

Disaster Recovery Plans – What We Look For and Why

Either an Agency DRP Transmittal Letter (SIMM 70D) *or* DRP Certification (SIMM 70B) form - *either one signed by the agency secretary/director or by a SIMM 70A pre-identified designee*, delivered in accordance with the DRP submission schedule.

- An agency director is ultimately responsible for recovery of the IT environment and may identify a designee to sign for him/her. That designee is signing FOR the director and is accepting responsibility on his/her behalf. We must have that form on file indicating that responsibility has been identified and accepted.
- A Certification may be submitted every other year provided a full plan was filed the previous year and nothing has changed (either by the agency or required by the OIS based on review of prior submission).

Compliance with SAM 5355.2 requirements and SIMM 65A format (refer to cross-reference sheet/checklist to be sure).

- The SIMM 65A format ensures that all required components are addressed. If the format is not used, the cross-reference sheet may be used in its place to identify where required components may be found. If the format is not used *and* a cross-reference sheet is not included, the plan cannot be reviewed.

Evidence that the plan was written for the organization, not for the OIS. This is typically demonstrated through verbiage addressed to recovery staff, and step-by-step instructions for recovery of technical environment.

- Specific recovery procedures for essential/critical data/ applications are for recovery staff (may or may not be your employees) to follow – remember, your primary SME may not be available! This is your agency’s plan for recovery, and procedures must be clear enough for anyone technically savvy enough to follow and recover your IT systems.

Critical/essential BUSINESS functions have been identified, with recovery plans for the critical/essential applications that support them.

- Plans must be developed based on recovery of an organization's mission critical business functions. The executive level business management team decides what is mission critical, and the recovery priorities and objectives for your organization.

Critical inter and intra departmental dependencies, such as those with a state data center, SCO, SPB, DOF, etc., and coordinating recovery procedures.

- Recovery of state government cannot occur successfully if all attempt to recover in silos. We are all inter-dependent and must consider those inter and even intra-dependencies.

Critical data/applications hosted at a state data center and recovery plans and procedures for those, and inter-relationships between the data center plan and your agency plan with coordinating recovery procedures.

- Each agency that employs the services of a state data center must develop an understanding of the existing service level agreement for recovery services, and its recovery plan must document the data center services that will be required during recovery. Don't assume the data center will be automatically recovering data/applications hosted at the data center.
- Each agency that employs the services of a data center must also provide the data center with a subset of its plan containing enough information for the data center to recover the agency's systems and/or data.

Exercise schedule, description, results, remediation plans. The agency must perform an alternate exercise every other year so different components of the plan are tested.

- Exercises must be a regular part of disaster recovery planning to ensure that assumptions made during plan development play out as designed. The worst time to discover that plans are based on mistaken assumptions is during a disaster!