**Note: for all the below tasks please follow resource group and other azure resources names as per your convenient, please use AVM modules in the module requirements.**

1. Design a Bicep template to create an Azure Key Vault in the Resource Group (RG-EY-India). The template should include parameters for configuring access policies and private endpoint requirements. It should also integrate with a Log Analytics workspace. set the Key Vault SKU to Standard, configure network ACLs to deny access, and grant access policies for only 'Get' and 'List' secret permissions.

2. Create a **Storage Account that meets below specifications**.

* Specifies allowed types for the storage account (StorageV2, Blob Storage, File Storage).
* Restricts redundancy options to Standard\_LRS and Standard\_ZRS.
* Configures private endpoint access.
* Integrates with Log Analytics Workspace.
* Enables Blob Lifecycle Management to automatically delete blobs older than 365 days.

3. Create an Bicep template with **Azure App Service**, **Azure Application Insights**, including the configuration for performance and availability metrics, as well as network settings to ensure the service is exposed **via private endpoint only**.

4.Create an Azure Load Balancer within a dedicated virtual network and subnet and integrate it with a Log Analytics workspace. Implement this configuration in a module format.

5. Create a simple application architecture using a Bicep template, including the following resources:

* Deploy a virtual machine with an inbuilt IIS server in the Frontend subnet, ensuring the necessary NSG rules are applied.
* Deploy a SQL Server in the Backend subnet, with communication allowed only through the Frontend subnet's NSG rules.
* Create a Log Analytics workspace to capture logs from both the virtual machine and SQL Server.

6. task to configure Azure Data Factory within a dedicated private subnet. Ensure the Data Factory uses a system-assigned identity,

enables integration with a Log Analytics workspace and configures diagnostic settings for monitoring and logging.

7.task to create a Cosmos DB with primary and secondary locations and configure auto-failover priority. Additionally, set up an alert to notify when the database is deleted.

8. Create a production-grade Azure Kubernetes Service (AKS) cluster using a Bicep template, ensuring it meets all production standards, including the following:

* Set up a dedicated virtual network and subnet for the AKS cluster with proper network segmentation.
* Configure network policies to ensure secure communication between AKS nodes and other resources.
* Integrate the AKS cluster with a SQL Database hosted in a dedicated network.
* Implement network monitoring and set up alerts for critical network performance and security events.
* Enable auto-scaling, logging, and monitoring of the AKS cluster.
* Ensure proper security measures are applied, such as role-based access control (RBAC), Azure Active Directory integration, and network security groups (NSGs).

9. Create an Azure Migrate project using a Bicep template with the following requirements:

* Deploy an Azure Migrate project for assessment and migration purposes in the specified Azure region.
* Optionally create a Recovery Services Vault in the same region for storing replication and recovery data.
* Deploy an Azure Migrate appliance for discovering on-premises machines and enabling replication.
* Ensure that the project, appliance, and recovery vault are tagged appropriately for organizational purposes (e.g., 'Environment: Production', 'Department: IT').
* Output the IDs of the Azure Migrate project, Recovery Services Vault (if created), and the Azure Migrate appliance for future use or integration.

Ensure the deployment is flexible with parameters like location, project name, appliance name, and Recovery Services Vault name (optional).

10. Create a Bicep template to design a secure 3-tier architecture in Azure with the following resources:

**Requirements:**

1. **App Service with Staging and Production Slots**:
   * Deploy an Azure App Service with both Staging and Production slots.
   * Enable custom domains for each environment.
   * Configure auto-scaling options for handling traffic fluctuations.
2. **Function Apps**:
   * Create Function Apps for serverless processing, ensuring scalability and optimal resource usage.
3. **Log Analytics Workspace**:
   * Deploy a Log Analytics Workspace to collect and monitor logs across all resources in the architecture.
4. **SQL Server with Production and Staging Databases**:
   * Provision an Azure SQL Server and create separate Production and Staging databases with high availability configurations.
   * Ensure encryption at rest and enable secure connectivity.
5. **Storage Account with Blob Containers**:
   * Create an Azure Storage Account with Blob Containers for secure data storage.
   * Ensure secure access control and encryption.
6. **Traffic Manager**:
   * Set up Azure Traffic Manager for routing traffic between the different environments (App Service and Function Apps).
   * Ensure high availability and regional routing.
7. **Azure CDN**:
   * Configure Azure Content Delivery Network (CDN) to cache and deliver content globally, improving performance and reducing latency.
8. **Security Standards**:
   * Apply Azure security best practices across all resources:
     + Enable Network Security Groups (NSGs) and restrict access.
     + Use Managed Identity for secure access to resources.
     + Implement Role-Based Access Control (RBAC) for least privilege access.
     + Ensure encryption at rest and in transit for all resources.
     + Integrate with Azure Security center for continuous monitoring and security compliance.