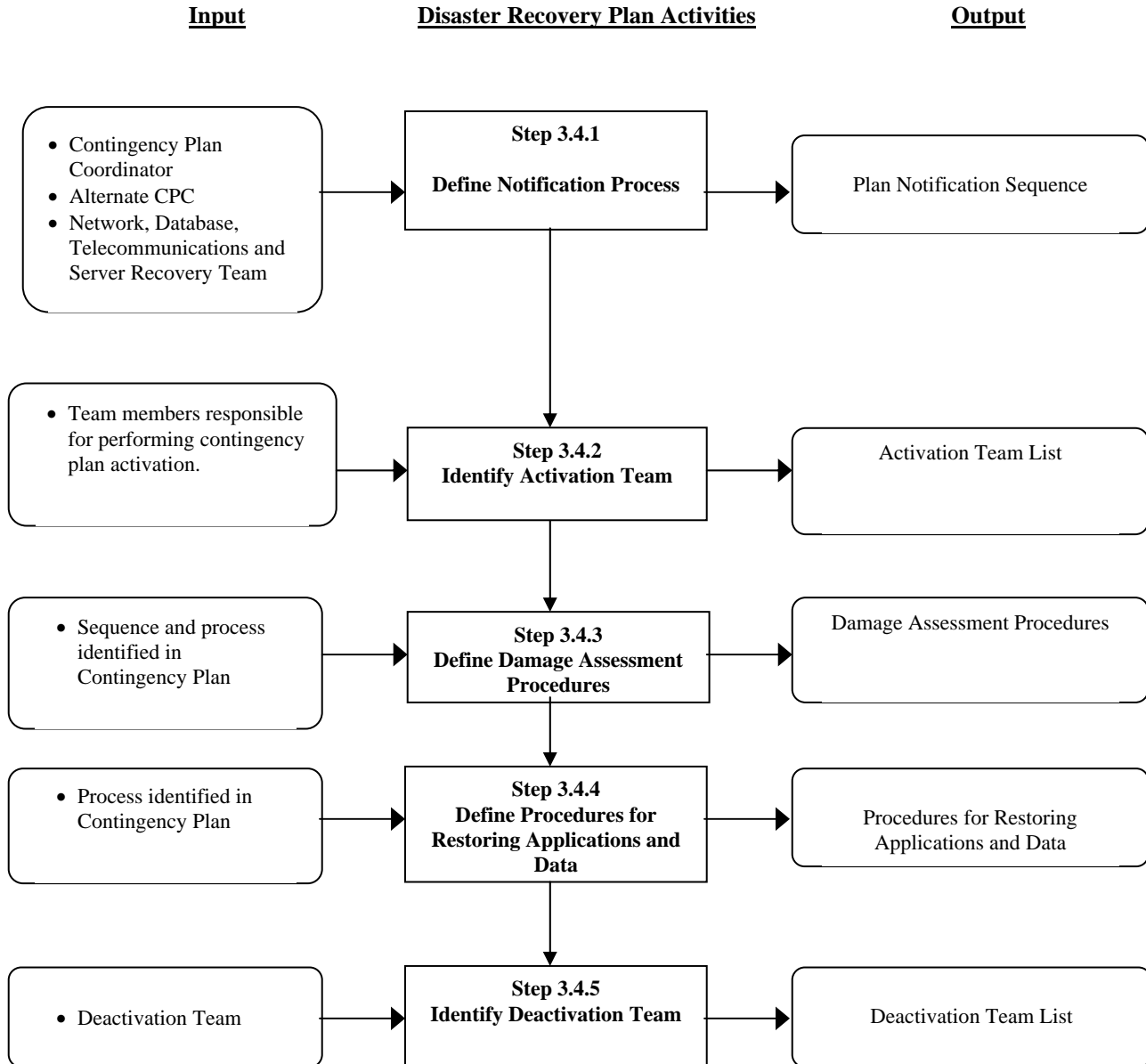
If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Appendix B: Data Backup



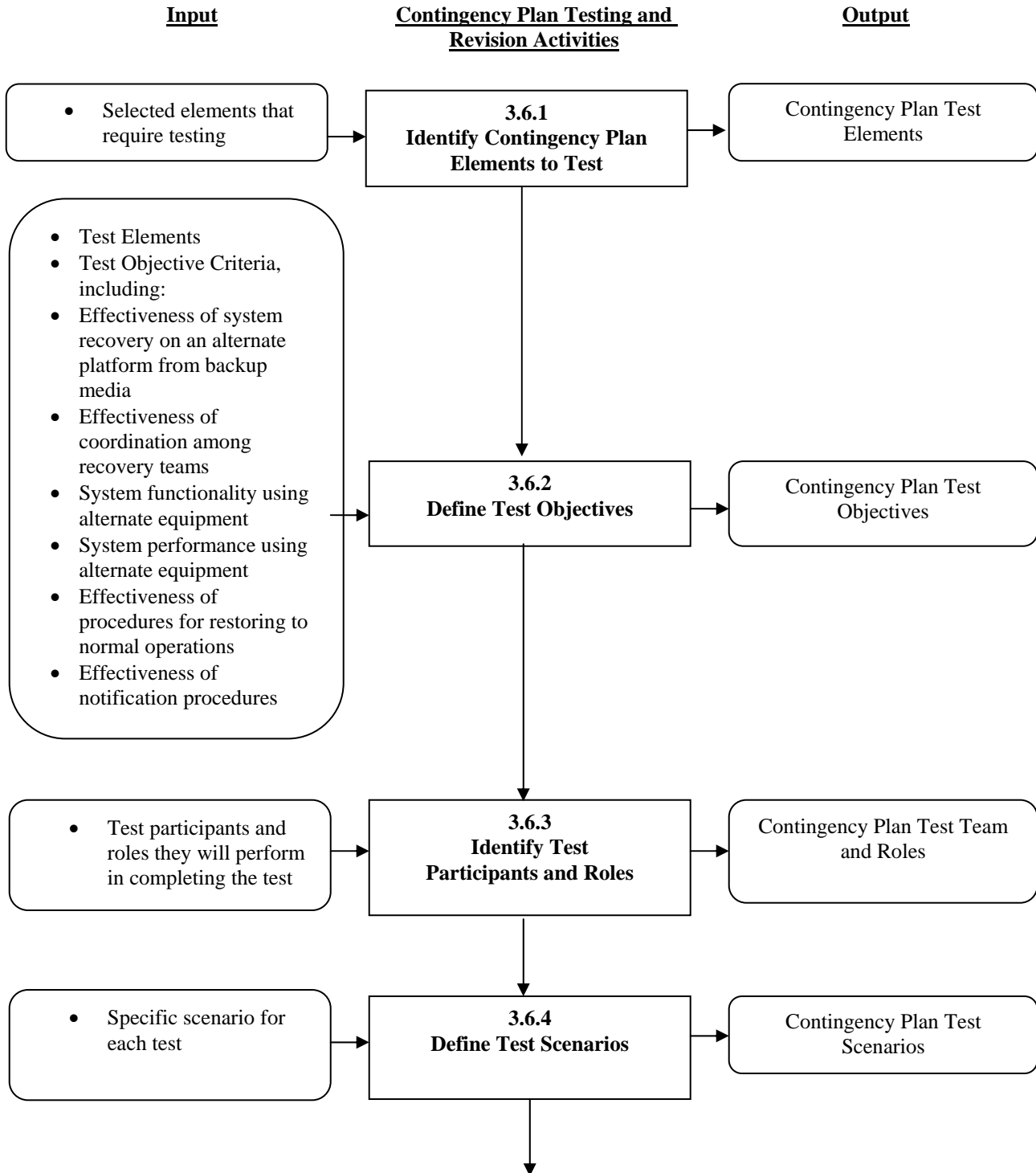
If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.

Appendix C: Disaster Recovery Plan



If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.

Appendix F: Contingency Plan Testing and Revision



If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.

