CoBro Consulting, LLC

Disaster Recovery Plan (DRP)

Business Process	Feature	Relevant Technical Components
Disaster Recovery Plan	*Compass*	*Web and Database Tiers*

January 1, 2019
Version 1.0

Table of Contents

1. Purpose and Objective

CoBro Consulting, LLC (CoBro Consulting) developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the Compass System. 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 addresses technical recovery only in the event of a significant disruption.

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, CoBro Consulting. This plan is designed to identify the steps CoBro Consulting is 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

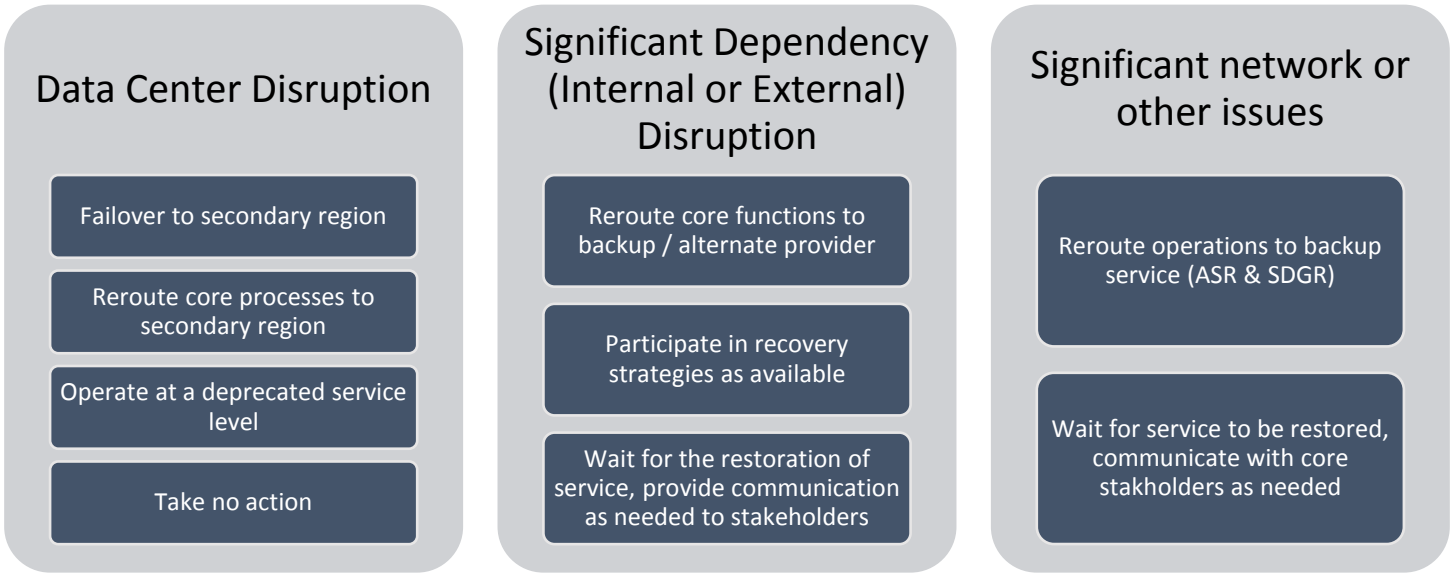
This section outlines the dependencies made during the development of this **Compass** application disaster recovery DRP. If, and when, needed, the disaster recovery (DR) TEAM will coordinate with their partner groups to enable recovery.

Dependency	Assumptions
User Interface / Rendering Presentation components	• Users (end users, power users, administrators) are unable to access the primary system through any part of the primary instance (e.g., web interface or server side in the primary region). • Azure infrastructure and back-end services are still assumed to be active/running on other regions. • Standard recovery processes (e.g., Azure Site Recovery (ASR)) are not impacted and the passive instances are assumed to be functioning.
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). • Specific types of disruptions could include components that process, match, and transform, 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. • Azure Service Health (ASH) indicates service issues with the affected region.
Storage Layer Infrastructure components	• Loss of Azure Storage component. • Azure Service Health (ASH) indicates service issues with the affected region.
Database Layer Database storage components	• Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable. • Standard backup and redundancy processes (e.g., SQL Database Backup (SDB) and SQL Database Geo-Replication (SDGR) respectively) are not impacted and the active or mirrored processes are assumed to be functioning.
Host Layer Hardware components	• Host layer components are unavailable or affected by a given event. • Azure Service Health (ASH) indicates service issues with the affected region.
Virtualizations (VMs) Virtual Layer	• Virtual components are unavailable. • Hardware and hosting services are still 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 CoBro Consulting 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.)



4. Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration.

Response Phase: The immediate actions following a significant event.

- On call personnel notified
- 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	15 minutes	• Issue communicated / escalated • Priority set
Identify the team members needed for recovery.	DR Team	15 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	10 minutes	Primary bridge line: **<Zoom Conference Info>** Secondary bridge line: **<Google Suite>** Alternate / backup communication tools: email, communicator
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	DR Team	20 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	• Validate traffic on the failover region

Below is a sample timeline for recovery actions associated with the failover of 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.

Reroute critical processes to alternate Data Center

Step	Owner	Duration	Components
Initiate Failover on both Web and Database Tiers to their respective Secondary Region	DR Team	TBD	• Azure Site Recovery

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	Hourly as needed	
Send out frequent updates to core stakeholders with the status.	DR Team	Hourly as needed	

External Dependency Recovery

Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies	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	
Send out frequent updates to core stakeholders with the status.	DR Team	Hourly as needed	

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

Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies	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	Hourly 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

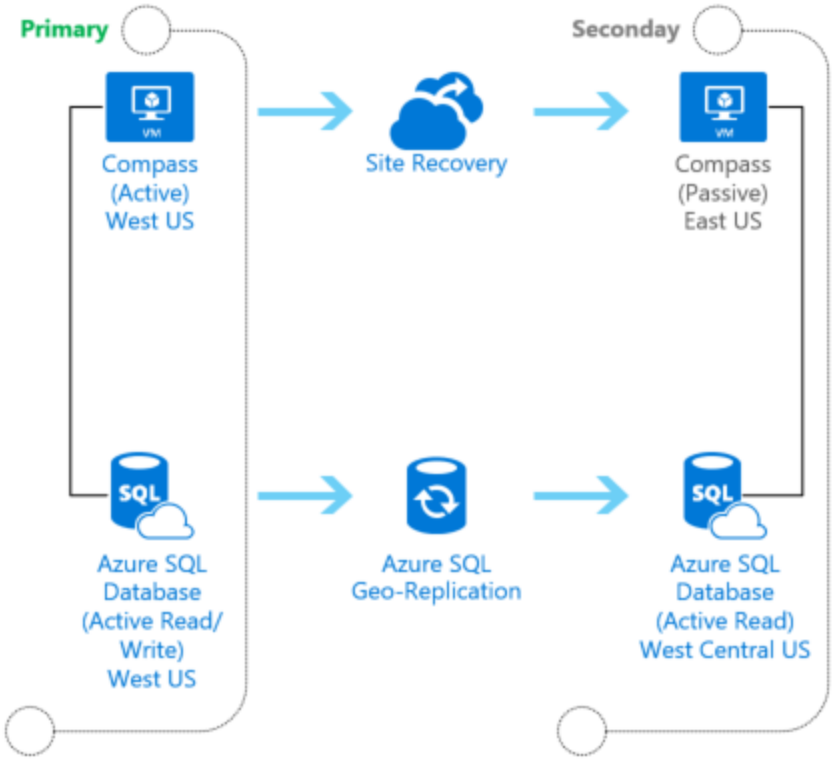
Full Data Center Restoration

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	• Primary region 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.

Azure Region Recovery

This section describes the process for recovering from a data center (Azure Region) failure, for a two-tier application architecture consisting of a *database tier* and a *web server tier* that serves the Compass web content.



External Dependency Recovery

Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event that no other options were available to the DR Team (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	
Send out frequent updates to core stakeholders with the status.	DR TEAM	Hourly as needed	

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

Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies	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 the DR Team (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	Hourly 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
Business Communication	Darlene Cole and Urban Pelicon
Cloud Administrator	Del Esposo
Application Administrator	Andy Hong

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

Dependency Name	Contact Information

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: Darlene Cole, CEO

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

Appendix C: Component Details

Compass Configuration (status as of January 1, 2019)

Webserver: Virtual Machine with Windows Server 2012, and IIS 8, Infrastructure as a service

Database: Azure SQL, Platform as a service

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.