```
DB01 public class Database
DB02 {
DB03   private string ConnectionString =
DB04
DB05  public async Task<object> LoadUserDetails(string userId)
DB06  {
DB07
DB08  return await policy.ExecuteAsync (async () =>
DB09  {
DB10    using (var connection = new SqlConnection (ConnectionString))
DB11    {
DB12      await connection.OpenAsync();
DB13      using (var command = new SqlCommand("_", connection))
DB14      using (var reader = command.ExecuteReader())
DB15       {
DB16            -
DB17       }
DB18    }
DB19   }};
DB20  }
DB21 }
```

ReceiptUploader.cs

```
RU01  public class ReceiptUploader
RU02  {
RU03    public async Task UploadFile(string file, byte[ ] binary)
RU04    {
RU05      var httpClient = new HttpClient();
RU06      var response = await httpClient.PutAsync( "…", new ByteArrayContent(binary));
RU07      while (ShouldRetry (response))
RU08      {
RU09        response = await httpClient.PutAsync ("…", new ByteArrayContent(binary));
RU10    }
RU11  }
RU12  private bool ShouldRetry(HttpResponseMessage response)
RU13  {
RU14
RU15   }
RU16 }
```

ConfigureSSE.ps1

```
CS01 $storageAccount = Get-AzureRmStorageAccount -ResourceGroupName "…" -AccountName "…"
CS02 $keyVault = Get-AzureRmKeyVault -VaultName "…"
CS03 $key = Get-AzureKeyVaultKey -VaultName $keyVault.VaultName -Name "…"
CS04   Set-AzureRmKeyVaultAccessPolicy'
CS05   -VaultName $keyVault.VaultName'
CS06  -ObjectId $storageAccount.Identity.PrincipalId'
CS07
CS08
CS09  Set-AzureRmStorageAccount"
CS10 -ResourceGroupName $storageAccount.ResourceGroupName'
CS11 -AccountName $storageAccount.StorageAccountName'
CS12 -EnableEncryptionService File '
CS13 -KeyvaultEncryption'
CS14 -KeyName $key.Name
CS15 -KeyVersion $key.Version'
CS16 -KeyVaultUri $keyVault.VaultUri
```

QUESTION 1
HOTSPOT
You need to ensure that security requirements are met.

How should you complete the code segment?

To answer, select the appropriate option in the answer area.

NOTE: Each correct selection is worth one point.

```
New-AzureRmSqlDatabaseDataMaskingRule '
      -ServerName          "datastore" '
      -DatabaseName        "expense" '
      -ResourceGroupName   "production" '
      -SchemaName          "dbo" '
      -TableName           "Users" '
-ColumnName                "
```

[▼]
- UserId" '
- SupervisorId" '
- ExpenseAccount" '
- AllowedAmount" '

```
-MaskingFunction
```

[▼]
- Text '
- Default '
- Number '
- NoMasking '

```
-SuffixSize
```

[▼]
- 2'
- 3'
- 4'
- 9'

```
-ReplacementString         "
```

[▼]
- xx"
- xxxx"
- xxxxxxx"
- xxxxxxxxx"

Correct Answer:

```
New-AzureRmSqlDatabaseDataMaskingRule '
      -ServerName          "datastore" '
      -DatabaseName        "expense" '
      -ResourceGroupName   "production" '
      -SchemaName          "dbo" '
      -TableName           "Users" '
-ColumnName                "
```

UserId" '
SupervisorId" '
ExpenseAccount" '
AllowedAmount" '

```
-MaskingFunction
```

Text '
Default '
Number '
NoMasking '

```
-SuffixSize
```

2'
3'
4'
9'

```
-ReplacementString         "
```

xx"
xxxx"
xxxxxxx"
xxxxxxxxx"

QUESTION 2
You need to ensure the security policies are met. What code do you add at line CS07?

A. -PermissionsToKeys wrapkey, unwrapkey, get
B. -PermissionsToKeys create, encrypt, decrypt
C. -PermissionsToCertificates wrapkey, unwrapkey, get
D. -PermissionsToCertificates create, encrypt, decrypt

Correct Answer: D
Explanation:
Scenario: All certificates and secrets used to secure data must be stored in Azure Key Vault.

You must adhere to the principle of least privilege and provide privileges which are essential to perform the intended function.

The Set-AzureRmKeyValutAccessPolicy parameter -PermissionsToKeys specifies an array of key operation permissions to grant to a user or service principal. The acceptable values for this parameter: decrypt, encrypt, unwrapKey, wrapKey, verify, sign, get, list, update, create, import, delete, backup, restore, recover, purge.

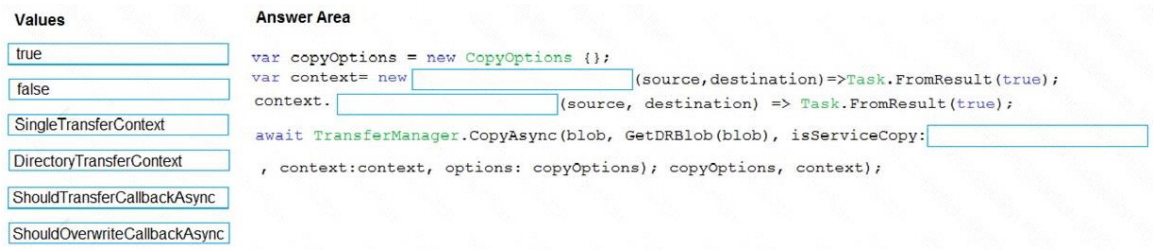
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurermkeyvaultaccesspolicy

QUESTION 3
DRAG DROP
You need to ensure disaster recovery requirements are met.

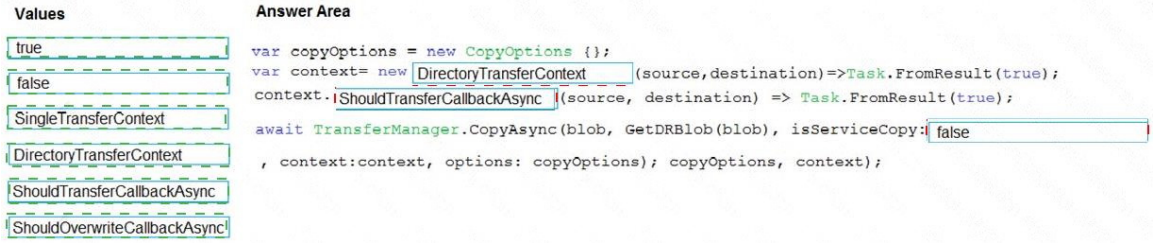
What code should you add at line PC16?

To answer, drag the appropriate code fragments to the correct locations. Each code fragment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Correct Answer:



QUESTION 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

You need to ensure that the SecurityPin security requirements are met.