**Overview**

Cloud Portal Hub is an ecommerce-based company. They currently have an Azure subscription and an Azure tenant in place.

**Current Environment**

* The company currently has two applications deployed to the Azure Web App service. One is used by customers to place orders and the other is used by the Customer Support Center staff. The name of the application used by the customers is “PortalHub” and the one used by the Customer Support Center staff is “SupportHub”
* They also have an Azure SQL Database which consists of Customer, Product, Order and other information pertinent to the application.
* The company’s Customer Support Center also has the ability to upload receipts. These receipts can be uploaded either via the web application “SupportHub” or by placing it in an Azure Files mounted folder.

The Customer table in the Azure SQL database has the following schema

|  |  |
| --- | --- |
| Column | Description |
| UserID | Unique identifier for the customer. |
| UserCode | Extra Code feature attached for a loyalty programme. The format of the code is 1234-123-1234 |
| UserName | Name of the Customer |
| City | City the Customer is located in |
| UserPin | A security number used as an additional authentication method |

* Managed Service Identity has been enabled for the web Application “SupportHub”
* The Azure Function is made to process all receipts. The Azure Function stores the results in Azure Blob Storage and the Azure SQL Database. An email summary with a link to a report is sent to either the user or the Customer Support Center representative. The report is stored in Azure Blob storage. The link to the report must remain valid even if the email it forwarded to another user.
* Concurrent processing of a receipt must be prevented.
* Application Insights is used to gather telemetry data and logging in both the Azure Function and in the web application “SupportHub”. TraceWriter logging is also enabled. Application Insights must always contain all log messages.

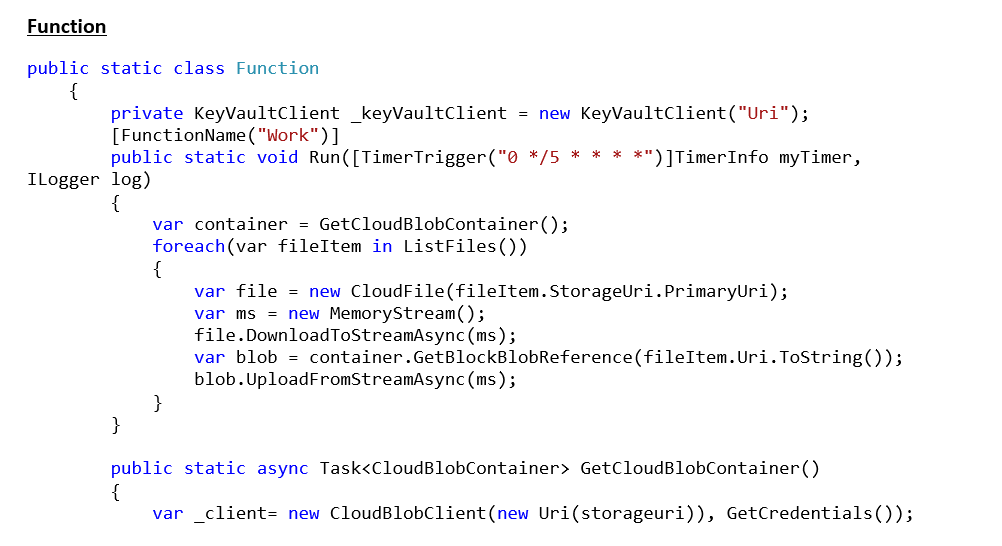
**Requirements**

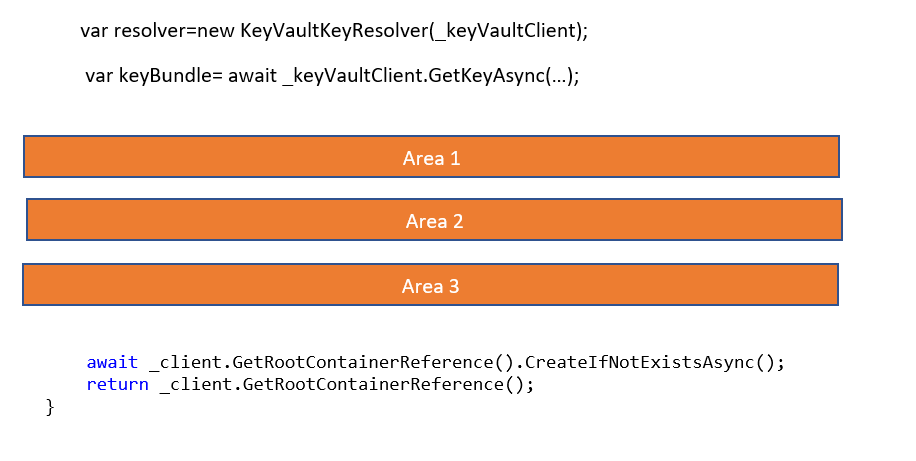
The company has the following requirements

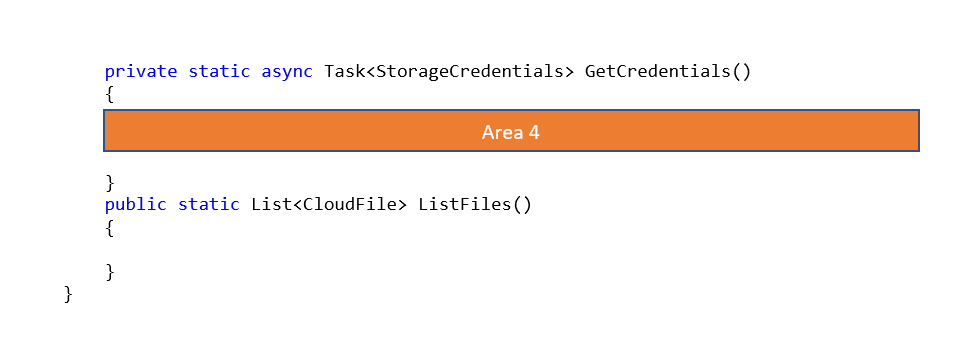
* Disaster recovery should be in place. It needs to be ensured that even a regional outage does not impact the availability of the web applications. All data in the DR region must be up to date. The operations for disaster recovery must not be dependent on the running application.
* The UserPin column data in the Customer table must be stored in such a way that it does not allow viewing of the column data in the table. Only the web applications should have access to the data.
* All access to storage accounts and the Azure SQL database must be carried out using Managed Service Identities.
* All certificates and secrets that is used to secure data must be stored in the Azure Key Vault
* All Order data must be encrypted at rest
* All data must be protected in transit
* The UserCode must only be visible to the logged in users. Any other view of the UserCode must only include the last segment and the remaining parts obscured.

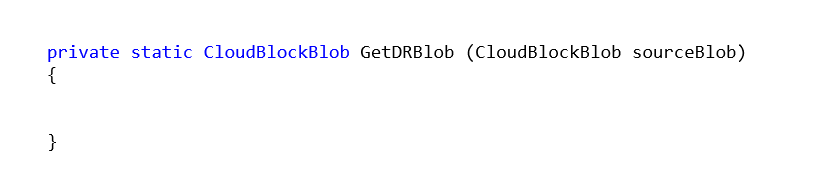
You have the following code files as well

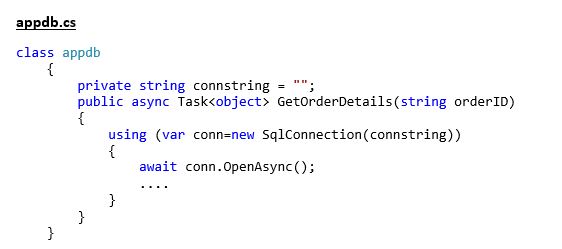
**Processing.cs**











You have the following PowerShell script to set the encryption for the underlying storage account

**Admin.ps1**

