IBM i / 7.3 / Change version

Feedback Product list

Section 11. Testing the disaster recovery plan

Last Updated: 2021-08-02

In successful contingency planning, it is important to test and evaluate the plan regularly.

Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document.

Table 1 should be helpful for conducting a recovery test.

Table 1. Checklist for testing the disaster recovery plan

Item	Yes	No	Applicable	Not applicable	Comments
Conducting a Recovery Test					

Item	Yes	No	Applicable	Not applicable	Comments
1. Select the purpose of the test. What aspects of the plan are being evaluated? 2. Describe the objectives of the test. How will you measure successful achievement of the objectives? 3. Meet with management and explain the test and objectives. Gain their agreement and support. 4. Have management announce the test and the expected completion time. 5. Collect test results at the end of the test period. 6. Evaluate results. Was recovery successful? Why or why not? 7. Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period? 8. Make suggestions for changes. Call for responses by a given date. 9. Notify other areas of results. Include users and auditors. 10. Change the disaster recovery plan manual as necessary.					

Item	Yes	No	Applicable	Not applicable	Comments
Areas to be tested					
1. Recovery of individual application systems by using files and documentation stored off-site. 2. Reloading of system save media and performing an initial program load (IPL) by using files and documentation stored off-site. 3. Ability to process on a different computer. 4. Ability of management to determine priority of systems with limited processing. 5. Ability to recover and process successfully without key people. 6. Ability of the plan to clarify areas of responsibility and the chain of command. 7. Effectiveness of security measures and security bypass procedures during the recovery period. 8. Ability to accomplish emergency evacuation and basic first-aid responses. 9. Ability of users of real time systems to cope with a temporary loss of online information. 10. Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical. 11. Ability to contact the key people or their designated alternates quickly.					

Item	Yes	No	Applicable	Not applicable	Comments
12. Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media. 13. Availability of peripheral equipment and processing, such as printers and scanners. 14. Availability of support equipment, such as air conditioners and dehumidifiers. 15. Availability of support: supplies, transportation, communication. 16. Distribution of output produced at the recovery site. 17. Availability of important forms and paper stock. 18. Ability to adapt plan to lesser disasters.					

Parent topic:

→ Example: Disaster recovery plan