Disaster Recovery Plan

Migration and DR Setup for Manufacturing Company project

Project Team

Dina Khaled Mohamed

Omnia Mahmoud Abdell-Rahman

Hanan Ahmed El-Sobky

Instructor

Eng/ Omar Sameh

Senior Cloud Engineer-Global Brands Group (GBG) Company

Date

11 July 2025

TABLE OF CONTENTS

1) Introduction

The Disaster Recovery (DR) Runbook provides a comprehensive plan for maintaining business continuity for the ERP system of a manufacturing company. The company is migrated its ERP workloads from an on-premises environment to Microsoft Azure and requires a fully functional Disaster Recovery setup using an Active/Passive model via Azure Site Recovery (ASR).

1.1) Objectives

- Ensure rapid recovery of ERP system Components in case of outages.
- Define clear procedures for failover and failback operations.
- Minimize Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as possible.
- Provide a structured and tested response plan for business continuity.
- Enable secure remote access via VPN P2S during disasters.
- Ensure replication of critical systems to the DR region using ASR.

1.2) Scope of Disaster Recovery Plan

This Disaster Recovery Plan defines the systems and services that are included in the scope of disaster protection, as well as the boundaries of responsibility for the DR team.

The plan covers only critical workloads hosted on Microsoft Azure that are part of the ERP system and its supporting infrastructure. The Disaster Recovery team is responsible for managing the protection and recovery of these components in case of service interruption or regional failure.

1.2.1) In Scope

- ERP Application Servers (IIS) hosted on Azure VMs.
- Azure SQL Database for ERP.
- On-premises SQL Server integrated via Azure Arc.
- Structured and Unstructured File Servers.
- Azure Load Balancer.
- Azure Front Door for global routing.
- VPN Point-to-Site (P2S) for remote access.
- Azure Landing Zone: VNets, Subnets, NSGs, Route Tables.
- Monitoring Tools: Azure Monitor and Log Analytics.
- Azure Firewall.
- Recovery Service Vault hosted in the primary region.

1.2.2) Out of Scope

- On-premises infrastructure and hardware not integrated with Azure.
- End-users devices such as desktops and Laptops.
- Third-Party Cloud Provider and Services such as (AWS, GCP).
- External SaaS application not hosted within the Azure environment.
- Internal helpdesk or ticketing systems.

2) Infrastructure Environment

2.1) Primary Site Architecture

The production environment is hosted in Microsoft Azure within the West Europe region, the primary site includes:

- Azure SQL Database (PaaS).
- On-premises SQL Server (via Azure Arc).
- ERP Application Server (IIS) hosted on Azure VMs.
- File Servers (Structures and unstructured data) implemented using Azure File Shares hosted in Storage Account and mounted to Azure VM.
- Azure Load Balancer for backend load distribution.
- Azure Front Door for public access and global routing.
- VPN Gateway (point-to-site) for secure remote connectivity.

- Azure Firewall.
- Azure Landing Zone: VNets, Subnets, Route Tables, and NSGs.
- Azure Monitor and Log Analytics.
- Recovery Services Vault for replication configuration and DR control.

2.1) DR Site Architecture

The disaster recovery site is hosted in the North Europe Azure region. The DR Environment includes:

- Replicated ERP Application Servers (IIS).
- Azure SQL Geo-redundant Database.
- SQL Server VM (via Azure Arc).
- Replicated File Share.
- Azure Landing Zone.
- Load Balancer.
- Azure Front Door.
- VPN Gateway (point-to-site).
- Azure Firewall.
- Azure Monitor and Log Analytics.

3) Disaster Recovery Team and Role

A clearly defined disaster recovery team ensures fast and effective response during a disaster or major outage. The team includes representatives from infrastructure, application, database, and security teams. Each member has a specific role to ensure proper coordination and execution of the recovery plan.

Role	Responsibility
DR Coordinator / Team Lead	Oversees the entire DR process, initiates the failover, and communicates status with stakeholders
Azure Infrastructure Engineer	Executes the failover process in Azure, ensures VMs and services come up correctly
Application Support Engineer	Validates ERP application functionality after failover
Database Administrator (DBA)	Ensures SQL database connectivity and consistency during and after failover
Network & Security Engineer	Validates connectivity (VPN, Front Door), ensures NSGs/firewall rules are applied
Monitoring & Logging Specialist	Monitors system performance and collects logs during the DR event
Compliance/Backup Specialist	Ensures backup availability, verifies retention and compliance policies

4)Disaster Types and Severity Level

Classification of disaster types that may affect the ERP system and related services. Disasters are grouped as planned or unplanned and given a severity level from 1 to 3. This helps decide the right response, priority, and how to perform failover.

Disaster Type	Severity Level	Description	Example	Action Required
Planned	N/A	Pre-scheduled event for testing or maintenance	DR test failover of ERP system	Controlled failover and no business impact
Unplanned	Level 1	Minor/local issue affecting a single component	One App server VM crash	Restart VM or restore from backup
Unplanned	Level 2	Major issue affecting multiple workloads	File Share & SQL Database degraded	Partial Failover or notify DR team
Unplanned	Level 3	Full disaster causing complete outage in primary site	Full Azure region un - available	Full DR failover to secondary Site

5) RTOs and RPOs

- RTO (Recovery Time Objective): The maximum acceptable time a system or service can be down after a disaster before it must be restored.
- RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time. It defines how much data can be lost before affecting business operations.

This table describes the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the critical services in the ERP system.

Service	RTO	RPO
SQL Server (Cloud & Arc)	30 minutes	15 minutes
ERP Application Servers	1 hour	30 minutes
File Servers (structure)	1 hour	30 minutes
File Servers (Unstructured)	2 hours	1 hour
Azure Front Door	30 minutes	15 minutes
VPN Gateway (P2S)	2 hours	1 hour
Azure Monitor	4 hours	2 hours

Hint:

in the event of a failover, Azure Firewall must be reconfigured or redeployed within 1 hour to maintain the same level of network protection. As the firewall does not store user data, RPO is not applicable.

6) Failover Environment

The failover environment is hosted in the North Europe Azure region and is designed to support the ERP system in case of a disaster affecting the primary site. The environment includes all critical components required to maintain business continuity and user access during failover.

Service	Details
ERP Application Servers (IIS)	Replicated VMs with latest status using Azure Site Recovery (ASR)
SQL Server	Geo-replicated Azure SQL + VM with Arc-enabled SQL Server
File Servers	Replicated Structured & unstructured shares via storage account and mount
Azure Front Door	Configured for global routing, switched to DR backends on failover
Load Balancer	DR Load Balancer configured for new backend pool
VPN Gateway (P2S)	DR VPN deployed for secure admin access
Azure Firewall	Replicated rules applied to secure DR environment
Azure Monitor	Activated for diagnostics and alerts in DR

7) Failover Procedure

In case of a disaster, the following steps must be followed to initiate the failover process and shift operations to the DR site.

1- Declare the disaster and get internal approval to start the DR process.
2- Access Azure Site Recovery Vault in the DR region.
3- Trigger failover for the replicated VMs for ERP Application servers and, file servers and Arc-enabled SQL VM.
4- Promote Azure SQL GEO-replica to primary if automatic promotion is not enabled.
5- Update Azure Front Door to point to DR backends.
6- Ensure Load Balancer is configured and routing traffic to DR VMs.
7- Activate VPN Gateway (P2S) in the DR environment for admin access.
8- Apply NSGs and Firewall rules to secure the DR site.
9- Validate system functionality by checking ERP frontend, SQL database, and file server access.

10- Enable Azure Monitor and logs in DR to track system health.

11- Notify stakeholders that the DR site is now active.

8) DR Order of Completion

It defines the recommended order in which services should be brought online in the DR environment. The sequence ensures dependencies are respected, services start in a logical order, and users experience minimal disruption.

- **Networking and Security Components:**
  Deploy DR Virtual Network, Subnets, NSGs, VPN Gateway.
  Ensure Connectivity between Components is working.
  Apply Azure Firewall rules.

- **Storage Services:**
  Ensure File shares (Structured and Unstructured) are accessible and mounted to VMs.

- **Database:**
  Promote Azure SQL database (Geo-replica).
  Start the Arc-enabled SQL VM.

- **Applications:**
  Start ERP Application Servers (IIS).

- **Traffic Management:**
  Update Azure Load Balancer and Azure Front Door backends to point to DR services.

- **Monitoring:**
  Activate Azure Monitor and Log Analytics for DR resources.

- **Final Validation:**
  Test application functionality.
  Inform stakeholders that DR environment is fully operational.

9) Failback Procedure

The failback procedure outlines the steps required to transition operations from the DR site back to the primary site once it becomes available and stable. This ensures continuity while minimizing risks during the switchover.

- **Validate Primary Site Readiness:**
  Ensure all infrastructure is back online (networking, VMs, Storage)
  Perform health checks on the sites.

- **Replicates latest data back to primary:**
  Sync database (from Azure SQL to primary SQL if applicable).

Copy file shares and any updated configuration files from DR to primary.

- **Test Primary services in isolated mode:**
  Start ERP application and DB in test mode.
  Verify data integrity and service performance.

- **Update traffic routing:**
  Switch Azure front door and load balancers backends to point to primary site endpoints.

- **Trigger failback via ASR:**
  Use Azure Site Recovery to reverse replicate the VMs from DR to primary.
  Monitor failback job status and logs.

- **Activate Primary Site for users:**
  Notify stakeholders once validation is complete.
  Resume normal operations from primary.

10) Testing and Maintenance

To ensure the effectiveness of the Disaster Recovery Plan, regular testing and ongoing maintenance are required. Testing helps verify the readiness of the DR environment,

while maintenance ensures that the plan remains aligned with infrastructure changes.

10.1) Testing Types

1- **Planned DR Drill:** scheduled simulation where failover is triggered to the DR site in a controlled scenario

2- **Unplanned Simulation**: Surprise test to simulate real disaster behavior. Usually for internal validation.

3- **Component Validation:** Test individual components like SQL replication, VPN, firewall rules.

10.2) Recommended Testing Frequency

1- Full DR drill: Every 6 months.
2- Component checks: Every 1-3 months.
3- After major infrastructure or configuration change.

10.3) Maintenance Plan:

1- Review and update the runbook quarterly.
2-Validate that all scripts (failover, monitoring, automation) are working.
3) Document lessons learned from any previous test or incident.