
State of California
California Information Security Office
Technology Recovery Plan
Instructions

SIMM 5325-A

(Formerly SIMM 65A)

September 2013

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	November 2009	Office of Information Security and Privacy Protection	
Minor Update	September 2013	California Information Security Office (CISO)	SIMM number change, change “agency” to “state entity”, change “disaster recovery” to “technology recovery”, and change references to other related SIMM documents

TABLE OF CONTENTS

INTRODUCTION AND APPLICABILITY	1
INSTRUCTIONS	1
SECTION 1: MINIMUM TRP REQUIREMENTS	1
1.0 STATE ENTITY ADMINISTRATIVE INFORMATION	1
2.0 CRITICAL BUSINESS FUNCTIONS/APPLICATIONS	2
3.0 RECOVERY STRATEGY	2
4.0 BACKUP AND OFFSITE STORAGE PROCEDURES	2
5.0 TECHNOLOGY RECOVERY PROCEDURES	3
6.0 DATA CENTER SERVICES.....	3
7.0 RESOURCE REQUIREMENTS	3
8.0 ASSIGNMENT OF RESPONSIBILITY	3
9.0 CONTACT INFORMATION.....	3
10. TESTING.....	4
SECTION 2: SUPPLEMENTAL TRP REQUIREMENTS	4
1.0 DAMAGE RECOGNITION AND ASSESSMENT	4
2.0 MOBILIZATION OF PERSONNEL	4
3.0 PRIMARY SITE RESTORATION AND RELOCATION.....	5
SECTION 3: APPENDICES.....	5

INTRODUCTION AND APPLICABILITY

The requirements included in this document are applicable to all state entities that operate, manage, or use information technology to support business functions in the State of California. This document identifies sections that describe the minimum requirements that a state entity must include as components of its Technology Recovery Plan (TRP), previously known as a Disaster Recovery Plan (DRP). The TRP is just one portion of contingency planning and business continuity. A full business continuity plan includes emergency/disaster management, business resumption, and technology recovery plans.

As required in State Administrative Manual (SAM) Section 5325 (Business Continuity with Technology Recovery), each state entity is required to participate in technology recovery planning processes to reduce the risks associated with unanticipated outages for their critical applications and systems. Additionally, SAM Section 5325.1 (Technology Recovery Plan) requires each state entity to maintain an up-to-date and tested TRP. Finally, as required in SAM Section 5330.2, by January 31st of each year, or as designee changes occur, agencies must designate and provide contact information for their Technology Recovery Coordinator by submitting the Designation Letter (SIMM 5330-A) to the California Information Security Office (CISO).

INSTRUCTIONS

These sections generally describe the minimum requirements for TRP development. If the state entity's TRP does not follow this format, then include a cover sheet to indicate where information on each component can be located.

SECTION 1: MINIMUM TRP REQUIREMENTS

1.0 STATE ENTITY ADMINISTRATIVE INFORMATION

- 1.1 An executive summary that serves as a guide to the structure of the plan, the procedures for updating (plan maintenance) and distributing the plan, and a description of the state entity's test and awareness programs.
- 1.2 A description of the state entity's mission, including the organizational, managerial and technical environments. This section should include organization charts, business functions, and a description of the state entity's information technology environment.
- 1.3 A list of state entities that are included in your recovery plan (e.g., if your state entity includes TRP recovery for another state entity or organization).
- 1.4 A communication strategy noting information flow, decision making, and interrelationship among state entity core resources for response, recovery, and resumption.

- 1.5 A list of state agencies that provide services required in your recovery plan (i.e., State Controller's Office, Department of General Services, Department of Technology).

2.0 CRITICAL BUSINESS FUNCTIONS/APPLICATIONS

- 2.1 A description of critical business functions and their supporting applications, a designation of maximum acceptable outage timeframes for each application, and the recovery priorities.
- 2.2 This section should include a chart that lists the critical business functions, the supporting applications, designation of maximum acceptable outages for the applications and the recovery priorities.
- 2.3 The state entity may also include information on the approach used to determine the recovery priorities (e.g., a business impact assessment or planning committee meeting).

3.0 RECOVERY STRATEGY

- 3.1 A description of the portions of the plan that will be implemented based on various levels of incident severity, for example, minor interruption of service, total service failure or loss of facility. Recovery strategies should be built to accommodate a worst case scenario, loss of service and facility. Plans for catastrophic or regional disasters should be addressed in the COOP/COG Plan.
- 3.2 A description of the recovery strategy that supports the state entity's critical application priorities, including identification and evaluation of alternative recovery strategies. Will the state entity sustain critical business functions manually until the applications are recovered? Does the state entity contract with an outside source for recovery services? Will the state entity's information technology infrastructure be rebuilt at another location? Will a hot or cold site be used?
- 3.3 Alternate recovery sites should be detailed within the plan that includes location, contact numbers and the type of facilities/equipment that will be available.

4.0 BACKUP AND OFFSITE STORAGE PROCEDURES

- 4.1 Backup and retention schedules and procedures are critical to the recovery of an state entity's applications and data.
- 4.2 The detailed procedures should include hardware, software (including version), data file back-up and retention schedules, off-site storage details, and appropriate contact and authority designation for personnel to retrieve media.

5.0 TECHNOLOGY RECOVERY PROCEDURES

- 5.1 This section systematically details the operational procedures that will allow recovery to be achieved in a timely and orderly way.
- 5.2 Detailed recovery procedures (including manual processes) that support the state entity's recovery strategy and provide for the recovery of critical applications within the established maximum acceptable outage time frames. Included would be the process for recovering the critical data-processing activities, application and data recovery, and the process for suspending non-critical activities and any relocation to an interim (back-up) processing site.
- 5.3 The procedures should be detailed enough so that another trained information technology professional would be able to recover the state entity's infrastructure should those with primary responsibility be unavailable during the recovery process. Include a high-level network diagram that includes all critical applications.

6.0 DATA CENTER SERVICES

- 6.1 For agencies using the services of a data center, a description of data center services that will be provided during recovery must be documented.
- 6.2 Include information on any interagency agreements, memorandums of understanding, or contracts.
- 6.3 If specific coordination of efforts with the data center is critical to the state entity's recovery, those procedures should be included within Section 5 above.

7.0 RESOURCE REQUIREMENTS

- 7.1 A comprehensive list of the equipment, space, telecommunication needs, data, software, hard-copy references (forms and procedures), and personnel necessary for recovery is essential.
- 7.2 Identification of resources that will be available at an alternate site should also be documented.

8.0 ASSIGNMENT OF RESPONSIBILITY

- 8.1 Distinct management and personnel assignment of responsibilities must be clearly designated within the technology recovery plan. Within procedures, job titles (rather than the names of individuals) should be used to assign responsibility as it lessens maintenance on procedures as personnel changes.

9.0 CONTACT INFORMATION

- 9.1 Separate contact lists should include the names of individuals, job title and contact information. If home phone numbers are included, the contact lists should be designated as confidential sections of the technology recovery plan.
- 9.2 Contact lists for vendors, other government entities, and outside resources critical to the state entity's recovery process.

10. TESTING

- 10.1 A description of the annual technology recovery test(s) performed, including how the test(s) were conducted, high level timeframes for each test, and the level of testing appropriate to the complexity of the system(s), program(s), process(es), or organization(s) being recovered. Examples of testing may include tabletop exercises, data recovery testing, forced testing (actual recovery due to an unplanned outage or failure), and/or full plan testing.

SECTION 2: SUPPLEMENTAL TRP REQUIREMENTS

Agencies that have not developed and implemented a full business continuity plan or COOP/COG must also include the following three supplemental components in their TRP.

1.0 DAMAGE RECOGNITION AND ASSESSMENT

- 1.1 This section details the emergency response actions necessary immediately following the disaster including: protecting the health and safety of all personnel; gaining immediate emergency assistance from state entity security, fire, police, hospitals, etc.; notifying state entity personnel that are members of an coordinating the response/recovery program, disseminating information and assembling personnel.
- 1.2 Damage assessment includes the procedures and personnel necessary to assess the damage and determine the level of severity of the incident, including the decision support mechanism required to declare a disaster versus a less severe interruption in processing capability.

2.0 MOBILIZATION OF PERSONNEL

- 2.1 This section details personnel and management responsibilities for putting the remainder of the plan into effect. Included may be team or individual assignments of responsibility by area of expertise such as:
 - 2.1.1 Technical personnel in the areas of systems software, telecommunications, and computer operations.
 - 2.1.2 User personnel and management to assist in resolution of programmatic issues.
 - 2.1.3 Business services to support such tasks as arranging for office space, supplies, equipment, and processing of emergency contracts.
 - 2.1.4 Personnel and communications staff to disseminate information regarding special work assignments, conditions, or locations.

3.0 PRIMARY SITE RESTORATION AND RELOCATION

- 3.1 This section includes detailed procedures to be followed after the interim processing situation has stabilized. The intent is to provide a framework for restoring full processing capability at a permanent location. Many of the same procedures will be used as were included during the moving of applications and systems to an interim site as described in the Recovery Plan Implementation procedures.

SECTION 3: APPENDICES

A variety of appendices may be attached to the TRP. Many of the plan sections described above will contain static procedures, while others may contain operational information that requires continual maintenance.

Some examples of appendix topics may include:

- Emergency action notification information containing the names and phone numbers of the various management, personnel and specialty team members;
- Damage assessment or disaster classification forms intended to function as a guide to supplement/support the management decision process;
- Profiles of critical applications;
- State entity hardware and system software inventory; and
- Any data communications network routing information necessary for providing interim processing capability and restoring full processing capacity.