

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

**DISASTER RECOVERY PLANNING**

**5355.1**

(Revised 10/09)

Disaster recovery planning (formerly known as operational recovery planning) provides for continuity of computing operations in support of critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly migration toward the resumption of all computing services within an agency following a business disruption. It is essential that critical IT services and critical applications be restored as soon as possible.

It is significant to recognize that no disaster recovery program is ever complete. All disaster recovery planning is based upon available knowledge and assumptions, and must be adapted to changing circumstances and business needs, as appropriate. Strategies, procedures, and resources must be adapted as often as necessary in order to recover critical applications. Recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

The disaster recovery planning process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. Agencies should consider the results of their risk analysis process and their business impact analysis when developing their Disaster Recovery Plan (DRP). See SAM Section 5305 for requirements regarding risk analysis. Each agency's process should culminate in a viable, fully documented, and tested DRP. See SIMM Section 65A for requirements and guidelines regarding disaster recovery.

To provide for recoverability of new systems, all agencies must include disaster recovery considerations and costs in project authority documents and budget proposals. See SAM Section 4900 et seq. and SIMM Section 20 for requirements and guidelines.

To improve the likelihood for the full recovery of key business processes, DRPs should be developed as part of a complete business continuity program which includes emergency response and business resumption plans.