

Software Data Restoral Evaluation – Examples

Mission Assurance Category Requirements

Mission assurance category (MAC) requirements for data backup procedures and for disaster and recovery planning directly affect data restoral requirements and can be found in DoD Directive 8500.1 and DoD Instruction 8500.2.

- MAC I:
 - Continuity of Operations – Data Backup (CODB)-3 Procedures

Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

- CODP-3 Disaster and Recovery Planning

A disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

- MAC II:
 - CODB-2 Data Back-up Procedures

Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

- CODP-2 Disaster and Recovery Planning

A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Example TEMP entry for MAC-I System:

Global Command and Control System – Joint (GCCS-J) is a command and control system rated as Mission Assurance Category I. The Joint Operations Planning and Execution System (JOPES) within GCCS-J has four primary, fully redundant strategic server enclaves (SSEs), with data also fully replicated across all four SSEs. The following criteria for JOPES have been summarized to capture the most relevant parts.

3.2 Evaluation Framework (for JOPES)

- System Availability: more than 99.7 percent.
- Disaster Recovery. Mean time to restore function (MTTRF) on any single system shall be within 24 hours. JOPES SSE database recovery backup must be within 12 hours.

Software Data Restoral Evaluation – Examples

- System ability to support mission essential JOPES activities (minimize in effect) following loss of one or more sites:
 - Capable of supporting users after loss of 50% of the sites for not less than 96 hours.
 - Capable of supporting users after loss of JOPES Network Support for not less than 4 hours.
- Strategic servers will have the capability to be mirrored, maintain data accuracy, and process data consistently.
 - Most current update available in a server to an authorized GCCS-J application user within 3 minutes.
 - JOPES SSE - Upload and network, to all available servers, a 150,000 Time Phased Force Deployment Decision (TPFDD) in an average of 8 hours.

Example TEMP entry for MAC-II System:

Global Combat Support System – Army (GCSS-A) is a tactical logistics data system rated as Mission Assurance Category II. GCSS-A has a primary server center and an alternate Continuity of Operations (COOP) center. Data is mirrored from the primary site to the alternate site at some specified interval of time which does not exceed four hours. The data restoral KPP for GCSS-A addresses both the disaster recovery time (24 hours threshold) as well as the mirroring frequency (not more than 4 hours).

3.2 Evaluation Framework (for GCSS-A)

(other information goes here)

KPP or KSA	Threshold	Objective
1.Continuity of Operations and System Restoration	GCSS-Army shall recover GCSS-Army critical capabilities within 24 hours (the MAC II requirement) of declaration of a disaster to a state not more than 4 hours prior (the data mirroring frequency) to disaster.	GCSS-Army shall recover GCSS-Army critical capabilities within 24 hours of declaration of a disaster to a state not more than 2 hours prior to disaster.