Designing Security for Microsoft SQL Server 2005

- **Course Number:** 2787
- **Length:** 2 Day(s)

Certification Exam

This course will help you prepare for the following Microsoft Certified Professional exams:

- **MCITP Exam 70–443:** Designing a Database Server Infrastructure by Using Microsoft SQL Server 2005
- **MCITP Exam 70–444:** Optimizing and Maintaining a Database Administration Solution by Using Microsoft SQL Server 2005
- **MCITP Exam 70–447:** MCITP Upgrade for existing MCDBA Database Administrators.

Course Overview

This two-day course enables database administrators who work with enterprise environments to design security for database systems using Microsoft SQL ServerT 2005. The course emphasizes that students should think about the whole environment, which includes business needs, regulatory requirements, network systems, and database considerations during design. Students will also learn how to monitor security and respond to threats.

Prerequisites

Before attending this course, students must:

- Have basic knowledge of security protocols and how they work. For example, Windows NT LAN Manager (NTLM) or Kerberos.
- Have basic knowledge of public key infrastructure (PKI) systems. For example, how public and private keys work, strengths and weaknesses, and what they are used for.
- Have working knowledge of network architectures and technologies. For example, how a firewall works, how IPSec works in a networking context, and common vulnerability points.
- Have working knowledge of Active Directory directory service. For example, security models, policies, group policy objects (GPOs), and organizational units (OUs).
- Be able to design a database to third normal form (3NF) and know the tradeoffs when backing out of the fully normalized design (denormalization) and designing for performance and business requirements in addition to being familiar with design models, such as Star and Snowflake schemas.
- Have strong monitoring and troubleshooting skills.
- Have experience creating Microsoft Office Visio drawings or have equivalent knowledge.
- Have strong knowledge of the operating system and platform. That is, how the operating system integrates with the database, what the platform or operating system can do, interaction between the operating system and the database.
- Have basic knowledge of application architecture. That is, different methods of implementing security in an application, how applications can be designed in three layers, what applications can do, the interaction between applications and the database, and interactions between the database and the platform or operating system.
- Have knowledge about network security tools. For example, sniffer and port scanning. Must understand how they should be used.
- Be able to use patch management systems.
- Have knowledge of common attack methods. For example, buffer overflow, and replay attacks.
- Be familiar with SQL Server 2005 features, tools, and technologies.

- Have a Microsoft Certified Technology Specialist: Microsoft SQL Server 2005 credential or equivalent experience.

In addition, it is recommended, but not required, that students have completed:

- Course 2778: Writing Queries Using Microsoft SQL Server 2005 Transact-SQL.
- Course 2779: Implementing a Microsoft SQL Server 2005 Database.
- Course 2780: Maintaining a Microsoft SQL Server 2005 Database.

Audience

This course is intended for current professional database administrators who have three or more years of on-the-job experience administering SQL Server database solutions in an enterprise environment.

Course Outline

- Module 1 - Introduction to Designing SQL Server Security
- Lesson 1: Principles of Database Security
- Principle of Least Privileges
- International Common Criteria for Information Technology Security
- C2 Compliance Requirements
- Lesson 2: Designing a SQL Server Security Policy
- Benefits of a Security Policy
- Lesson 3: Monitoring SQL Server Security
- Auditing Tools
- Monitoring Tools
- Module 1 - Review
- Module 2 - Designing a SQL Server Systems Infrastructure Security Policy
- Lesson 1: Integration with Enterprise Authentication Systems
- Determining the Appropriate Enterprise Authentication Method
- Server-Level Security with Active Directory
- Guidelines for Implementing a Server-Level Security Policy
- High-Availability Solutions Security
- Best Practices
- Lesson 2: Windows Server-Level Security Policies
- Determining Service Accounts Permissions
- Identifying Required Windows Services
- Interacting with Network Firewalls
- Planning the Physical Security of Servers
- Lesson 3: Secure Communication Policy
- Choosing Network Libraries
- Encryption Methods
- Choosing an Appropriate Encryption Method
- Securing Communication with Endpoints
- Lesson 4: SQL Server Security Monitoring Standards
- Determining What to Monitor
- Determining the Classification System for Alerts
- Determining the Notification Policy
- Lab 1 Introduction
- Module 2 - Review
- Module 3 - Designing Security Policies for Instances and Databases
- Lesson 1: Instance-Level Security Policy

- Determining Authentication Modes and Login Security
- Securing the SQL Server Agent Service
- Maintaining Updated Hotfixes or Service Packs
- Lesson 2: Database-Level Security Policy
- Database Schemas
- Designing Database Schemas
- Designing Database Users' Privileges
- Securing Database-Level DDL Events
- Lesson 3: Object-Level Security Policy
- Designing a Permission and Data Access Strategy
- Securing Module Execution
- Designing a Security Policy for CLR Objects
- Lesson 4: Security Monitoring Standards for Instances and Databases
- Determining What to Monitor
- Determining the Classification System for Alerts
- Determining the Notification Policy
- Lab 2 Introduction
- Module 3 - Review
- Module 4 - Integrating Data Encryption into a Database Security Design
- Lesson 1: Securing Data with Encryption and Certificates
- What are Certificates?
- Determining Data Security Methods
- Lesson 2: Data Encryption Policies
- Impact of Data Encryption
- Lesson 3: Key Storage Method
- Selecting a Key Storage Method
- Lab 3 Introduction
- Module 4 - Review
- Module 5 - Designing a Security Exceptions Policy
- Lesson 1: Business and Regulatory Requirements
- Gathering Business and Regulatory Requirements
- Determine Variations
- Lesson 2: Exceptions and Their Impact
- Determine Possible Exceptions
- Evaluating the Impact of Exceptions
- Lab 4 Introduction
- Module 5 - Review
- Module 6 - Designing a Response Strategy for Threats and Attacks
- Lesson 1: Designing a Response Policy for Virus and Worm Attacks
- Threats by Viruses and Worms
- Best Practices
- Responding to Virus and Worm Attacks
- Lesson 2: Response Policy for Denial of Service Attacks
- Symptoms
- Possible Responses to a Denial of Service Attack
- Lesson 3: Response Policy for Internal and SQL Injection Attacks
- Responding to Internal Attacks
- Reducing the Likelihood of SQL Injection Attacks
- Lab 5 Introduction
- Module 6 - Review Closure