

**SAM – INFORMATION SECURITY**  
**(Office of Information Security)**

**BUSINESS CONTINUITY WITH TECHNOLOGY RECOVERY**

5325

(Revised 12/13)

**Introduction:** The entire concept of business continuity is based on the identification of all business functions within a state entity, and then assigning a level of importance to each business function. A business impact assessment is the primary tool for gathering this information and assigning criticality, recovery point objectives, and recovery time objectives, and is therefore part of the basic foundation of contingency planning and business continuity.

**Policy:** Each state entity shall ensure individuals with knowledge about business functions of the organization lead and participate in the business continuity planning process to:

1. Identify and document all business functions;
2. Conduct a business impact assessment to identify:
  - a. critical functions and systems, and prioritize them based on necessity;
  - b. threats and vulnerabilities; and
  - c. preventive controls and countermeasures to reduce the state entity's risk level.
3. Develop recovery strategies to ensure systems and functions can be brought online quickly;
4. Develop the Business Continuity Plan to include procedures for how the state entity will stay functional in a disastrous state;
5. Conduct regular training to prepare individuals on their expected tasks;
6. Conduct regular tests and exercises to identify any deficiencies and further refine the plan; and
7. Develop steps to ensure the Business Continuity Plan is maintained and updated regularly.

Note: The Business Continuity Plan must also address the Office of Emergency Services' continuity planning requirements. These are available at: <http://www.calema.ca.gov/PlanningandPreparedness/Pages/Continuity-Planning.aspx>

**Implementation Controls:** NIST [SP 800-34](#); NIST SP 800-53: [Contingency Planning \(CP\)](#)