# Question10 Manage data security

Case Study

**Instructions**  
  
This case study contains 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.  
  
Note: You cannot go back or review questions of this type on the actual certification exam.

## Question 10.1-

You manage an Azure SQL Database containing a column with sensitive data. The column is used for joins by an application.  
  
You need to configure encryption for this database to protect the column.  
  
Solution: You configure Always Encrypted with a randomized type.  
  
Does the solution meet the goal?

No

Yes

## Question 10.2-

You manage an Azure SQL database containing a column with sensitive data. The column is used for joins by an application.  
  
You need to configure encryption for this database to protect the column.  
  
Solution: You configure Always Encrypted with a deterministic type.  
  
Does the solution meet the goal?

No

Yes

## Question 10.3-

You manage an Azure SQL database containing a column with sensitive data. The column is used for joins by an application.  
  
You need to configure encryption for this database to protect the column.  
  
Solution: You configure dynamic data masking (DDM) with random masking.   
  
Does the solution meet the goal?

No

Yes

## Question 10.4-

You manage an Azure SQL database containing a column with sensitive data. The column is used for joins by an application.  
  
You need to configure encryption for this database to protect the column.  
  
Solution: You configure dynamic data masking (DDM) with partial masking.  
  
Does the solution meet the goal?

No

Yes

# Question71 - Manage data security-

Your company stores your consumer contact details in an Azure SQL Database. Data is encrypted at rest with the default Microsoft-managed transparent data encryption (TDE).  
  
Because of the company’s new security policy, you are asked to re-encrypt consumer database with your company’s own asymmetric key and enable auditing on its use.  
  
To support this, you set up a new Azure Key Vault and import a custom encryption key into it.  
  
You need to enable TDE with the new custom key from Azure Key Vault. You will use PowerShell cmdlets, not Azure Portal, for this configuration.  
  
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

Create a list in the correct order

Possible actions

Actions in order

* Export an Azure SQL Database to a BACPAC file.
* Import a BACPAC file to an Azure SQL Database.
* Assign an Azure AD identity to the Azure SQL Database server.
* Grant Key Vault permissions to the Azure SQL Database server.
* Add the Key Vault key to the Azure SQL Database server and set it as TDE Protector.
* Turn on TDE.

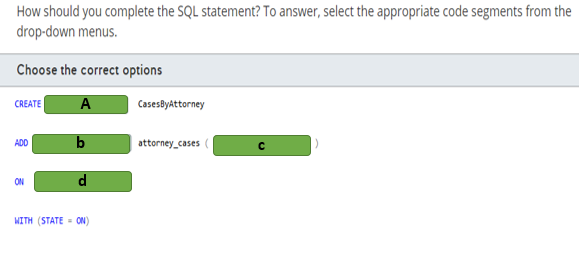
# Question72- Manage data security-

You are a data engineer for a law firm. You create the following Azure SQL Database table:  
  
CREATE TABLE [Case]  
(  
  [CaseNumber] [int],  
  [Attorney] [sysname],  
  [Type] [varchar] (50),  
  [Docket] [varchar] (10)  
)  
  
Each attorney has a database user account. The Attorney column represents a database user account. You create the following function:  
  
CREATE FUNCTION attorney\_cases(@Attorney as sysname)  
RETURNS TABLE  
WITH SCHEMABINDING  
AS  
RETURN SELECT 1 as retVal WHERE USER\_NAME() = @Attorney  
  
You need to write a query that performs the following:

* Enforce row-level security on the Case table.
* Ensure that rows are returned only for the attorney performing the query.

You need to construct the query.  
  
How should you complete the SQL statement? To answer, select the appropriate code segments from the drop-down menus.

Choose the correct options



A)

1. FILTER PREDICATE
2. FUNCTION
3. SECURITY POLICY

B)

1. FILTER PREDICATE dbo
2. SECURITY POLICY

C)

1. Attorney
2. [dbo].[Case]
3. CURRENT\_USER

D)

1. Attorney
2. [dbo].[Case]

# Question73- Manage data security-

You are a data engineer. The following query creates a table in an Azure SQL Database:  
  
CREATE TABLE Employee (  
  [ID] [int],  
  [GivenName] [varchar](50)  
    COLLATE Latin1\_General\_BIN2  
    ENCRYPTED WITH (COLUMN\_ENCRYPTION\_KEY = EmployeeCEK,  
    ENCRYPTION\_TYPE = RANDOMIZED ,   
    ALGORITHM = 'AEAD\_AES\_256\_CBC\_HMAC\_SHA\_256'),  
  [SurName] [varchar](50),  
  [SSN] [char](9)   
    COLLATE Latin1\_General\_BIN2  
    ENCRYPTED WITH (COLUMN\_ENCRYPTION\_KEY = EmployeeCEK,  
    ENCRYPTION\_TYPE = DETERMINISTIC ,   
    ALGORITHM = 'AEAD\_AES\_256\_CBC\_HMAC\_SHA\_256'),  
)  
  
You write the following query to insert data into the table:  
  
DECLARE @SSN = '123456789';  
INSERT INTO Employee(ID, GivenName, SurName, SSN)  
SELECT 1, 'Sam', 'Jack', @SSN  
  
You need to determine which queries will return data when you enable Always Encrypted and Parameterization for Always Encrypted.  
  
For each of the following queries, select Yes if the query returns data. Otherwise, select No.

|  |  |  |
| --- | --- | --- |
| **Query** | **Yes** | **No** |
| DECLARE @SSN char(9) = '123456789'; SELECT GivenName FROM Employee WHERE SSN=@SSN |  |  |
| DECLARE @Name varchar(50) = 'Sam'; SELECT SSN FROM Employee WHERE GivenName = @Name |  |  |
| SELECT GivenName, SSN FROM Employee |  |  |

# Question74- Manage data security - D

You are a data engineer. You create a table with the following query:  
  
CREATE TABLE License (  
  [ID] int,  
  [Number] char(9)  MASKED WITH (FUNCTION = 'partial(3, "xxxxx", 1)') NULL,  
  [GivenName] varchar(20),  
  [SurName] varchar(20)  
)  
  
You insert data by using the following query:  
  
INSERT INTO License (ID, Number, GivenName, SurName)  
SELECT 1, '111222333', 'Sam', 'Jack'  
  
You then run the following query to return data:  
  
SELECT Number FROM License where ID=1  
  
You need to determine which value is returned from the query.  
  
Which value is returned?

Choose the correct answer

22233

xxx22233x

1113

111xxxxx3

# Question75- Manage data security - D

You are a data engineer for your company. You manage a SQL Server 2019 database on an Azure virtual machine (VM). A developer at the company needs to connect to the database from a client application. The client application passes the credentials in the connection string.  
  
You need to allow the developer to return decrypted values for encrypted columns.  
  
Which parameter should the developer specify in the connection string?

Choose the correct answer

Integrated Security = false

Column Encryption Setting = enabled

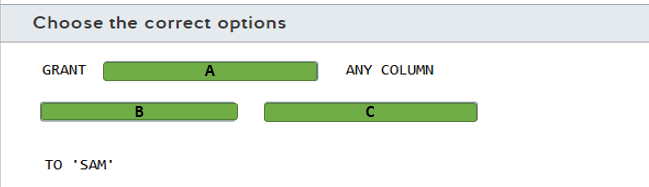
Integrated Security = true

Column Encryption Setting = disabled

# Question76- Manage data security-

You are a data engineer for your company. You manage a SQL Server 2019 database on an Azure virtual machine (VM). You configure the database to use Always Encrypted.  
  
You need to grant a user named Sam permission to manage the key that is used to encrypt and decrypt column encryption keys.  
  
How should you complete the SQL statement? To answer, select the appropriate code segments from the drop-down menus.

Choose the correct options



A)

1. ALTER
2. VIEW

B)

1. ENCRYPTION
2. MASTER

C)

1. KEY
2. KEY DEFINATION

# Question77- Manage data security-

You are a data engineer for your company. You manage a SQL Server 2019 database on an Azure virtual machine (VM). You configure the database to use Always Encrypted.  
  
You need to grant a user named Sam permission to query encrypted columns.  
  
Which minimal permissions should you grant to Sam? For each of the following statements, select Yes if the statement is true. Otherwise, select No.

|  |  |  |
| --- | --- | --- |
| **Statement** | **Yes** | **No** |
| Grant the ALTER ANY COLUMN MASTER KEY permission. |  |  |
| Grant the ALTER ANY COLUMN ENCRYPTION KEY permission. |  |  |
| Grant the VIEW ANY COLUMN MASTER KEY DEFINITION permission. |  |  |
| Grant the VIEW ANY COLUMN ENCRYPTION KEY DEFINITION permission. |  |  |

# Question78 - Manage data security-

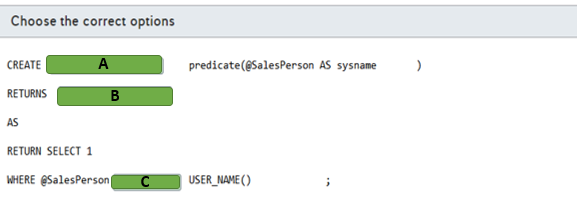
You are a data engineer for your company. Your company is developing a new application that uses Azure SQL Database. You are designing a security policy to help keep the company's data secure.  
  
You need to provide instructions to developers on how to prevent SQL injection attacks.  
  
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

|  |  |  |
| --- | --- | --- |
| **Statement** | **Yes** | **No** |
| Eliminate the use of stored procedures. |  |  |
| Use ad-hoc queries. |  |  |
| Validate user input. |  |  |

# Question79 - Manage data security-

You manage an Azure SQL Database that has the following table definition:  
  
CREATE TABLE [Order]   
(  
  OrderID int,  
  SalesPerson sysname,  
  ProductID int,  
  Quantity int,  
  Price decimal(8, 2)   
);  
  
The SalesPerson field represents the database user of a sales person responsible for the order. A sales person should only be able to query his or her own orders. You want to use a security policy and row-level security to enforce this.  
  
You need to define the security policy predicate.  
  
How should you complete the code? To answer, select the appropriate code segments from the drop-down menus.

Choose the correct options



A)

1. FUNCTION
2. TABLE

B)

1. FUNCTION
2. TABLE

C)

1. =
2. <>

# Question80- Manage data security - D

You are a data engineer for an Azure SQL Database. You write the following SQL statements:  
  
CREATE TABLE Customer (  
  CustomerID int IDENTITY PRIMARY KEY,  
  GivenName varchar(100) MASKED WITH (FUNCTION = 'partial(2,"XX",0)') NULL,  
  SurName varchar(100) NOT NULL,  
  Phone varchar(12) MASKED WITH (FUNCTION = 'default()')  
);  
  
INSERT Customer (GivenName, SurName, Phone) VALUES ('Sammy', 'Jack', '555.111.2222');  
  
SELECT \* FROM Customer;  
  
You need to determine what is returned by the SELECT query?  
  
What data is returned?

Choose the correct answer

1 SaXX Jack xxxx

1 XXXX Jack XXX.XXX.XXXX

1 SaXX Jack XXX.XXX.2222

1 xx Jack XXX.XXX.2222

# Question81- Manage data security-

Your company’s accounting system uses Azure SQL Database as a backend. You enable geographic redundancy between the primary and secondary Azure SQL Database instances hosted in two different Azure regions.  
  
Your corporate IT security policy dictates that, instead of Microsoft-managed keys, you should use your own asymmetric keys for Azure SQL Database Transparent Data Encryption (TDE). You deploy Azure Key Vaults in both Azure regions, create a new encryption key (TDE protector) in the primary region’s Key Vault, and clone it into the secondary region’s Key Vault via backup and restore.  
  
You need to configure TDE in your geo-redundant Azure SQL Database environment to use your TDE protector. You should perform these tasks in Azure portal.  
  
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

Create a list in the correct order

Possible actions

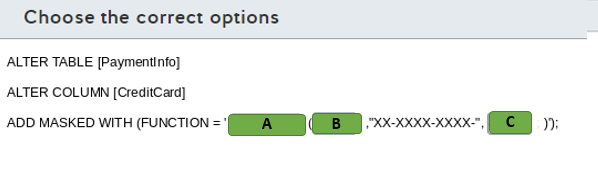
Actions in order

* On the primary Azure SQL Database server, set the Advanced Data Security feature to Off.
* On the secondary Azure SQL Database server, set the Advanced Data Security feature to Off.
* On the primary Azure SQL Database server, set the Advanced Data Security feature to On.
* On the secondary Azure SQL Database server, assign a Key Vault from the same region.
* On the secondary Azure SQL Database server, assign the TDE protector.
* On the primary Azure SQL Database server, assign a Key Vault from the same region.
* On the primary Azure SQL Database server, assign the TDE protector.

# Question83-

You work for a call center company that uses Azure SQL Database. The database stores customer credit card numbers in a table named PaymentInfo. Telemarketing attendants will consult this table to help with customer payment support.  
  
You need to implement dynamic data masking (DDM) in the PaymentInfo table to mask credit card numbers for telemarketing attendants. Only the two first digits and the last four digits should be visible.  
  
How should you complete the T-SQL query? To answer, select the appropriate options from the drop-down menus.

Choose the correct options



A)

1. Default
2. Partial
3. random

B)

1. 0
2. 2
3. 4

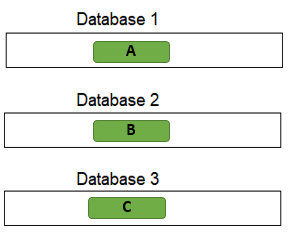
C)

1. 0
2. 2
3. 4

# Question84-

You are a data engineer. You manage three SQL Server databases in Azure. The databases must meet the following security requirements:  
  
Database 1 - Only specific columns in the 10 tables must be encrypted.  
Database 2 - All data in the entire database must be encrypted at rest.  
Database 3 - Data must be encrypted while in transit between the client application and Azure.  
  
You need to determine which encryption technology to use for each database.  
  
Which encryption technology should you use for each database? To answer, choose the correct encryption technology from the drop-down menus.

Choose the correct options



A)

1. Always Encrypted
2. Transparent Data Encryption

B)

1. Always Encrypted
2. Transparent Data Encryption

C)

1. Always Encrypted
2. Transparent Data Encryption

# Question85-

You manage an Azure SQL database for a financial application.   
  
You need to configure a dynamic data mask to completely mask the data of a specific varchar field.   
  
Which masking function should you use?

Choose the correct answer

Email

Default

Partial

Random

# Question86-

You manage an Azure SQL Database for a mission-critical application named ElectronicsProduction. The database stores personal information about your users.  
  
You need to implement Transparent Data Encryption (TDE) with a customer-managed encryption key in this database. You assign an Azure Active Directory (AD) identity in Azure SQL Database.  
  
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of possible actions to the answer area and arrange them in the correct order.

Create a list in the correct order

Possible actions

Actions in order

* Create a master key in the master database.
* Create a server certificate using the master key.
* Create a database encryption key from the certificate in ElectronicsProduction.
* Create an Azure Key Vault and generate a new key.
* Grant Key Vault permissions to the Azure SQL Database server.
* Add the Key Vault key to the Azure SQL Database server.
* Set the TDE Protector to use the Key Vault key.
* Enable encryption in the ElectronicsProduction database.