Data Masking

What is data masking?

Data masking is process of modifying actual data using some characters or numbers to protect the sensitive data. Data masking is also known as data obfuscation.

Why data masking is done?

Data masking is used to protect sensitive data from threats while providing the similar functionality of the original version. It ensures sensitive information is not available beyond production environment.

Which techniques are used for data masking?

- Data Pseudonymization
- Data Anonymization
- substitution
- Encryption
- Redaction
- Averaging
- Shuffling
- Date Switching
- Nulling out

Where data masking is implemented/When data masking is required?

- Personally identifiable information
- Protected health information
- Intellectual property
- Payment card information

What are all the types of data masking?

- Static data masking
- Dynamic data masking
- On the fly data masking,
- Deterministic data masking.

How data masking is implemented?

Data masking is three step process:

- First, Sensitive information is identified.
- Secondly, appropriate data masking technique is applied on the sensitive information
- Finally, continuous auditing is done to ensure whether the required output is reached. In other words, continuously auditing is done to ensure whether data masking is working as expected.

Where data masking is used?

In user training, sales demos, software testing.