Computing Sector has created an overall IT Service Continuity Management Plan that covers the key areas that each individual plan would rely upon in a continuity situation such as command center information, vital records, personnel information. The purpose of this document is to describe the key information needed to recover this service in a business continuity situation once a decision to invoke has been made, and then to manage the business return to normal operation once the service disruption has been resolved.

Scope
Service Area: Backup and Restore Service

Sub-service: Desktop Backup Service

Service Offerings:

The backup and restore service is intended to be used to backup system information (OS) and user areas located on network storage devices. The desktop backup service provides the infrastructure services for user-driven backup and restore of user data on desktops and laptops.

Service Areas that depend on this service:

All service areas listed in the Backup and Restore Service OLA.

Recovery Objectives

Recovery Time Objective (RTO)

< 12 hrs.

*RTO is defined as the length of time processes could be unavailable before the downtime adversely impacts business operations.*

Recovery Point Objective (RPO)

< 24 hrs.

*RPO is defined as the maximum interval of data loss since the last backup that can be tolerated and still resume the business process.*

Recovery Team

In this section describe the other services, roles, and responsibly required for recovering this service.

<table>
<thead>
<tr>
<th>Service/Role/Function</th>
<th>Responsibility</th>
<th>Dependencies</th>
<th>Expected Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities Operations</td>
<td>Service Owner</td>
<td>Data center, power, environment</td>
<td>Reference OLA DocDB 4594</td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## IT Service Continuity Plan – Backup and Restore Service

<table>
<thead>
<tr>
<th>Service</th>
<th>Service Owner</th>
<th>Network/Storage cabling</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Services</td>
<td></td>
<td>Network/Storage cabling</td>
<td>SLA DocDB 4312</td>
</tr>
<tr>
<td>Networked Storage Services</td>
<td>Service Owner</td>
<td>SAN/NAS Storage Facilities required to run VM’s</td>
<td>SLA DocDB 4311</td>
</tr>
<tr>
<td>Authentication Services</td>
<td>Service Owner</td>
<td>Preferred availability to allow multiple system admins to login to servers and add virtual file servers to Active Directory if necessary.</td>
<td>OLA DocDB 4314</td>
</tr>
<tr>
<td>IT Server Hosting Services</td>
<td>Service Owner</td>
<td>Support for Backup Servers (if needed)</td>
<td>OLA DocDB 4316</td>
</tr>
<tr>
<td>Backup and Restore Services</td>
<td>Service Owner</td>
<td>Coordinate with other service owners and drive recovery operation</td>
<td>OLA DocDB 4315</td>
</tr>
<tr>
<td>External Service Provider (only if needed)</td>
<td>Works with Backup and Restore Services</td>
<td>TiBS, EMC, CrashPlan, HDS, SpectraLogic, ExaGrid</td>
<td>Contracts for production systems &lt; 4 hrs.</td>
</tr>
</tbody>
</table>
Recovery Strategy

Because of the high cost of equipment, lack of space, licensing costs, and complexity of supporting redundant site backup infrastructures, site backups rely on FCC2 being available. The financial and business systems backups rely on both the FCC2 datacenter and LCC datacenter being available. Critical financial data is stored offsite (Iron Mountain) in the event that resources at Fermilab are unavailable. A loss of the FCC2 datacenter would mean a loss of all backup and restore services, including the desktop backups.

Backup and Restore High-Level Recovery Strategy

1. Verify underlying infrastructure is available. This includes facilities (power/cooling), networking (DNS, firewalls, routers, switches), SAN Storage (backup cache area), and authentication services.
2. Restore site backup environment (Spectra T950, Nexsan, chasm, canyon, finbak, Exagrid appliances, MSL4048, HDS disk cache)
3. Verify environment readiness:
   a. Login to chasm, canyon, and finbak backup servers and check system health of backup servers
   b. Test connectivity to tape/storage devices used for backup targets (i.e. T950, Nexsan array, Exagrid appliances, MSL4048).
   c. Perform confidence tests (i.e. backup/restore several files or folders) after startup and initial checks of devices has completed
4. Communicate system availability to customers

Desktop Backup High-Level Recovery Strategy

1. Verify underlying infrastructure is available. This includes facilities (power/cooling), networking (DNS, firewalls, routers, switches), SAN Storage (backup cache area), Virtual Services, and authentication services.
2. Restore arrays (used as store points), CrashPlan storage servers, and management server.
3. Verify environment readiness:
   b. Check the Destination Overview screen to verify store points are available:

<table>
<thead>
<tr>
<th>Destination Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>Ravine T950 Server</td>
</tr>
<tr>
<td>Vauln 48T</td>
</tr>
<tr>
<td>Vauln 313</td>
</tr>
</tbody>
</table>

c. Perform confidence tests (i.e. backup/restore several files or folders) from a CrashPlan client device.
4. Communicate system availability to customers if necessary. The Desktop Backup Service is generally meant to be something that happens in the background, so customer communication is expected to be minimal.
Strategy for initial recovery
Assess infrastructure readiness for Backup and Restore resources and review situation with recovery team.

Overall recovery strategy
- If the FCC2 datacenter is out of service, all backup and restore services will be unavailable.
- If the LCC datacenter is out of service, backup and restore services for the financial systems will be unavailable. The primary site backup system running in FCC2 has no dependency on the LCC computer room.
- If all of FCC is lost, build primary site backup system from scratch.
- If the LCC datacenter is lost, build financial systems backup infrastructure from scratch.

Recovery Scenarios
Please provide high-level checklist or plan for each recovery scenario. If you have additional recovery scenarios that need to be accounted for because they require different procedures, please document them here. If all the scenarios require the same response, then you can state that in this section then outline the plan.

For the checklist/plan please use a list or table format to make this easy to pick up and use in a continuity situation. Include links or references and location of actual recovery detailed procedures. Document any key dependencies and command center reporting checkpoints.

Building not accessible (Data Center Available)
Document checklist/plan
- Verify Site VPN is available for remote administration.
- Verify private/management networks are available for backup and restore service administration
- Refer to the “Backup and Restore High Level Recovery”

Data Center Failure (Building Accessible)
Document checklist/plan
- Refer to the “Backup and Restore High-Level Recovery Strategy” steps on the previous page.
- Refer to the “Desktop Backup High-Level Recovery Strategy” steps on the previous page.

Building not accessible and Data Center Failure
Document checklist/plan
- No alternative datacenter recovery sites have been defined. If just one datacenter (FCC2 or FCC3) has failed, refer to the “Overall recovery strategy” steps on previous page, then execute the startup
Critical recovery team not available

Document checklist/plan

Call vendor depending on type of assistance needed (found in Backup and Restore Service OLA):

- Sun/Oracle Maintenance contract for Backup Servers
- Nexsan maintenance contract for disk cache
- HDS maintenance contract for DB disk resources and disk cache
- BlueArc maintenance contract for NDMP server
- TiBS software maintenance contract for TiBS backup software
- SpectraLogic maintenance contract for SpectraLogic tape library
- Exagrid maintenance contract for Exagrid backup appliances
- CrashPlan maintenance contract for CrashPlan software

Failed storage array for Desktop Backup

Document checklist/plan

- Re-generate from remaining storage server, including all backup history and device information.
  Note: Client backups and restores can still occur with just one storage server and no visible impact to customers
- Check CrashPlan management console under Destination Overview to verify both storage servers and all storage is available
- Test backup and restore from specific storage server utilizing the recovered storage array

Return to Operations

1. Recover environment (Tape Libraries, Dedupe appliances, backup servers, arrays) to previous state/capabilities (follow startup/shutdown procedures)
2. Restore data (if necessary)
3. Run confidence tests prior to release of environment to customers
   a. Test backup job
   b. Test restore job
## Document Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author(s)</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>8-15-2012</td>
<td>Mike Rosier</td>
<td>Initial Document</td>
</tr>
<tr>
<td>1.1</td>
<td>10-23-2013</td>
<td>Mike Rosier</td>
<td>2013 yearly review</td>
</tr>
<tr>
<td>1.2</td>
<td>10-29-2014</td>
<td>Mike Rosier</td>
<td>2014 yearly review</td>
</tr>
<tr>
<td>2.0</td>
<td>10/16/2015</td>
<td>R. Ramos</td>
<td>Annual Review by Service Continuity Manager</td>
</tr>
</tbody>
</table>