Multi-Phase Project Plan

Phase 1: Planning & Preparation

1) Create resource groups in subscriptions needed.
2) Plan non-overlapping address spaces:

- Hub VNet: 10.5.0.0/16 (Region 1 North Europe)
- Hub VNet: 10.10.0.0/16 (Region 2 UK South)
- Spoke VNet (Sub1): 10.15.0.0/16
- Spoke VNet (Sub2): 10.20.0.0/16

3) Identify security, compliance, and naming conventions.

Phase 2: Networking Setup

1) Create Hub VNet with:

- Virtual Network Gateway Subnet
- Subnet for Gateway
- Bastion Subnet

2) Create Spoke VNets in each subscription with:

- Subnet for App Services VNet integration
- Subnet for hosting SQL Database server

3) Create VPN S2S connections between Hub VNets in both regions and peering for hub and spoke connection.

Phase 3: Core Services Deployment

1) Deploy Application Gateway with WAF in Spoke VNet.
2) Deploy Azure App Services (API + Web) using Basic SKU, deploy your mobile backend code.
3) Deploy Azure SQL Database with Private Endpoint in Spoke VNet.
4) Deploy Traffic Manager to redirect traffic to App Gateway.

Phase 4: Private Endpoints & DNS

1) Create Private DNS Zones (e.g., privatelink.database.windows.net) in Hub.
2) Configure Private Endpoints for App Service and SQL Database.
3) Link Private DNS Zone to Spoke VNets and configure DNS forwarding if needed.

Phase 5: Security Hardening

1) Enable Azure Defender on App Service and SQL selectively.
2) Use Application Gateway with WAF for incoming traffic.
3) Validate Azure DDoS Basic enabled on VNets.
4) Configure NSGs to limit unnecessary traffic.

Phase 6: Monitoring & Logging

1) Enable Diagnostics on App Services, Application Gateway, and SQL.
2) Use AppInsight service for monitoring.

Phase 7: Testing & Handover

1) Test:

- VPN S2S connectivity.
- DNS resolution for private endpoints.
- App accessibility via Application Gateway.
- Database connectivity from App Service via Private Endpoint.

2) Document procedures and credentials securely.
3) Conduct performance, failover, and cost validation tests.