CONTINUITY PLANNING WITH TECHNOLOGY RECOVERY - 5325

(Revised: ~~114~~309/~~2025~~2026)

Introduction:

Continuity planning establishes procedures to sustain business and mission-essential functions during and after a significant disruption or disaster. A Business Impact Analysis (BIA) is a critical input to effective continuity planning, providing the foundation for contingency strategies and the development of a Technology Recovery Plan (TRP).

The BIA identifies and prioritizes system components by mapping them to the business or mission processes they support, enabling organizations to assess the potential impact if those systems become unavailable. The TRP is an official, detailed plan that supports technology-related continuity, recovery, and restoration objectives defined through the BIA and broader Continuity Planning efforts.

Policy: Each state agency or entity must ensure that individuals with subject matter expertise in business and mission-essential functions lead and actively participate in continuity and technology recovery planning efforts. These individuals must:

1. Conduct an enterprise-wide BIA to support the development of a comprehensive inventory of IT system(s) consistent with SIMM 5325-B categories that enable business and mission essential functions. The BIA should identify key components such as system dependencies, recovery criticality, resource requirements, recovery time objectives (RTOs), and sequencing priorities. These elements should align with the requirements outlined in SAM 5325.1 and SIMM 5325-A.
2. Develop a Continuity Plan that outlines procedures for how the state agency or entity will maintain essential functions and continue delivering necessary services during a significant disruption or disaster. The Continuity Plan should align with the California Office of Emergency Services (CalOES) State Continuity Planning Objectives, as outlined in Executive Order S-04-06. For guidance or assistance, contact Cal OES Continuity Planning at continuity@caloes.ca.gov.
3. Leverage the BIA and Continuity Plan to develop a TRP that includes detailed recovery procedures and supporting documentation, in accordance with SAM 5325.1 and SIMM 5325-A requirements. The TRP must ensure that critical systems and services can be restored to support business and mission essential functions.
    a. To facilitate recovery and restoration efforts, ensure the following are developed or conducted for critical systems to support TRP activities:

i. Information system recovery plans are developed and included in the TRP.

ii. System security plans (SSP), developed in accordance with SAM 5315, SIMM 5325-A, and SIMM 5355-B, are maintained and available for inspection upon request by OIS. Self-assessments of NIST controls for SSPs have been completed and documented in Cal-CSIRS.~~consistent with SAM 5315, SIMM 5325-A, and SIMM 5355-B requirements, are developed and available for inspection upon OIS request.~~

iii. Privacy Threshold Assessment (PTAs) and, where applicable, Privacy Impact Assessments (PIAs), consistent with SAM 5310.8 and SIMM 5310-C requirements, are conducted and available for inspection upon OIS request.

iv. TRP training is developed and delivered at least annually, consistent with SAM 5325.2, to ensure personnel are prepared to execute recovery procedures.

v. TRP testing is conducted at least annually, in accordance with SAM 5325.3 and SIMM 5325-A, to validate the effectiveness of recovery strategies and identify areas for improvement.

4. Develop and document procedures to ensure the BIA, Continuity Plan, and TRP with supporting documentation, are maintained and updated annually or when necessary, as significant changes or lessons learned resulting from post-incident analysis, training, testing, or TRP review occur.

Note: Continuity Plans must address CalOES' Continuity Planning requirements available at: https://www.caloes.ca.gov/office-of-the-director/operations/planning-preparedness-prevention/planning-preparedness/continuity-planning/

Implementation Controls: NIST SP 800-34; NIST SP 800-53: Contingency Planning (CP) section described in NIST SP 800-53; NIST IR 8286D; NIST CSF 2.0 IDENTIFY (ID), PROTECT (PR), RESPOND (RS), RECOVER (RC); SIMM 5325-A; SIMM 5355-B; SIMM 5310-C; SAM 5300.4; SAM 5305.6; SAM 5305.7; SAM 5305.5, SAM 5310.8, SAM 5315, SAM 5325.1, SAM 5325.2; Executive Order S-04-06

REVISIONS

- BUSINESS CONTINUITY WITH TECHNOLOGY RECOVERY – 06/2018