COMPANY

Disaster Recovery Plan (DRP) for [*PRODUCT*]

(Note: this DRP document is somewhat specific to SharePoint, but can be adapted for other products/technologies as needed)

Plan and related Business Processes

Business Process	Feature	Relevant Technical Components
		•

December 29, 2014

Table of Contents

1. Purpose and Objective

COMPANY developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the features listed in the table above. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope

The scope of this DRP document addresses technical recovery only in the event of a significant disruption. The intent of the DRP is to be used in conjunction with the business continuity plan (BCP) COMPANY has. A DRP is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan and/or the Corporate Incident Response and Incident Management plans COMPANY has in place.

The link to the specific BCP document related to this DRP can be found here: **LINK TO BCP**

This disaster recovery plan provides:

- Guidelines for **determining plan activation**;
- Technical **response flow** and recovery strategy;
- Guidelines for **recovery procedures**;
- References to key **Business Resumption Plans** and technical dependencies;
- **Rollback procedures** that will be implemented to return to standard operating state;
- **Checklists** outlining considerations for escalation, incident management, and plan activation.

The specific objectives of this disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside COMPANY. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

2. Dependencies

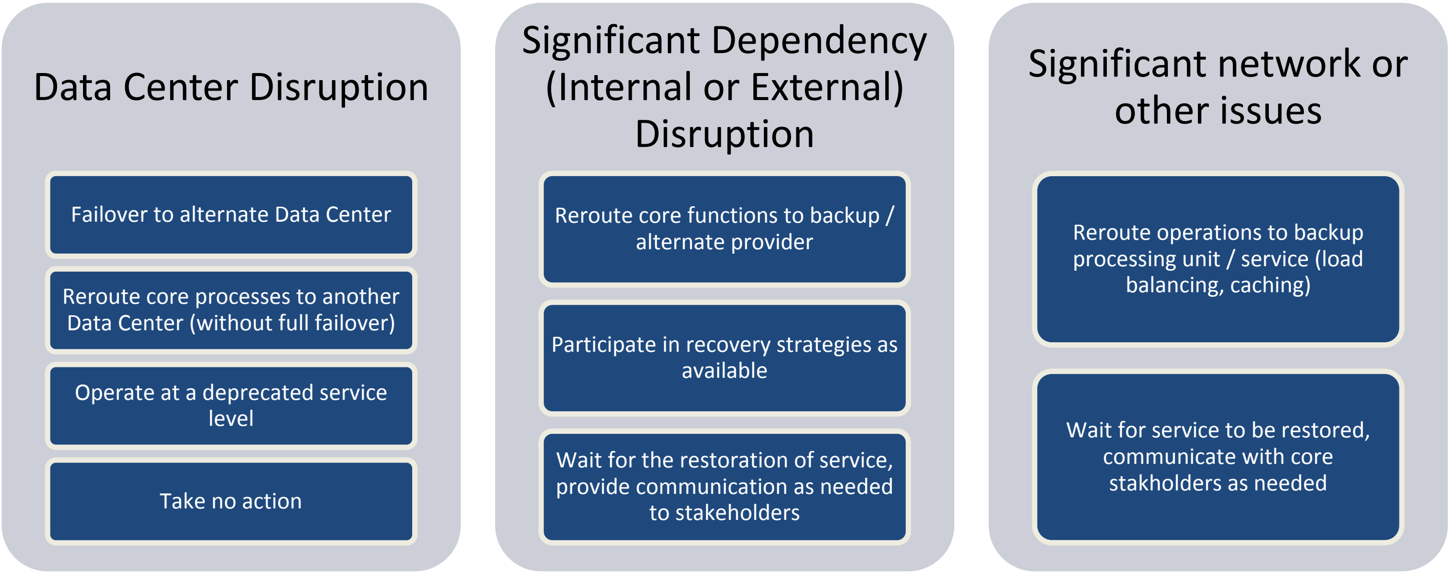
This section outlines the dependencies made during the development of this SharePoint disaster recovery plan. If and when needed the DR TEAM will coordinate with their partner groups as needed to enable recovery.

Dependency	Assumptions
User Interface / Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application). • Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence / Reporting Processing components	• The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). • Standard backup processes (e.g. tape backups) are not impacted, but the active / passive or mirrored processes are not functioning. • Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	• Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. • Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	• Loss of SAN, local area storage, or other storage component.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable
Hardware/Host Layer Hardware components	• Physical components are unavailable or affected by a given event
Virtualizations (VM's) Virtual Layer	• Virtual components are unavailable • Hardware and hosting services are accessible
Administration Infrastructure Layer	• Support functions are disabled such as management services, backup services, and log transfer functions. • Other services are presumed functional
Internal/External Dependencies	• Interfaces and intersystem communications corrupt or compromised

In addition assumptions within the Business Continuity Plan for this work stream still apply.

3. Disaster Recovery Strategies

The overall DR strategy of xyz is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, reporting, etc.)



Data Center Disruption

- Failover to alternate Data Center
- Reroute core processes to another Data Center (without full failover)
- Operate at a deprecated service level
- Take no action

Significant Dependency (Internal or External) Disruption

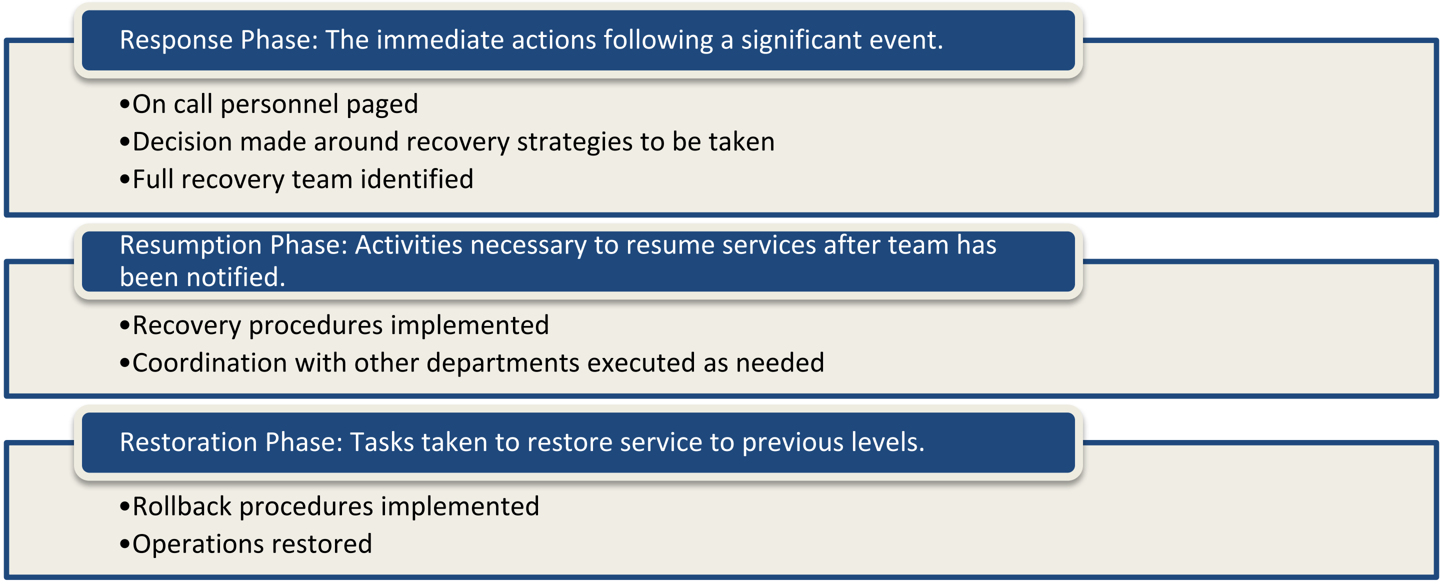
- Reroute core functions to backup / alternate provider
- Participate in recovery strategies as available
- Wait for the restoration of service, provide communication as needed to stakeholders

Significant network or other issues

- Reroute operations to backup processing unit / service (load balancing, caching)
- Wait for service to be restored, communicate with core stakeholders as needed

4. Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.



Response Phase: The immediate actions following a significant event.

- On call personnel paged
- Decision made around recovery strategies to be taken
- Full recovery team identified

Resumption Phase: Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

Restoration Phase: Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

Response Phase

The following are the activities, parties and items necessary for a DR response in this phase. Please note these procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario).

Response Phase Recovery Procedures – All DR Event Scenarios

Step	Owner	Duration	Components
Identify issue, page on call / Designated Responsible Individual (DR TEAM)	DR TEAM	x minutes	• Issue communicated / escalated • Priority set
Identify the team members needed for recovery	DR TEAM	x minutes	Selection of core team members required for restoration phase from among the following groups: • Operations •
Establish a conference line for a bridge call to coordinate next steps	DR TEAM or Ops	x minutes	Primary bridge line: **NUMBER** Secondary bridge line: **NUMBER** Alternate / backup communication tools: email, communicator
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	DR TEAM	x minutes	• Documentation / tracking of timelines and next decisions • Creation of disaster recovery event command center / “war room” as needed

This information is also summarized by feature in Appendix A: Disaster Recovery Contacts - Admin Contact List.

Resumption Phase

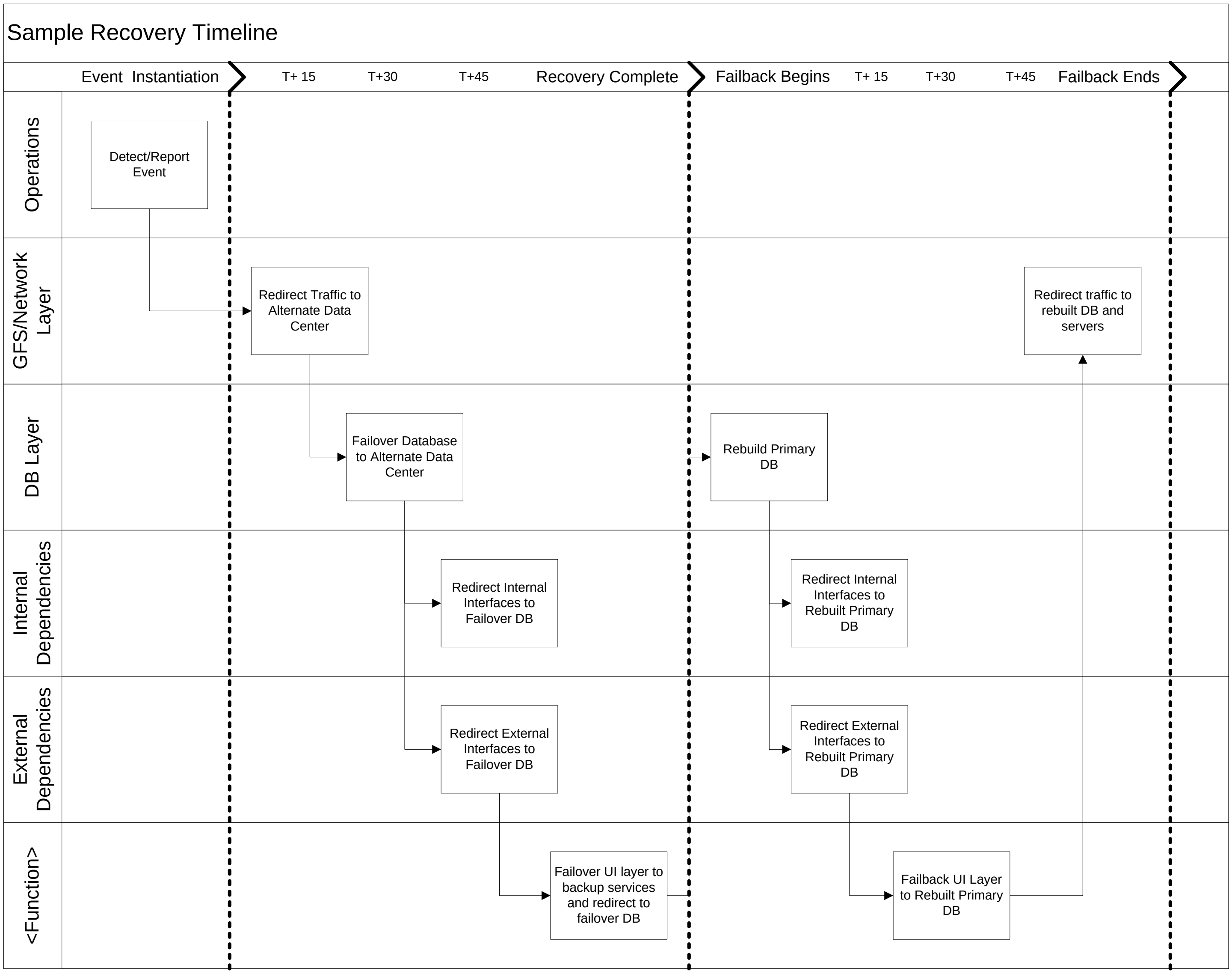
During the resumption phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Data Center Recovery

Full Data Center Failover

Step	Owner	Duration	Components
Initiate Failover	DR TEAM	TBD	• Restoration procedures identified • Risks assessed for each procedure • Coordination points between groups defined • Issue communication process and triage efforts established
Complete Failover	DR TEAM	TBD	• Recovery steps executed, including handoffs between key dependencies
Test Recovery	DR TEAM	TBD	• Tests assigned and performed • Results summarized and communicated to group
Failover deemed successful	DR TEAM	TBD	•

Below is a sample timeline for recovery actions associated with the failover the technical components between different data centers to provide geo-redundant operations. Coordination of recovery actions is crucial. A timeline is necessary in order to manage recovery between different groups and layers.


Sample Recovery Timeline
Event Instantiation
T+ 15
T+30
T+45
Recovery Complete
Failback Begins
T+ 15
T+30
T+45
Failback Ends
Operations
GFS/Network Layer
DB Layer
Internal Dependencies
External Dependencies
<Function>
Detect/Report Event
Redirect Traffic to Alternate Data Center
Failover Database to Alternate Data Center
Redirect Internal Interfaces to Failover DB
Redirect External Interfaces to Failover DB
Failover UI layer to backup services and redirect to failover DB
Rebuild Primary DB
Redirect Internal Interfaces to Rebuild Primary DB
Redirect External Interfaces to Rebuild Primary DB
Failback UI Layer to Rebuild Primary DB
Redirect traffic to rebuild DB and servers

Reroute critical processes to alternate Data Center

Step	Owner	Duration	Components
			●
			●

Operate at deprecated service level – prioritize critical feeds

Step	Owner	Duration	Components
			●
			●

Take no action – monitor for Data Center recovery

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the Data Center is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	•
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	

Internal or External Dependency Recovery

Reroute operations to backup provider

Step	Owner	Duration	Components
			•
			•

Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies	DR TEAM	As needed	
	DR TEAM	As needed	•

Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	• Provide feedback about SharePoint service availability
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	

Significant Network or Other Issue Recovery (Defined by quality of service guidelines)

Reroute operations to backup provider

Step	Owner	Duration	Components
			•
			•

Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies	DR TEAM	As needed	• Hardware (CPU, Memory, Hard disk, Network requirements) •
teams	DR TEAM	As needed	
	DR TEAM	As needed	•

Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	• Provide feedback about SharePoint service availability
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	

Restoration Phase

During the restoration phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Data Center Recovery

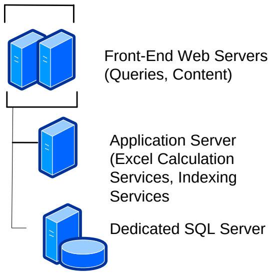
Full Data Center Restoration

Step	Owner	Duration	Components
Determine whether failback to original Data Center will be pursued	DR TEAM	TBD	• Restoration procedures determined
Original data center restored	DR TEAM	TBD	• Server Farm level recovery
Complete Failback	DR Team	TBD	• Failback steps executed, including handoffs between key dependencies
Test Failback	DR Team	TBD	• Tests assigned and performed • Results summarized and communicated to group • Issues (if any) communicated to group
Determine whether failback was successful	DR TEAM	TBD	• Declaration of successful failback and communication to stakeholder group. • Disaster recovery procedures closed. • Results summarized, post mortem performed, and DRP updated (as needed).

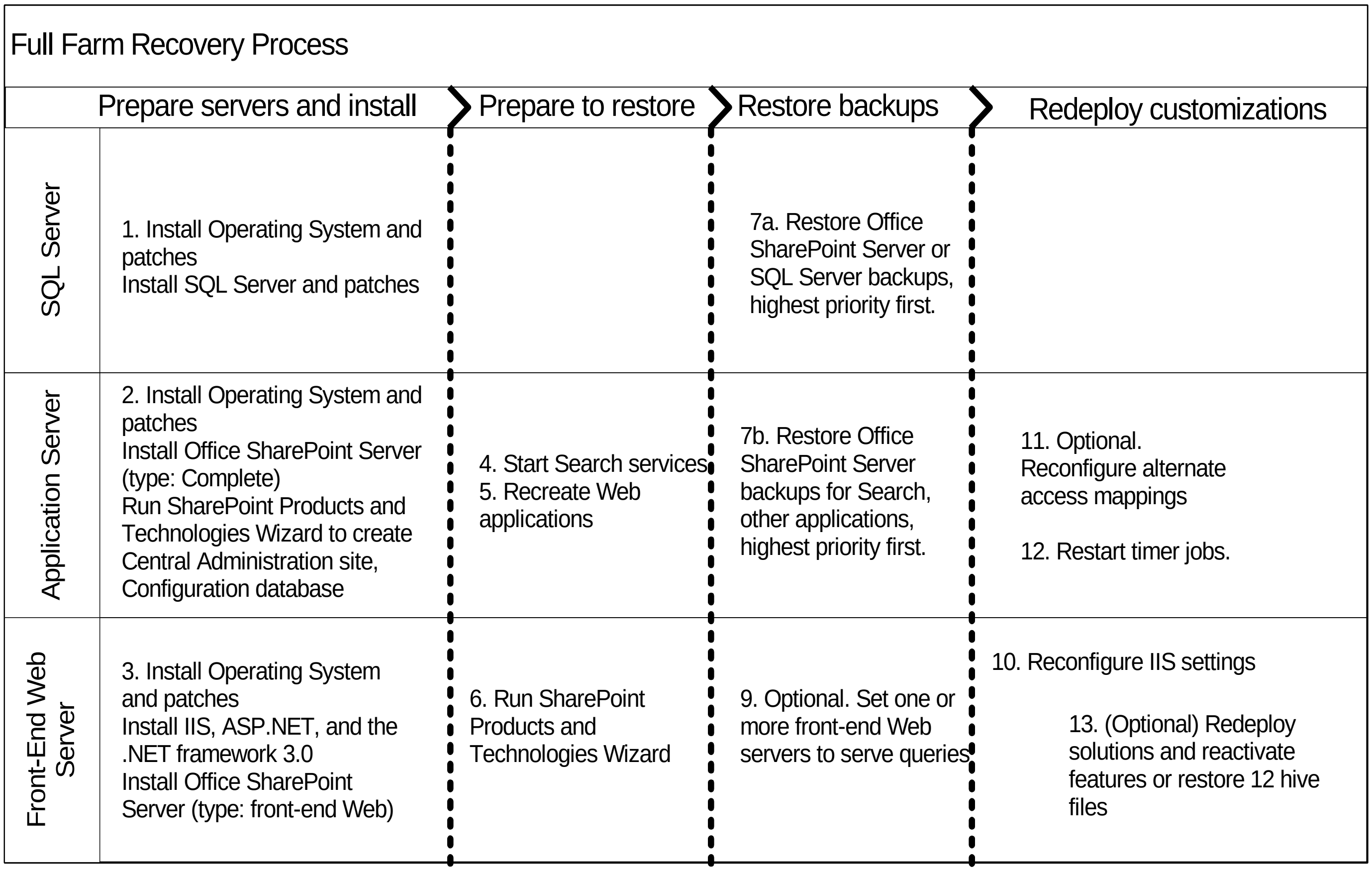
The following section contains steps for the restoration procedures.

Full Server Farm Recovery

This section describes the process for recovering from a farm-level failure, for a: three-tier server farm consisting of a *database server*, an *application server* that provides Index, Query, InfoPath Forms Services and Excel Calculation Services, and *two front-end Web servers* that service search queries and provide Web content.



The following diagram describes the recovery process for a farm.



Full Farm Recovery Process

	Prepare servers and install	Prepare to restore	Restore backups	Redeploy customizations
SQL Server	1. Install Operating System and patches Install SQL Server and patches		7a. Restore Office SharePoint Server or SQL Server backups, highest priority first.	
Application Server	2. Install Operating System and patches Install Office SharePoint Server (type: Complete) Run SharePoint Products and Technologies Wizard to create Central Administration site, Configuration database	4. Start Search services 5. Recreate Web applications	7b. Restore Office SharePoint Server backups for Search, other applications, highest priority first.	11. Optional. Reconfigure alternate access mappings 12. Restart timer jobs.
Front-End Web Server	3. Install Operating System and patches Install IIS, ASP.NET, and the .NET framework 3.0 Install Office SharePoint Server (type: front-end Web)	6. Run SharePoint Products and Technologies Wizard	9. Optional. Set one or more front-end Web servers to serve queries	10. Reconfigure IIS settings 13. (Optional) Redeploy solutions and reactivate features or restore 12 hive files

Overview of a farm-level recovery

Add Farm restore steps

Internal or External Dependency Recovery

Execute available recovery procedures

Step	Owner	Duration	Components
	DR TEAM	As needed	•
	DR TEAM	As needed	

Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	• Provide feedback about SharePoint service availability
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	

Significant Network or Other Issue Recovery (Defined by quality of service guidelines)

Execute available recovery procedures

Step	Owner	Duration	Components
	DR TEAM	As needed	•

Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	•
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	

Appendix A: Disaster Recovery Contacts - Admin Contact List

The **critical team members** who would be involved in recovery procedures for feature sets are summarized below.

Feature Name	Contact Lists

For the key internal and external dependencies identified, the following are the primary contacts.

Dependency Name	Contact Information

In addition the key BCP individuals are:

-

Appendix B: Document Maintenance Responsibilities and Revision History

This section identifies the individuals and their roles and responsibilities for maintaining this Disaster Recovery Plan.

Primary Disaster Recovery Plan document owner is:
Primary Designee:

Alternate Designee: [**NAME**]

Name of Person Updating Document	Date	Update Description	Version #	Approved By

Appendix C: Server Farm Details

Farm Configuration (status as of date)

Table

Appendix D: Glossary/Terms

Standard Operating State: Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

Presentation Layer: Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed and system requests are passed for processing and data retrieval to the appropriate layer.

Processing Layer: System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically this layer processes data from the other layers. Typically these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

Database Layer: The database layer is where data typically resides in an application stack. Typically data is stored in a relational database such as SQL Server, Microsoft Access, or Oracle, but it can be stored as XML, raw data, or tables. This layer typically is optimized for data querying, processing and retrieval.

Network Layer: The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

Storage Layer: This is typically an infrastructure layer and provides data storage and access. In most environments this is usually regarded as SAN or NAS storage.

Hardware/Host Layer: This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

Virtualization Layer: In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

Administrative Layer: The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.