What's covered here?

- Security Implementation

Transparent Data Encryption (TDE)

- Protect data on physical media, such as hard drives
- TDE performs real-time I/O encryption and decryption of the data and log files
- Enables software developers to encrypt data by using AES and DES encryption algorithms without changing existing applications

SQL Injection

- Dynamic SQL
  - Concatenate strings to create dynamic SQL queries
- SQL Injection
  - Hackers make substitution for variables from front-end application
- SQL injection can provide a back door for hackers to access or destroy data and system

How To Prevent SQL Injection

- Use sp_executesql Stored Procedure if possible
- Always validate the input data
- Disallow apostrophes, semicolons, parentheses, and double hyphens (––) in the input if possible
- Reject strings that contain binary data, escape sequences, and multiline comment markers (/* and */)
- Validate XML input data against an XML schema when possible

Ownership Chains

- When multiple database objects access each other sequentially, the sequence is known as a chain
- Ownership chaining enables managing access to multiple objects, such as multiple tables, by setting permissions on one object, such as a view

Contained Database

(new in SQL Server 2012)

- Isolated from other databases and from the instance of SQL Server that hosts the database
- Much of the metadata that describes a database is maintained in the database itself
- User authentication is performed by the database
- Eliminate dependency on the logins of the instance of SQL Server
- Increase database portability

SQL Server Audit

- Common Criteria Audit Option
- Using C2 Audit Mode
- Using SQL Trace for Auditing
- Using Triggers for auditing