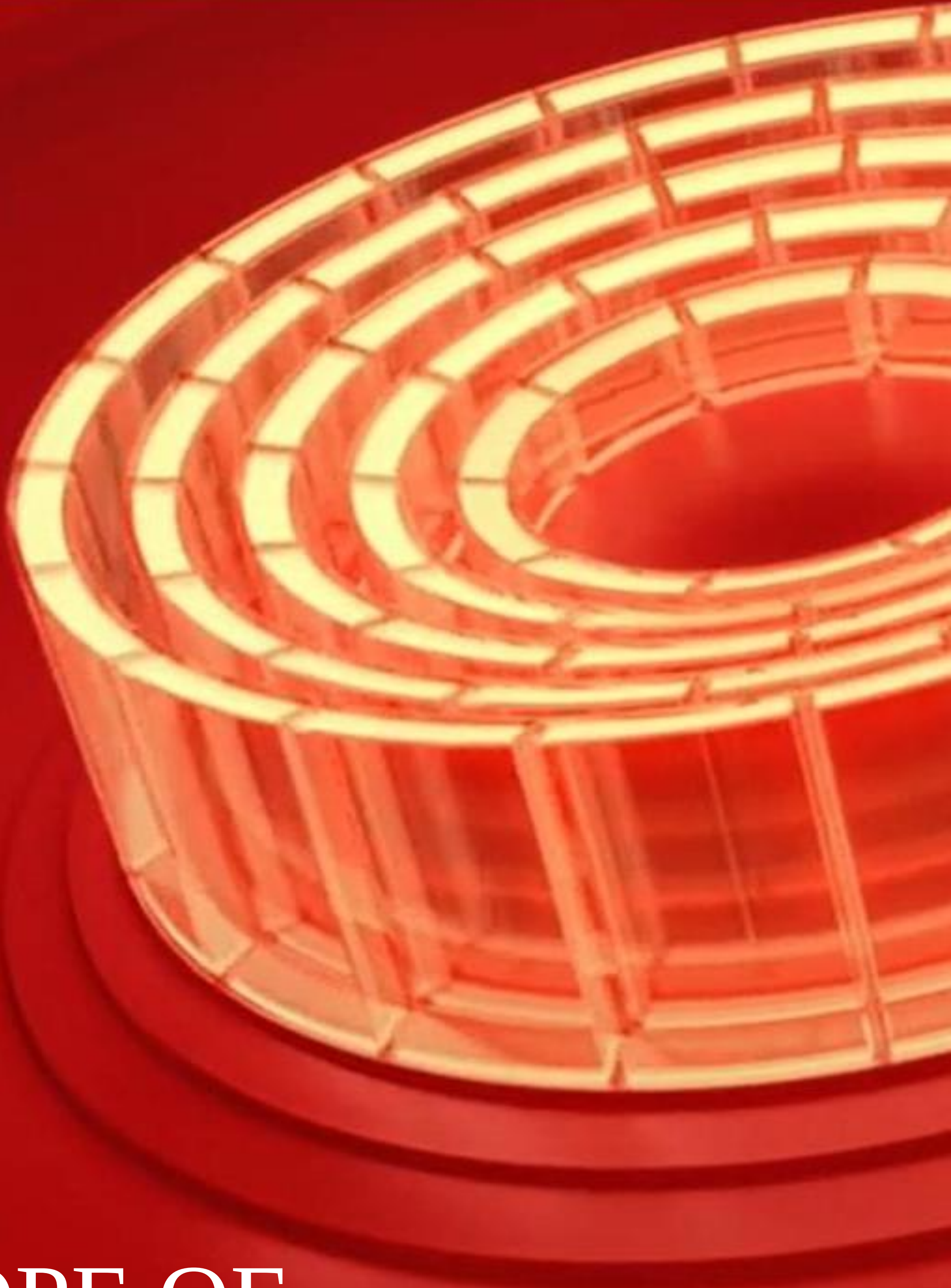

# SCOPE OF WORK

# 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 Content

1. Project Overview……………………………….4
2. Project Objectives……………………………….5
3. In-Scope Deliverables…………………………..6
3.1 Azure InfrastructureDeployment……………..6
3.2 Application Layer..........................................7
3.3 File Storage Layer..........................................7
3.4 Network and Security.....................................8
3.5 Database Layer...............................................9
3.6 Load Balancing and Access............................9
3.7 Disaster Recovery..........................................10
3.8 Documentation and Handover........................10
4. Out-of-Scope Items…………………………..11
5. Scope of Work Man-days…………………….12
6. Roles & Responsibilities……………………..13
7. Assumptions…………………………………..14
8. Final Deliverables……………………………..16

## 1) Project Overview

The project involves migrating the client’s on-premises ERP system to Microsoft Azure. It includes deploying a secure Azure Landing Zone, hosting application servers (IIS), setting up two types of file servers, deploying an Azure SQL Database, integrating the on-prem SQL Server using Azure Arc, and providing secure remote access via VPN P2S. Azure Front Door will ensure global availability and performance, while a full Disaster Recovery (DR) solution will be implemented using Azure Site Recovery (ASR) in a secondary region to meet the client's high availability and business continuity requirements.

## 2) Project Objectives

- Migrate the ERP system from the on-premises environment to Microsoft Azure to improve scalability, flexibility, and manageability.

- Deploy a secure Azure Landing Zone to host and manage all cloud resources in alignment with Microsoft’s best practices.
- Set up Application Servers (IIS) on Azure Virtual Machines to host the ERP frontend components.
- Deploy File servers :
  - Azure File Share for structured file storage with standard SMB access.
  - Azure Blob Storage: For unstructured data (e.g., logs, documents, backups) with mount capability or application-level integration.
- Deploy an Azure SQL Database for the ERP backend, leveraging PaaS capabilities.
- Integrate the on-prem SQL Server with Azure using Azure Arc to enable centralized management and hybrid capabilities.
- Configure VPN Point-to-Site (P2S) to allow secure access for remote users and admins.
- Implement traffic management and high availability using both:
  - Azure Load Balancer: To distribute traffic internally between IIS Application Servers hosted in Azure.

- Azure Front Door: To provide global access, intelligent traffic routing, SSL termination, and health monitoring for external users accessing the ERP system.

- Establish a full Disaster Recovery (DR) plan using Azure Site Recovery (ASR) to replicate workloads to a secondary region with an Active/Passive configuration.

# 3) In-Scope Delverables

## 3.1) Azurte Infrastructure Deployment

Design and deploy an Azure Landing Zone:

1- Virtual Networks (VNETs), Subnets, and Network Security Groups (NSGs).

2- Logging and monitoring with Log Analytics and Azure Monitor.

3- Configure Resource Groups, naming conventions, and tagging strategies.

4- Establish Hub-and-Spoke or flat architecture as per design decision.

## 3.2) Application Layer

1- Provision Azure Virtual Machines to host IIS Application Servers.

2- Install and configure Internet Information Services (IIS).

3- Ensure availability using Azure Load Balancer to distribute traffic across IIS servers.

4- Ensure the application layer integrates properly with backend SQL and file storage.

## 3.3) File Storage Layer

- Deploy and Configure two types of file storage

1- Azure File Share (SMB): Mounted to VMs for structured file sharing.

2- Azure Blob Storage: For unstructured data (e.g., documents, media, logs).

- Mount required file storage types to VMs.

## 3.4) Network and Security

- Deploy and configure VPN Point-to-Site (P2S) for secure remote access to Azure resources.
- Implement Azure Network Security Groups (NSGs) and Route Tables to manage and control internal traffic between subnets.
- Deploy Azure Firewall to enforce centralized traffic filtering and security policies across the environment.
- Provision and configure Azure Bastion for secure browser-based RDP/SSH access to Virtual Machines without exposing them to the public internet.
- Configure Private Endpoints to securely connect to Azure PaaS services (e.g., Azure SQL, Blob Storage).
- Enable diagnostics and logging using Azure Monitor and Log Analytics for full visibility and auditing.

## 3.5) Database Layer

- Deploy and configure VPN Point-to-Site (P2S) for secure remote access.
- Configure NSGs, route tables, and optional Private Endpoints.
- Enable diagnostics and logging for all network components.

## 3.6) Load Balancing and Access

- Implement Azure Load Balancer (Internal) for high availability of IIS VMs.

- Configure Azure Front Door to:

- Route external traffic globally.
- Provide SSL offloading, caching, and WAF (if required).
- Monitor backend health and auto-failover based on probe responses.

## 3.7) Disaster Recovery

- Deploy Azure Site Recovery (ASR) in a secondary region.

- Configure replication for:IIS VMs and File Server VMs

- Set replication policies, recovery plans, and failover/failback procedures.

- Conduct test failover to validate DR readiness.

## 3.8) Documentation and Handover

- Deliver full documentation including:

  - Architecture diagrams.
  - IP addressing and resource inventory.
  - VPN and storage configuration details.
  - DR runbooks and procedures.

- Conduct a handover session with the client’s technical team.

## 4) Out-of-Scope Items

➢ Application code development or modification

Any changes to the ERP application codebase or internal logic are not included in this project.

### ➢ End-user training

Training sessions for ERP users or IT staff are not included unless requested separately.

### ➢ On-premises hardware upgrades

No physical infrastructure changes or upgrades will be made to the on-premises data center.

### ➢ Long-term support or managed services

Ongoing support, patching, monitoring, or system administration post-deployment is not part of the scope unless a separate support agreement is signed.

### ➢ Data migration from on-prem file servers to Azure

Only the infrastructure for file storage will be deployed. Data copy/migration tasks must be handled by the client or addressed in a separate statement of work.

### ➢ **Third-party software licensing and procurement**

Procurement or management of licenses for OS, SQL, or any third-party software is the responsibility of the client.

- **Backup & Recovery of on-prem resources**

Only disaster recovery through Azure Site Recovery is included. On-prem backup solutions are not part of this scope.

## 5) Scope of Work Man-days

The table below outlines the estimated level of effort required to complete each migration phase. These figures reflect technical implementation, configuration, and validation

.

| Phase | Man-days |
|---|---|
| Planning & Assessments | 3 |
| Landing Zone Deployment | 5 |
| Workload Deployment | 7 |
| Database Setup | 3 |
| Networking and Access | 3 |
| Front Door and Load Balancer | 2 |

| | |
|---|---|
| Site Recovery Deployment | 5 |
| Testing & Validation | 3 |
| Documentation & handover | 2 |
| **total** | **33 days** |

## 6) Roles & Responsibilities

defines the key roles involved in the project and their associated responsibilities to ensure smooth delivery and collaboration between teams.

| Role | Responsibility |
|---|---|
| Client – IT Team | -provide access to on-premises infrastructure<br>- Share ERP architecture details<br>- Participate in testing (VPN, DR, App access)<br>- Handle file/data migration if required |
| Cloud Architect | Design Azure architecture (Landing Zone, VNETs, ASR, Front Door, etc.)<br>- Ensure best practices and security standards are applied |
| Azure Engineer | Deploy and configure Azure resources (VMs, SQL, VPN, Storage, Bastion, Arc)<br>- Mount file storage and set up internal/external connectivity |
| Security Engineer | Implement Azure Firewall, NSGs, and VPN P2S<br>- Ensure secure access (RBAC, Bastion)<br>- Validate compliance with security policies |

| | |
|---|---|
| Project Manager (if applicable) | - Monitor progress<br>- Coordinate between client and technical team.<br>-Track timelines and deliverables. |

## 7) Assumptions

This section outlines the assumptions made during the planning and execution of the project. These assumptions are critical to ensuring the timeline, scope, and responsibilities are accurate and achievable.

### Key Assumptions:

1- Azure subscription is already created and active with appropriate permissions granted to the deployment team.

2- On-premises SQL Server meets the prerequisites for Azure Arc onboarding (supported OS, network connectivity, agent installation allowed).

3- The client will provide access to require on-prem systems and documentation (e.g., ERP system specs, firewall rules, IP schema)

4- ERP application installation media and licenses will be provided by the client if needed on the Azure VMs.

5- The client will handle any file data migration from on-prem to Azure File Share or Blob unless otherwise specified.

6- The required public domain name and SSL certificates for Azure Front Door (if custom domain is used) will be provided by the client.

7- VPN P2S configuration will be tested and approved with support from the client's IT/network team.

8- Disaster Recovery is focused on Azure-hosted workloads only; on-prem DR is not part of the scope.

9- Client will review and sign off on the design before deployment begins.

## 8) Final Deliverables

At the end of the project, the following deliverables will be provided to the client to ensure full visibility, operational readiness, and documentation of the deployed environment.

### ➢ List of Final Deliverables

- **Azure Landing Zone Deployment Report**
- VNETs, Subnets, NSGs, Route Tables, Azure Firewall, Bastion, Resource Groups, and tagging schema.
- **IIS Application Server Deployment**
- VM specifications, installed roles, load balancing configuration, and monitoring setup.
- **File Server Configuration Document**
- Azure File Share and Blob Storage details, mount points, permissions, and usage instructions.
- **SQL Layer Documentation**
- Azure SQL Database specs and configuration.

- Azure Arc onboarding steps, connectivity status, and hybrid integration details.

- **Network & Access Report**

- VPN P2S setup guide (with client profiles).
- Access control (RBAC), NSG and firewall rules summary.

- **Azure Front Door & Load Balancer Configuration**
- Front Door backend pool config, health probes, custom domain (if any), SSL settings.
- Internal Load Balancer settings and availability setup.
- **Disaster Recovery Documentation**
- ASR Vault configuration, replicated items, replication policies, RTO/RPO design.
- DR runbook with test failover results and failback steps.

- **Architecture Diagram**

- Visio or PDF format of full Azure deployment including regions, services, and flows.

- **Credentials & Access Matrix** (if included)

- Admin access, service accounts, vault keys (securely handed over).

- **Handover & Knowledge Transfer**

- Summary session with client’s IT team.
- Q&A and walkthrough of documentation.

---

# Thank You