DR Risk and Recovery Time Objective (RTO) Analysis

Customer Procedure

Primary Point of Contact: Mike Lowry

Overview:

The Information Security Office processes DR Risk and Recovery Time Objective (RTO) Analysis to capture DR information, provide realistic RTO expectations, and to provide the foundation for DR and risk mitigation discussions.

Customer Procedure:

1) Requester will be provided with a form to capture basic DR information for the system to be analyzed. Required information consists of:
   a. Priority/Criticality (High/Med/Low)
   b. Application Name
   c. Application Support Personnel
   d. Application Dependencies
   e. What is the application used for?
   f. Outage Impact?
   g. Hardware Platforms
   h. Hardware Support Personnel
   i. Operating System
   j. Database Architecture
   k. Local Storage required
   l. External Storage (SAN) required
   m. Host Name
   n. DNS Name
   o. TSM Node Name
   p. Network Address

   Note: ISO personnel will facilitate filling out this form if there are requirements that are not available to the requester.

2) Following completion of analysis, a meeting may be set up with the requester to discuss DR and RTO status for their system, potential business continuity needs based on anticipated recovery timelines, and any identified options for more responsive DR and/or risk mitigation. Whether a meeting is deemed necessary or not, a written response will be provided.
Measure of Completion:

DR Risk and Recovery Time Objective (RTO) Analysis will be considered complete when a written response has been prepared and either a meeting has been set or the response has been delivered.