

# Module 1:

## Security and Privacy Concepts in SQL Server

### Contents

<b>Module Overview .....</b>	<b>1</b>
<b>Lesson 1: Overview of Security .....</b>	<b>2</b>
What is Security? .....	3
Threat Modeling .....	4
SQL Server Security Model .....	6
Levels of Security in SQL Server .....	7
<b>Lesson 2: Overview of Privacy .....</b>	<b>8</b>
What is Privacy? .....	9
Balance between Privacy and Security .....	10
SQL Server and Data Privacy .....	11
<b>Lesson 3: Monitoring User Activity .....</b>	<b>12</b>
Auditing Basics .....	13
Access Controls .....	15
CSI SQL Server .....	16
<b>Lesson 4: Using SQL Server Tools .....</b>	<b>17</b>
Overview of SQL Tools .....	18
SQL Server Configuration Manager (SSCM) .....	19
SQL Server Management Studio (SSMS) .....	21
<b>Summary .....</b>	<b>22</b>



# Module Overview

- 
- Overview of Security
  - Overview of Privacy
  - Monitoring User Activity
  - Using SQL Server Tools

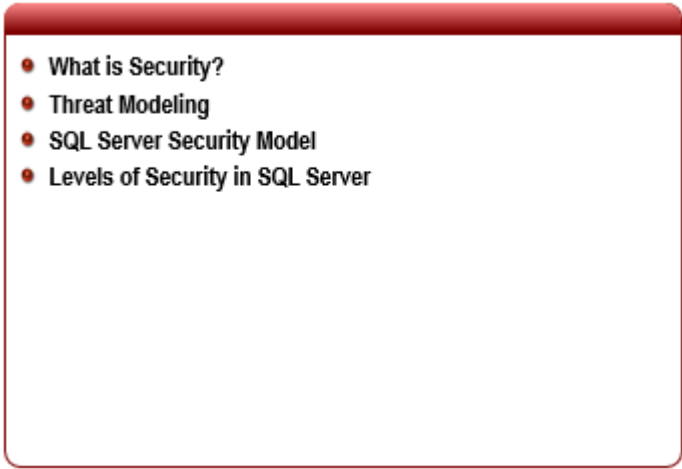
This module deals with the basics of security and privacy on SQL Server database server. You will learn what security is and why it is so important. Also, you will see that SQL Server has different levels (layers) of security; where each level is independent. You will get basic information about data auditing and understand the difference between security and privacy. Those two elements are most of the time in conflict with each other. Finally, you will see what SQL Server native tools are available to deal with security and privacy elements.

## Objectives

After completing this module, you will be able to:

- Understand the basic concepts of security and privacy on SQL Server
- Know the difference between security and privacy
- Understand the need for data auditing
- Recognize the correct tools for achieving all security tasks

# Lesson 1: Overview of Security

- 
- What is Security?
  - Threat Modeling
  - SQL Server Security Model
  - Levels of Security in SQL Server

---

In this lesson, you will learn what security is and why it is so important in the modern information age, and especial in database environments. Good security is based on threat modeling, which is the process of identifying all threats to your systems: database, software, network, etc.

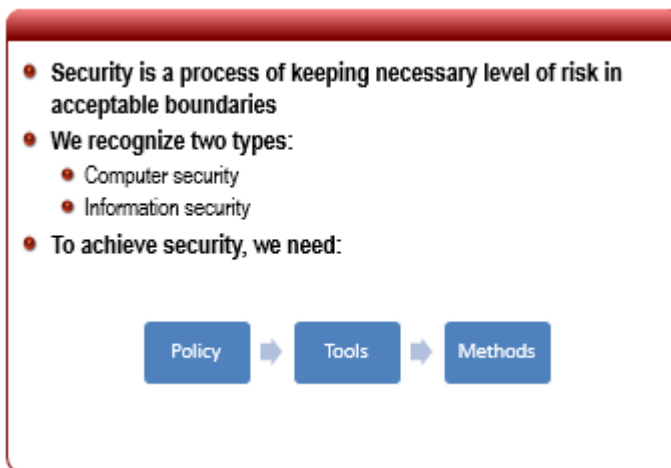
SQL Server security model is spread through different security levels. This lesson will teach you to recognize and understand them.

## Objectives

After completing this lesson, you will be able to:

- Recognize security
- Understand threat modeling
- Understand SQL Server security model
- Understand the levels of security in SQL Server

## What is Security?

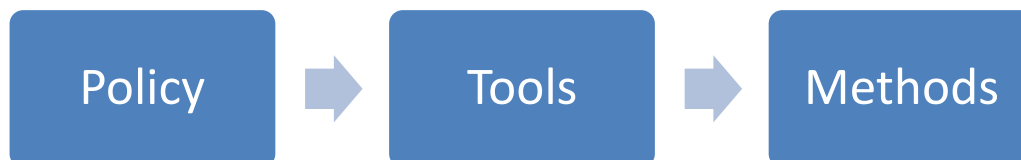


Security is a process of keeping necessary level of risk in acceptable boundaries. That means, security is a continual process and not a final state. An organization or institution cannot consider itself “secure” upon completion of a security check; the process needs to be continual. Security requires people, knowledge, and resources which are based on the following security trends:

- Computer security
- Information security

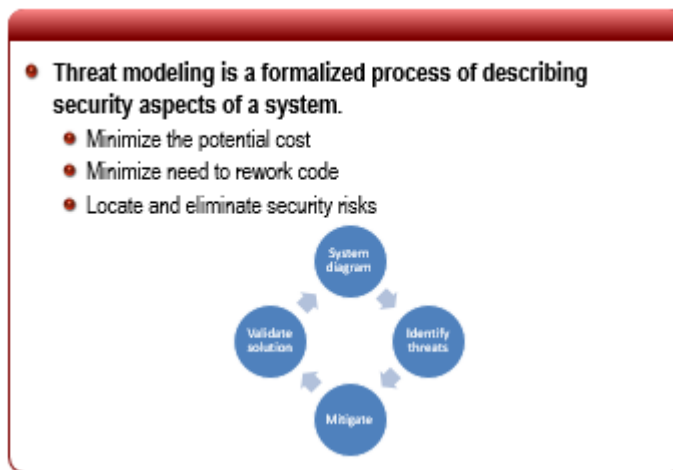
Computer security deals with hardware, software, and communication technologies. On the other hand, information security is part of computer security, but is focused on data security. SQL Server is a database management system involving data or information. Therefore, this course is focused on the information security trend. It is very important to note that a database is the last line of the defense in your IT infrastructure. Networks, firewalls, and operating systems will all be breached before an attacker has access to a database. Your job is to prevent unauthorized access to your corporate and sensitive data.

To achieve this, we need the following:

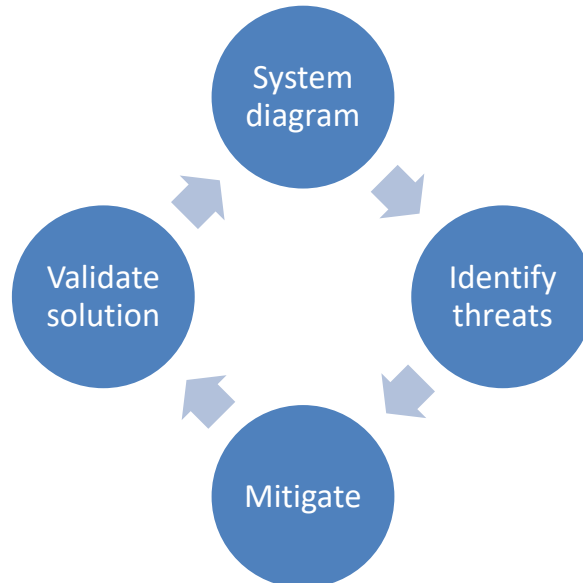


Policy, the starting point of the security process, involves the rules which can be different based on environments. By tools, we mean concrete software solutions such as applications or programming libraries where we can find necessary resources. Last are the methods which require knowledge. This course is about methods in the security process.

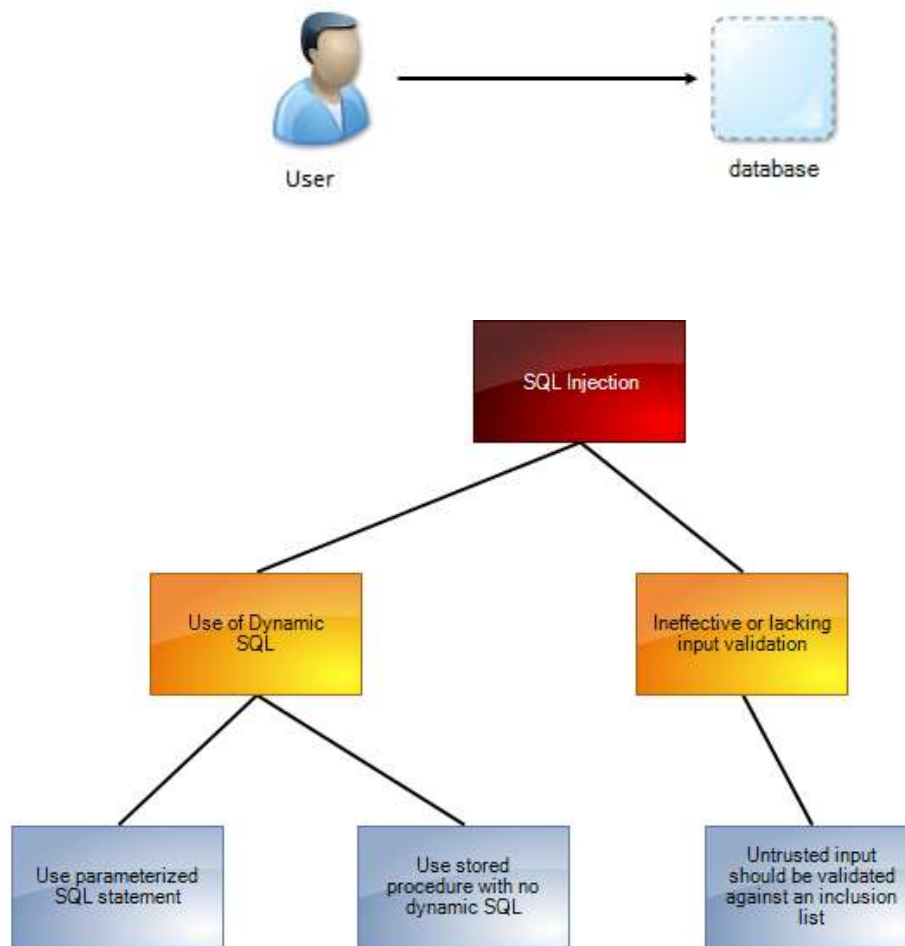
## Threat Modeling



Threat modeling is a formalized process of describing security aspects of a system. The threat modeling process often begins with a diagram of the system being modeled. It can help organizations to minimize the potential cost and need to rework code while in development or in post-production support. In a nutshell, the threat modeling process is involved in all phases of software development.

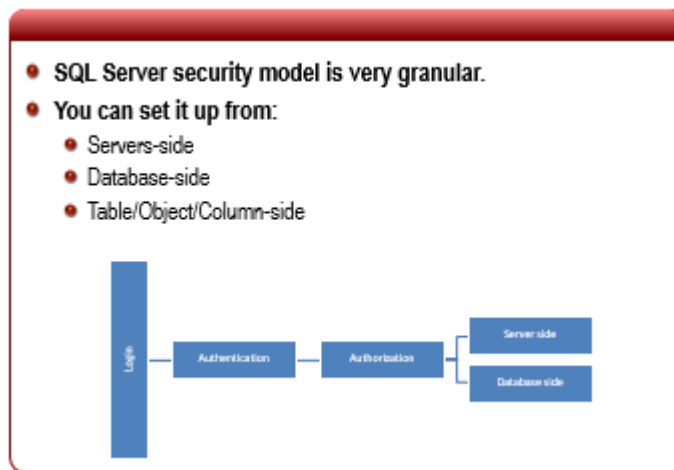


In the first phase, a system diagram needs to be created, similar to a classical software engineering process. Then, threats need to be identified in all aspects of the system. More precise detail is better. Even simple tasks like inserting a new record into a database can be a potential threat. In the mitigate phase, we need to eliminate/mitigate threats by using tools and methods. The final phase is the validating of solution phase. Threat modeling is a repeated cycle until the goal is achieved.

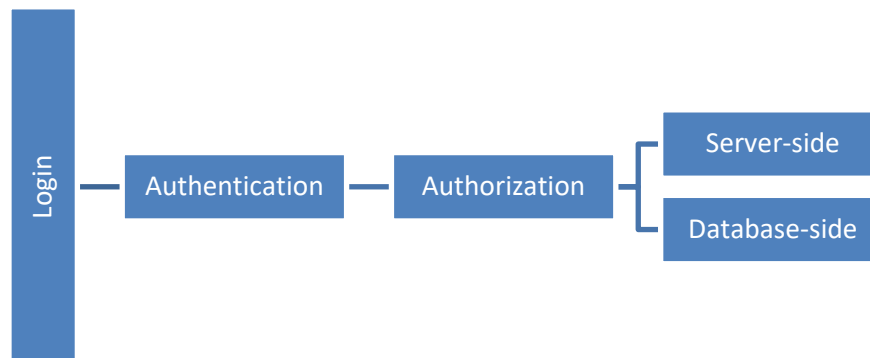


Threat modeling is the starting point for every security solution. The outcome is comprehensive documentation which is based on that development team's needs to implement all countermeasures. The database team (developers and administrators) needs to secure the database layer in every access point.

## SQL Server Security Model



SQL Server security model is very granular. It means that you can set it up from highest level of security (server -side) to the lowest level of security (table- or column- side). But before we start talking about levels of security, we need to look at the bigger picture and understand the basics.



- User needs to pass authentication and identify him/herself to SQL Server.
- If this step is correct, then SQL Server looks at the permissions to check the level of authorization for the user. If the user is not authorized, then access is denied.
- Based on permission level, the user can use the server-side or database-side or both together.

*Note: There is a difference between “logins” and “users” on SQL Server.*





## Levels of Security in SQL Server

- **Levels of security are:**
  - Principals
  - Server-level of security
  - Database-level of security
  - Securables
- **Principals are entities that can request SQL Server resources**
- **Server-level of security helps you to manage the permissions on a server**
- **Database-level of security helps you to manage the permissions on a database**
- **Securables request access to the resources**

Based on the model (lesson before), we can identify elements and levels of security in SQL Server. Understanding how to identify elements and levels of security is important because they are all required when dealing with real life security situations. Mistakes in this part can be hard to detect later in the deployment and maintenance phases because they only become visible after an incident.

The levels of security are:

- Principals
- Server-level of security
- Database-level of security
- Securables

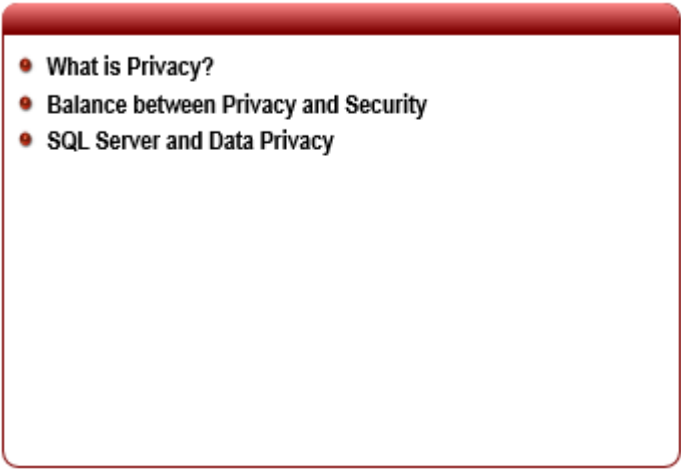
Principals are entities that can request SQL Server resources. Like other components of the SQL Server authorization model, principals can be arranged in a hierarchy. The scope of influence of a principal depends on the scope of the definition of the principal (Windows, server, database), and whether the principal is indivisible or a collection. A Windows Login is an example of an indivisible principal, and a Windows Group is an example of a principal that is a collection. In short, a principal is anything that requires access to SQL Server resources.

Server-level of security are used to manage the permissions on a server. These roles are security principals that group other principals. Server-level roles are server-wide in their permissions scope. Roles are like groups in the Windows operating system.

Database-level of security involves two types of database-level roles in SQL Server: fixed database roles that are predefined in the database, and flexible database roles that you can create. Fixed database roles are defined at the database-level and exist in each database. Every database user belongs to the public database role.

Securables are the resources to which the SQL Server Database Engine authorization system regulates access. For example, a table is a securable. Some securables can be contained within others which create nested hierarchies called "scopes" that can themselves be secured. The securable scopes are server, database, and schema.

## Lesson 2: Overview of Privacy

- 
- What is Privacy?
  - Balance between Privacy and Security
  - SQL Server and Data Privacy

---

In this lesson, you will learn what privacy is and why it is so important in modern information systems. Most software are built on top of a database which houses all business process data. As such, this portion of the course will focus on data privacy.

### Objectives

After completing this lesson, you will be able to:

- Understand what is data privacy
- Distinguish between security and privacy
- Recognize privacy elements in SQL Server

## What is Privacy?



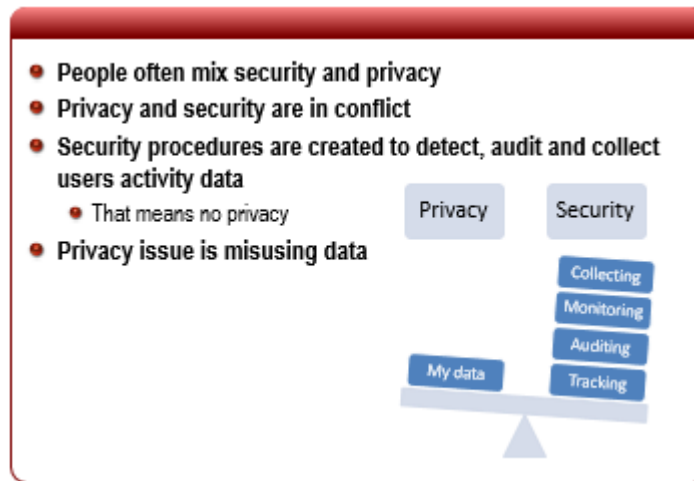
Privacy is top of mind for every individual: when, how and how much information will be available for storing and exchange between systems. Examples of violating privacy are not rare; on the contrary, the numbers of accidental and intentional violations are increasing. Usage examples of illegally collected information can be easily found.

Privacy is defined by state laws, regulations, policies and other legal documents. Keeping privacy in an application level is not a difficult task because it is implemented in the user interface. But when looking at the privacy issue from a database perspective, a whole new viewpoint is available. That is because database users with high access rights can compromise user data integrity and privacy. For that reason, it is important to pay attention to privacy issues at the database-level.

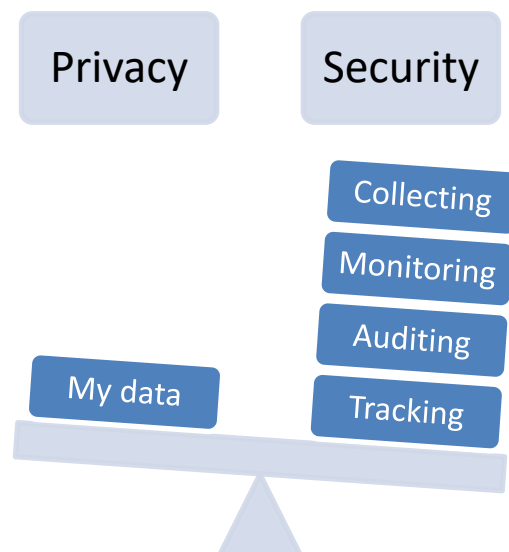
A privacy-conscious database should implement the following requirements:

1. Purpose specification. For personal information stored in the database, the purposes for which the information has been collected shall be associated with that information.
2. Consent. The purposes associated with personal information shall have the consent of the owner of the personal information.
3. Limited collection. The personal information collected shall be limited to what is necessary for accomplishing the specified purposes.
4. Limited use. The database shall run only those queries that are consistent with the purposes for which the information has been collected.
5. Limited disclosure. The personal information stored in the database shall not be communicated outside the database for purposes other than those for which there is consent from the owner of the information.
6. Limited retention. Personal information shall be retained only as long as necessary for the fulfillment of the purposes for which it has been collected.
7. Accuracy. Personal information stored in the database shall be accurate and up-to-date.
8. Safety. Personal information shall be protected by security safeguards against theft and other misappropriations.
9. Openness. An owner shall be able to access all information about the owner stored in the database.
10. Compliance. An owner shall be able to verify compliance with the above principles. Similarly, the database shall be able to address a challenge concerning compliance.

## Balance between Privacy and Security



People often mix security and privacy in information system environments. It is mistakenly assumed that when dealing with security elements, privacy issues are automatically solved. Privacy and security are in conflict with each other.



All standard security procedures are created to detect, audit and collect users' activity data. That means no privacy. This paradox situation is solvable with precise and transparent information to the end user (i.e. what kind of data, when and how will it be collected).

Another big issue with privacy is the misuse of data. For example, when individuals, groups, and whole organizations use user data without the owner's knowledge.

## SQL Server and Data Privacy

- **SQL Server can handle data privacy on many levels**
  - Server-side security (fixed or custom roles)
  - Database-side security (fixed or custom roles)
  - Database objects (views, stored procedures)
  - Using built-in cryptographic features in SQL Server
- **How to limit users with high access right?**
- **Cryptography**



SQL Server can handle data privacy on many levels. Depending on the kind of feature used and its location, nearly all ten principles of privacy can be implemented. The following elements, in SQL Server, can be used to protect a user's privacy:


- Server-side security (fixed or custom roles)
- Database-side security (fixed or custom roles)
- Database objects (views, stored procedures)
- Using built-in cryptographic features in SQL Server

*Note: List contains some security elements that can also be used to protect privacy.*



The major issue in privacy is how to limit users, with high access right, from viewing other users' private data. Cryptography is the only feature in SQL Server that can limit that kind of user.

## Lesson 3: Monitoring User Activity

- 
- Auditing Basics
  - Access Control
  - CSI SQL Server

---

Contemporary information systems such as eLearning, eUnivesity, eVoting, eHealth, are frequently used and misused for irregular data changes known as data tampering. Those facts force us to reconsider our security measures and find a way to improve them. Proving a computer crime requires very complicated processes which are based on digital evidence collecting, forensic analysis, and an investigation process. Forensic analysis of database systems is a very specific and demanding task.

Data tampering can be done with unauthorized access and, in some cases, by authorized users. Results of tampering can be unpleasant for businesses and their clients. There are many reasons and areas where someone could attempt to make malicious data modification with authorized and/or unauthorized access.

### Objectives

After completing this lesson, you will be able to:

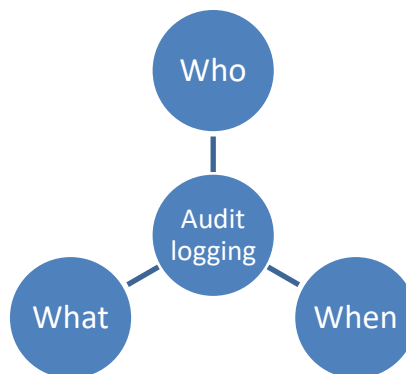
- Understand auditing basics
- Define Access Control
- Get basic facts about forensic analysis

## Auditing Basics

- Modern information society has a strong need to provide a secure data storage environment.
- A single change in a database can make a criminal from an ordinary citizen.
- Auditing process monitors user activity



There is only one way to provide valid forensic analysis of a database. That process requires creating an audit logging in all aspects of an information system. Based on that, a data investigation process can reconstruct what has really happened. Depending on the application architecture (i.e. web, desktop, or combined), there is a wide range of data that is necessary to be collected. For example: user name, IP address, time stamp, etc. But not all data is required in each situation. The IP address of the internet provider is not needed in a classical desktop environment. In other situations, the IP address of the internet provider can be crucial in determining a geographical location of the criminal. The basic task of audit logging is to give answers to three questions.



Depending on how much detail is required regarding changed data, audit logging can be divided in two groups: simple and advanced access control.

Simple access control collects basic data about actions in information systems and gives answers to the “Who” and “When” questions. It is important to note that simple access control is not enough to provide data for valid forensic analysis. The bottom line is that every system requires at least simple access control.

On the other hand, there are systems where integrity, data precisions, privacy, and security are the scope of the audit log. Advanced access control is ideal for such systems. In these environments,

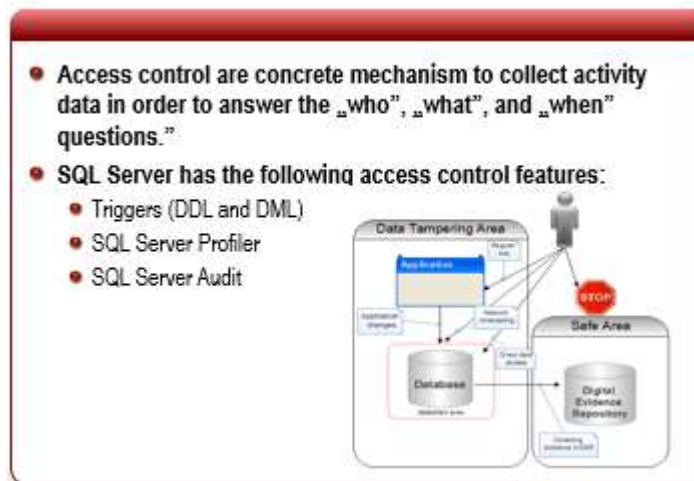
the “Who” and “When” questions are not enough. The biggest issue is the “What” question. The table below shows a list of activities for implementing advanced access control.

Who	When	What
Identity	Log in time	Data about data modifications
Location	Log out time	Data about data scheme modifications
Operating system and application	Timestamp	Cryptographic hash checksum

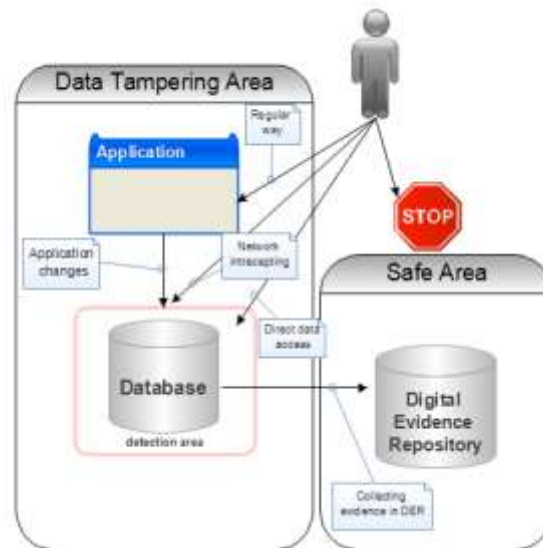
*SQL Server provides elements to answer all three questions.*



## Access Controls



Access controls are concrete mechanisms to collect activity data in order to answer the “Who”, “What” and “When” questions.



It can be noted that there are many places to intercept and tamper with data. SQL Server has the following access control features:

- Triggers (DDL and DML)
- SQL Server Profiler
- SQL Server Audit

## CSI SQL Server

- Critical part of digital evidence collected is data validity
- Digital forensics is based on the confiscation of digital evidence
- The investigation process and the forensic analysis on the database-level are extremely difficult



Data validity is the critical part in the collection of digital evidence. What if someone, with proper access right, accessed tables with digital evidences and tampered with the data? If the audit log of deleted records is deleted or tampered, the validity of evidence is compromised. Such tampering is very difficult to detect.

Digital forensics involves: confiscating digital evidence (i.e. PC, laptops, cell phones, USB memory modules, etc.), preserving, examining, analyzing, and reporting the facts.


The investigation process and forensic analysis, at the database-level, is extremely difficult. As an illustration, we will examine a hypothetical situation.

There was a data breach in a bank information system. Unauthorized access to clients' banking accounts has resulted in money problems for a certain number of clients. Somehow, the clients have a minus on their credit card accounts. Bank personnel are unable to do anything at the internal level. Clients decide to press charges. The prosecution department send a team of digital forensics who are tasked with collecting all evidence about suspicious transactions, examining such evidence, and making a report to the court of law. The team needs to follow a precisely defined procedure to provide valid court evidence, but the team has encountered some very serious problems in the early phase of the investigation. The first phase is collecting and copying data. In the case of a bank information system, those tasks are very difficult to accomplish. Here are some key points:

- Bank information system is based on a distributed database architecture
- Size of the database is over 1 TB
- To copy all disks with images of data, the system needs to be stopped
- Bank policy does not allow stopping of the system
- Backing up media is not enough because the team does not know the timeframe of the event

***This example clearly describes a situation where classical digital forensics is almost useless.***

## Lesson 4: Using SQL Server Tools

- 
- Overview of SQL Tools
  - SQL Server Configuration Manager
  - SQL Server Management Studio

---

In this lesson, you will learn the basics about built-in tools that can be used to achieve security tasks and procedures in your SQL Server environment.

### Objectives

After completing this lesson, you will be able to:

- Identify the set of SQL Server tools
- Understand what is SQL Server Configuration Manager
- Understand what is SQL Server Management Studio

## Overview of SQL Tools

- **We have tools for:**
  - Setup, configuration, server/database-side security and cryptographic elements
- **Setup procedure**
  - During installation
- **SQL Server Configuration Manager**
  - Preparing SQL Server for accessing
- **SQL Server Management Studio**
  - All other security tasks

What kind of tool you will use is dependent on the goal that you are trying to achieve (i.e. setup, configuration, server/database-side security, or cryptographic elements).

The task requiring the configuration of the initial security elements during installation can be done during the setup procedure.

Initial configuration after installation can be done through the SQL Server Configuration Manager.

All other task (server/database-side security, cryptographic elements, etc.) can be done using SQL Server Management Studio.

*Note: All tasks mentioned above can be done through the SQL Server console tool.*

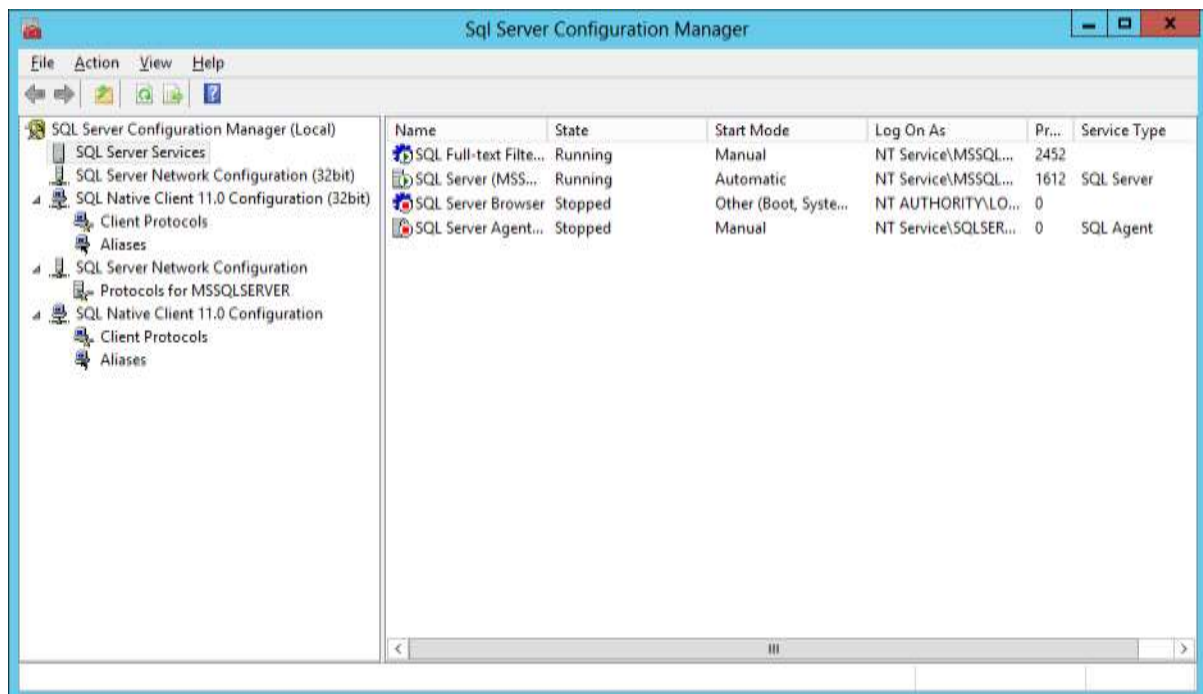


## SQL Server Configuration Manager (SSCM)

- Microsoft Management Console snap-in
- Tool to manage the services associated with SQL Server
- Configure the network protocols
- Manage the network connectivity configuration

The SQL Server Configuration Manager (SSCM) is a tool to: manage the services associated with SQL Server, configure the network protocols used by SQL Server, and manage the network connectivity configuration from SQL Server client computers.

The SSCM is a Microsoft Management Console snap-in that is available from the Start menu, or can be added to any other Microsoft Management Console display.



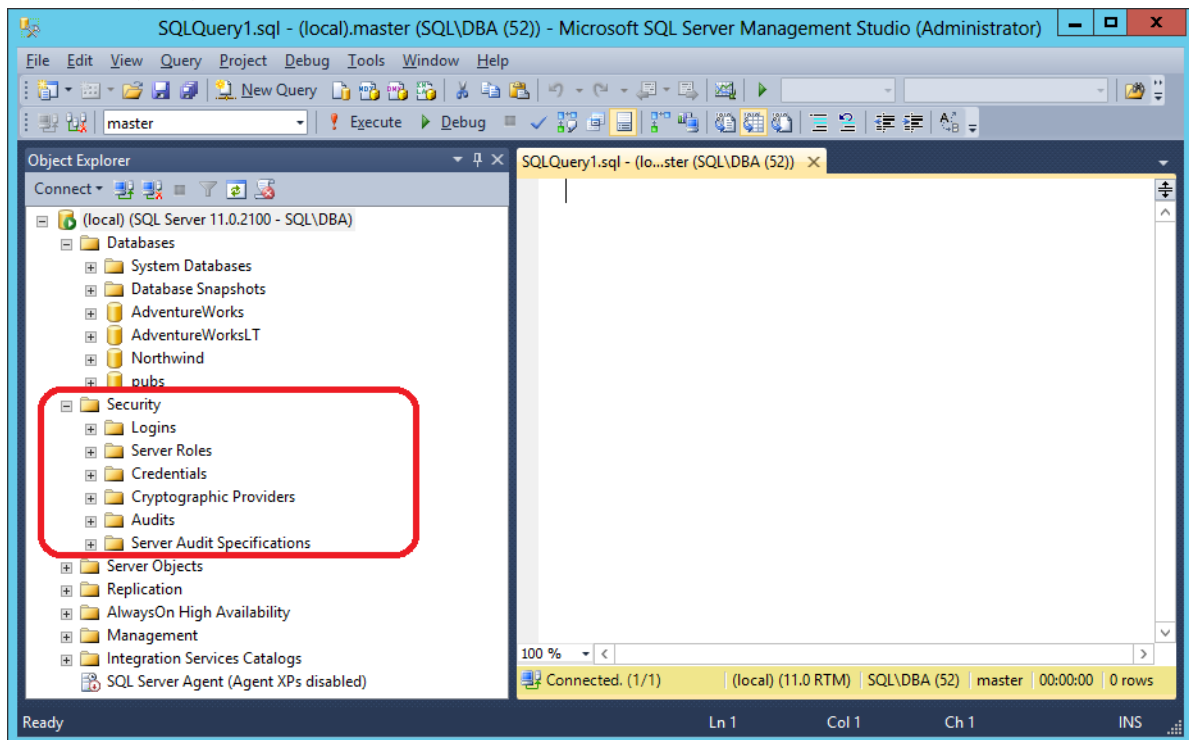
- Use the SSCM to:
  - start, pause, resume, or stop the services;
  - view service properties; or
  - change service properties.
- Use the SSCM to start the Database Engine using the startup parameters.

The SSCM allows you to configure server and client network protocols and connectivity options. After the correct protocols are enabled, you usually do not need to change the server network connections.

## SQL Server Management Studio (SSMS)

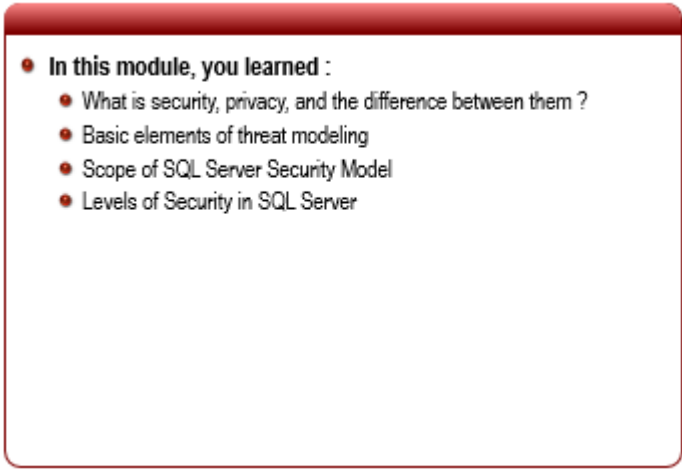


The SQL Server Management Studio (SSMS) provides a rich environment for managing and developing queries in SQL Server. Also, all security tasks can be done with SSMS Graphical User Interface (GUI).



As can be seen in the above figure, some of the security elements are marked. The figure does not show all of the security elements as there are too many, but all of them are topics of this course.

## Summary

- 
- **In this module, you learned :**
    - What is security, privacy, and the difference between them ?
    - Basic elements of threat modeling
    - Scope of SQL Server Security Model
    - Levels of Security in SQL Server

---

Database and data security are one of the most critical parts in modern IT society. In this lesson, you have learned the basic concepts of security and privacy and also how to identify the difference between them.

Good and detailed security analysis, known as threat modeling, is an important part in the process of achieving security.

Now, you understand why it is so important to create a data auditing system and where potential problems may arise, specifically in the area of digital forensics.

Finally, you can identify the correct tool for a specific security task.

### Objectives

After completing this module, you learned:

- What is security, privacy, and the difference between them
- Basic elements of threat modeling
- Scope of a SQL Server Security Model
- Levels of security in SQL Server