

Date Issued	March 2, 2004
Issued By	CEO
Revision Date	May 10, 2004
Approved By	Board of Directors

RM01 – Recovery Procedures CUSA Disaster Recovery Testing

The institution recognizes the need to evaluate the effectiveness, efficiency, and practicality of the institution's BCP strategies, policies, procedures, and provisions for disaster recovery. Section 6.2 | Testing Methodology of the BCP document outlines the institution's adopted testing strategies.

The procedures below have been specifically developed for hot-site testing, to ensure that the institution's location, internal and external resource, equipment, software, communications, forms, supplies, reports, documentation, and files requirements are adequately maintained at both the hot-site and final recovery site locations. They should be modified or additional procedures should be developed, as required, based upon the specific testing strategies of the institution.

BCP testing should occur at least annually and should coincide with annual plan maintenance (RM02-BCPMaintenance.doc). In addition to annual plan testing, BCP testing should be conducted any time significant changes are made to the institution's organization, IT/production environment, hot-site provider, or other-related recovery elements or as changes in external regulatory compliance requirements dictate.

In addition to DP recovery testing, the institution may choose to execute alternate BCP testing methodologies (e.g. walk-through, table top), which are described in Section 6.2 | Testing Methodology of the BCP document. Procedures for additional methodologies will be developed on an as-needed basis.

The CEO should oversee the completion of all testing procedures detailed below, as required based on the schedule described above.

CUSA Annual Plan Review

From the CUSA website: Periodically, the **CUSA Technologies'** disaster recovery team will perform a test of the processes upon under your recovery agreement. This test includes confirming the readability of your tapes with other optional procedures to better assure system communication between your credit union and **CUSA**. At this time, we also review your recovery agreement to assure the agreement meets your credit union's needs during an emergency. The plan can be amended at this time to include new modules and credit union growth. The scope of the annual review is dependent on the service level selected.

Further information on **CUSA's** DR testing procedures/annual review is detailed at the following address: <http://www.cusa.com/pubpages.nsf/5af9661752bc2b8387256d1a005481d9/d1539ba6af58168987256d19005d3b37!OpenDocument>

RP10-CUSADisasterRecovery.doc (Recovery Procedures) details the actual procedure to be used in the event of an emergency.

CUSA DR-Hot-site Testing

The following (adopted from the **CUSA** website) details the procedure to be followed in order to test the institution's ability to restore **CUSA** systems at the hot-site accurately and effectively.

1. The institution should ship test backup tape to **CUSA** headquarters (**Salt Lake City, UT**).
2. **CUSA** should ship agreed upon equipment to the hot-site/temporary operating location.
3. Once the backup tapes are received, **CUSA** should load the backup on a hot-site server at its headquarters.
4. A dial-up line should be connected to allow the institution to access its system data (via modem) from full tape backups in order to perform daily activities remotely.
5. The institution should run test scripts/transactions to validate the accuracy of transactions.
6. The institution should document and work to resolve any problems encountered.
7. The institution should print and save verification screens to document the successful completion of each test transaction.
8. Once all transactions are successfully completed, **CUSA** should supply the institution with a certificate documenting the successful completion of the DR test.