Solution:

Azure Region should be selected based on the lowest latency to the customer's region by using Azure Speed. Azure RBAC should be used for better security management and access to the resources.

Components

This architecture consists of the following components:

- **Azure Active Directory** – provides SSO and multi-factor authentication
- **4 Azure VMs** – with web server IIS role installed, that will run the .Net business application.
- **Azure Public Load balancer –** used to evenly distribute the incoming traffic to the servers.
- **Azure VM running Oracle DB –** easiest way to migrate an Oracle DB is the Lift and Shift approach. Having the proper license to use Oracle software, the customer can migrate their DB to Azure VMs. More info here.
    - Create Azure VM with the right specification.
    - Migrate the Oracle DB to the Azure VM
- **Azure Files –** is used for the 4 TB of shared data. Azure Files is a cost-effective solution and Azure File Share can span up to 5 TiB, which covers the customer's requirements. Azure Files offers a standard file share hosted on HDD-based hardware and premium file share hosted on SSD hardware. Plus Azure File Share can be backed up as well.

  I also took in account that Azure has a feature of using shared managed disks. But it is only available for ultra-disks and premium SSDs which are quite pricey. This can be taken in consideration if a disk share is required.

  Also, Azure NetApp Files can be taken in consideration as a share, but it is more suitable for large organization and is pricey.

- **Recovery Service Vault–** used to store the back up data for each protected resource.
- **Azure Backup –** selected to cover the RTO requirement of one business day. It provides a simple and cost-effective solution to back up the data and recover it from Microsoft Azure Cloud.
- **VPN Gateway** that is placed in its own subnet.
- **Site-to-site connection** allowing On-prem and Azure to communicate. So, the application is accessible from Data Center.

Data Flow

1. One of the Bank's employee authenticates within **Azure AD** and have access to the Web App. Azure AD B2B can be used to invite and collaborate with external users. The users can use their own credentials to access the resources.

   Also, Azure AD can sync with on-premises AD through Azure AD connect if that is the case.

2. As the requests are flowing in, Azure Load Balancer distributes them across the 4 VMs, according to the configured load-balancing rules and health probes.

3. The middle tier that processes the requests consists of **Service Bus** and **Function App**. Once the form is submitted, it is sent to a queue, which follow FIFO approach, in the message broker (**Service Bus**). Service Bus was chosen as the solution as it support asynchronism

which is relevant when a huge number of users is onboarded. Also, for its Duplicate detection feature, that will drop any duplicate.

4. The 4 Windows Server Virtual machines have access to shared data through Azure File Share with a total of 4 TB.

5. The app uses the Oracle DB that was migrated to an Azure VM, using Lift and Shift method.

6. For the application to communicate with the Data centre, a Site to Site connection is required. A VPN gateway is deployed in its own subnet. A VPN device must be configured on the on-premises location as well. Once done, we can create the S2S VPN connection between the virtual network gateway and on-prem VPN device.

7. Now the batch updates can reach the DB in Azure.

   I also took in consideration, the batch updates are more efficient to be sent rather each update separately, but this means that latency will occur. In this case Express Route can be taken in consideration. The connection does not go over public internet, therefore it has faster speed and consistent latency. The only downsize is it has a high cost. As reducing costs is a requirement, I chose Site to Site connection.
8. To cover the RTO requirement Azure Back Up is used. For our scenario, it can back up Azure VMs and Azure File shares.
9. Azure AD provides SSO, but in order to provide a recommendation, I would need more information on the legacy SSO solution from on-premises.

Some recommendations for increased security over Azure resources:

- Azure Security Center can be used for advanced threat protection for hybrid workload, as in our case. It is a management system that assess any new resource, if they are configured and deployed according to security best practices.
- Microsoft provides Basic DDoS protection as part of the Azure Platform. Standard DDoS protection is also available for a cost.
- Azure Disk Encryption can be integrated with Azure VMs, by using bit locker.
- And Azure BackUp will be used as well to protect from any human error or data deletion.

Related the compliance with regulation:

- Please find here all the Azure compliance documentation, for financial services and GDPR as well.
- Microsoft compliance offering for Azure can be found in here.
- Microsoft Compliance Manager – verifies the if the organization is compliant when using Microsoft Cloud Services
- Azure Security Center and Azur Policy can help you to apply security policies across hybrid cloud workload.

To cover the pricing concerns, I am sharing Azure Pricing Calculator Estimate for the proposed infrastructure.