Database Security and Auditing: Protecting Data Integrity and Accessibility

Chapter 1
Security Architecture

Introduction

- Security violations and attacks are increasing globally at an annual average rate of 20%.
- You serve as a database administrator to enforce security policies. Responsibilities can be:
  - Design and implement a new DB security policy.
  - Enforce a stringent security policy.
  - Implement functional specification of a module, i.e. encrypt the stored data, replace sensitive data using the data masking pack.

Introduction

- Security measures
  - Prevent physical access to the servers where the data resided.
  - Operating systems require authentication of the identity of computer users.
  - Implement security models that enforce security measures.
- DBA should manage databases and implement security policies to protect the data (assets).

Objectives

- Define security
- Describe an information system and its components
- Define database management system functionalities
- Outline the concept of information security

Objectives (continued)

- Identify the major components of information security architecture
- Define database security
- List types of information assets and their values
- Describe security methods

Security

- Database security: degree to which data is fully protected from tampering or unauthorized acts
- Comprises information system and information security concepts

Information Systems

- Wise decisions require:
  - Accurate and timely information
  - Information integrity
- Information system: comprised of components working together to produce and generate accurate information
- Categorized based on usage: low-level, mid-level and high-level

Information Systems (continued)

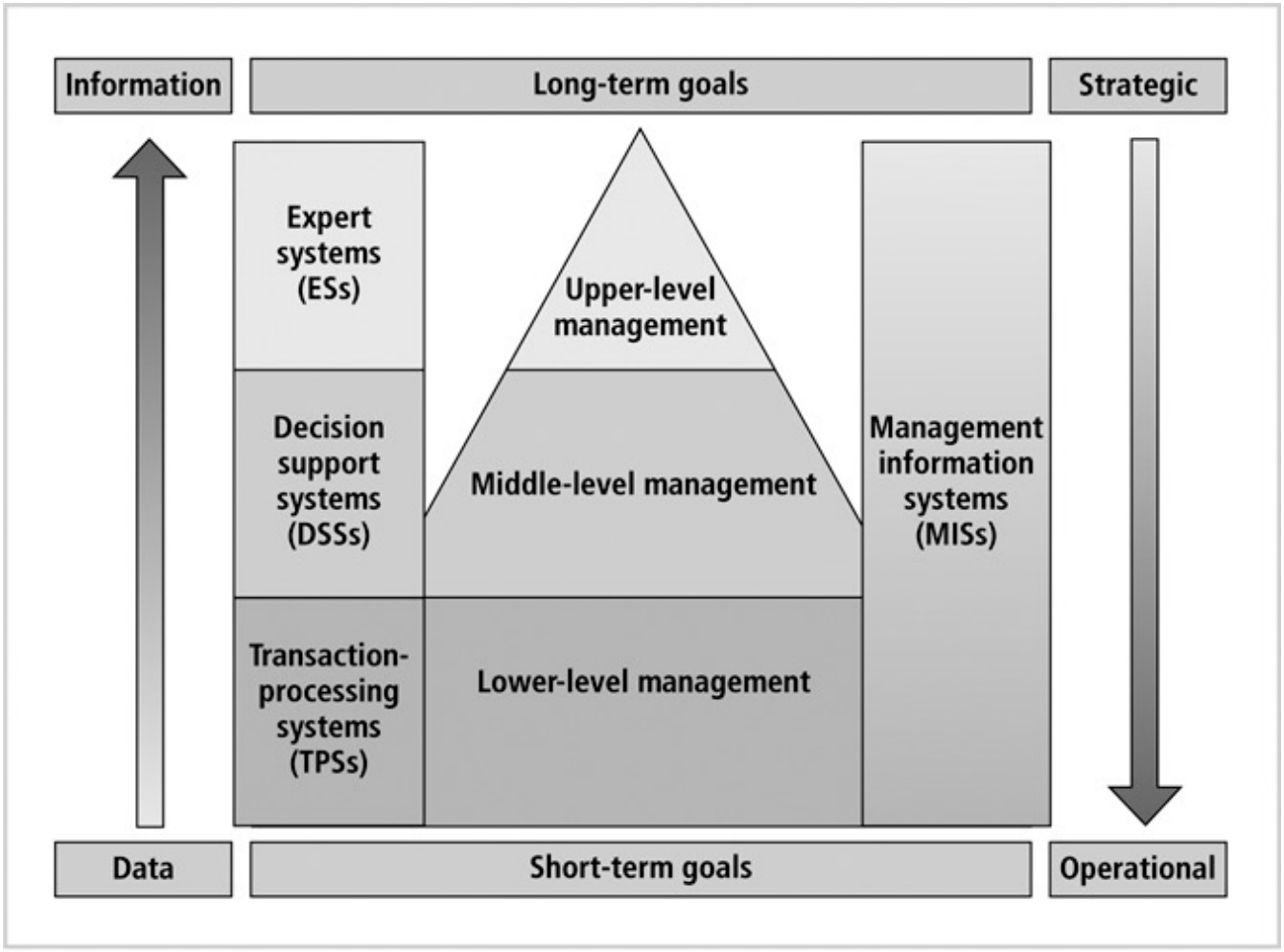

FIGURE 1-1 Typical use of system applications at various management levels

Information Systems (continued)

TABLE 1-1 Characteristics of information system categories

Category	Acronym	Characteristics	Typical Application System
Transaction-processing system	TPS	■ Also known as online transaction processing (OLTP) ■ Used for operational tasks ■ Provides solutions for structured problems ■ Includes business transactions ■ Logical component of TPS applications (derived from business procedures, business rules, and policies)	■ Order tracking ■ Customer service ■ Payroll ■ Accounting ■ Student registration ■ Car sales

Information Systems (continued)

TABLE 1-1 Characteristics of information system categories (continued)

Category	Acronym	Characteristics	Typical Application System
Decision support system	DSS	■ Deals with nonstructured problems and provide recommendations or answers to solve these problems ■ Is capable of performing "What-if?" analysis ■ Contains a collection of business models ■ Is used for tactical management tasks	■ Risk management ■ Fraud detection ■ Sales forecasting ■ Case resolution

Expert system	ES	■ Captures reasoning of human experts
		■ Executive expert systems (ESSs) are a type of expert system used by top-level management for strategic management goals
		■ A branch of artificial intelligence within the field of computer science studies
		■ Software consists of:
		  ■ Knowledge base
		  ■ Inference engine
		  ■ Rules
		■ People consist of:
		  ■ Domain experts
		  ■ Knowledge engineers
		  ■ Power users
			■ Virtual university simulation
			■ Financial enterprise
			■ Statistical trading
			■ Loan expert
			■ Market analysis

Information Systems (continued)

- Information system components include:
  - Data
  - Procedures
  - Hardware
  - Software
  - Network
  - People

Information Systems (continued)

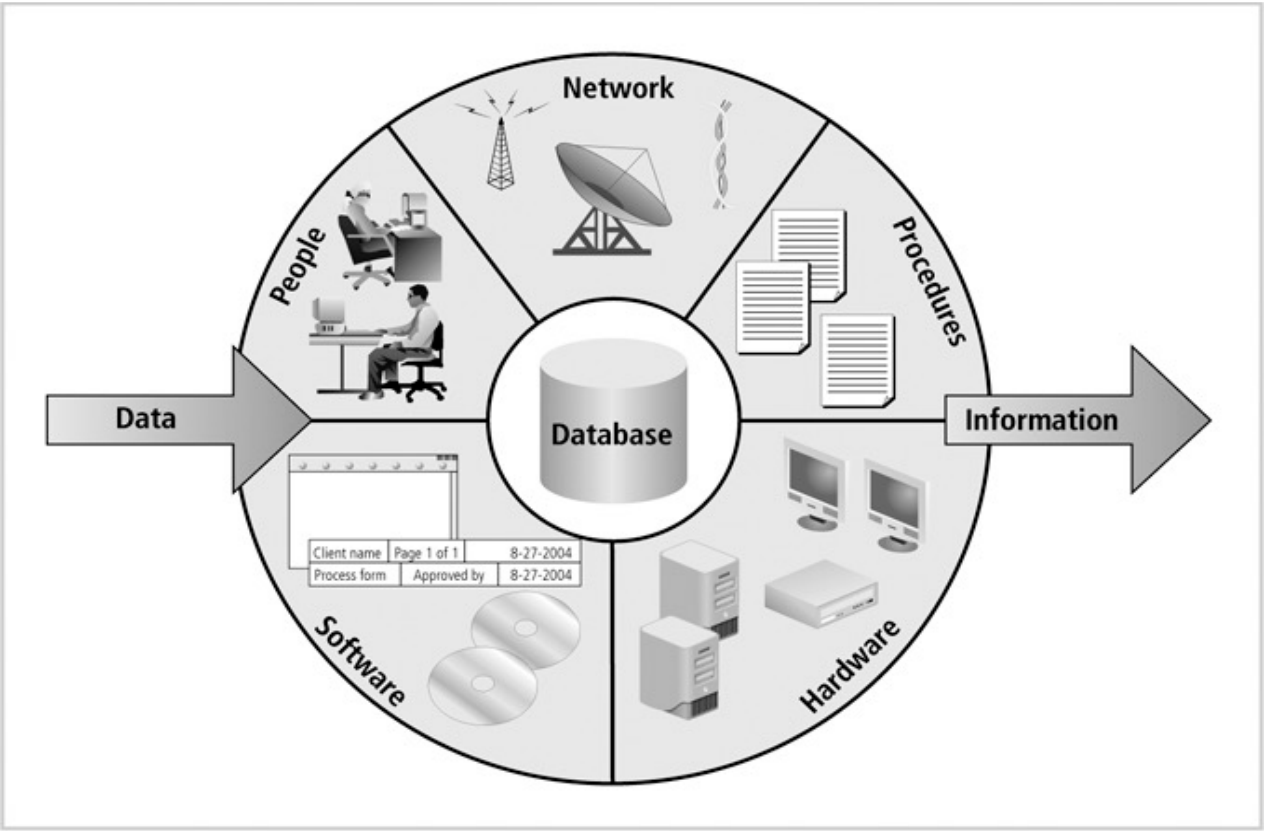

FIGURE 1-2 Information system components

Information Systems (continued)

- Client/server architecture:
  - Based on the business model
  - Can be implemented as one-tier; two-tier; n-tier
  - Composed of three layers
- Tier: physical or logical platform
- Database management system (DBMS): collection of programs that manage database

Information Systems (continued)

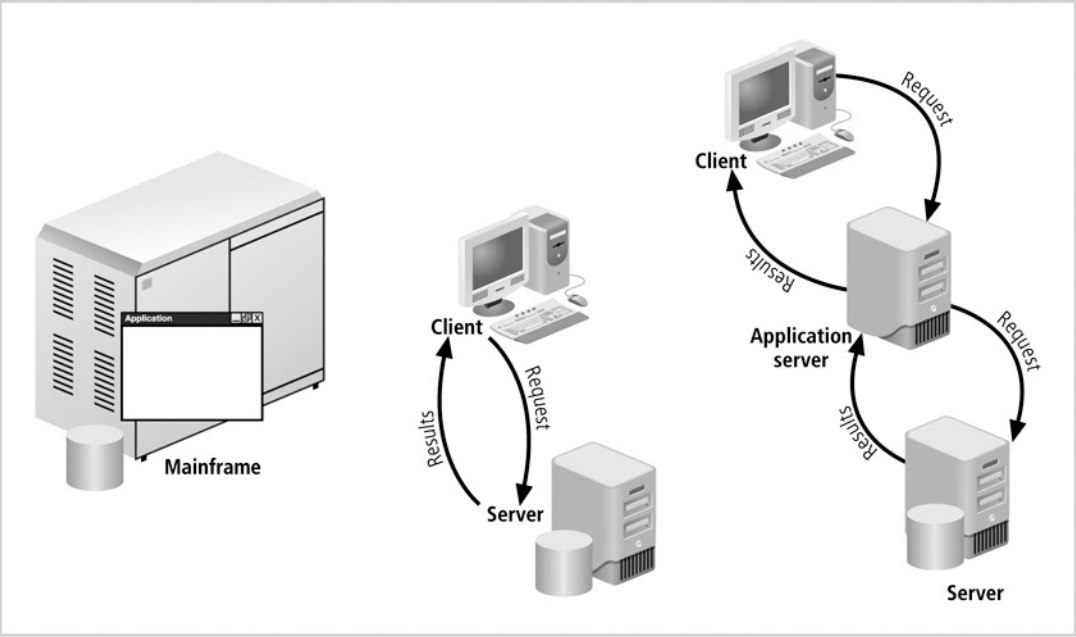

FIGURE 1-3 Examples of different client/server tier design

Database Management

- Essential to success of information system
- DBMS functionalities:
  - Organize data
  - Store and retrieve data efficiently
  - Manipulate data (update and delete)
  - Enforce referential integrity and consistency
  - Enforce and implement data security policies and procedures
  - Back up, recover, and restore data

Database Management (continued)

- DBMS components include:
  - Data
  - Hardware
  - Software
  - Networks
  - Procedures
  - Database servers

Database Management (continued)

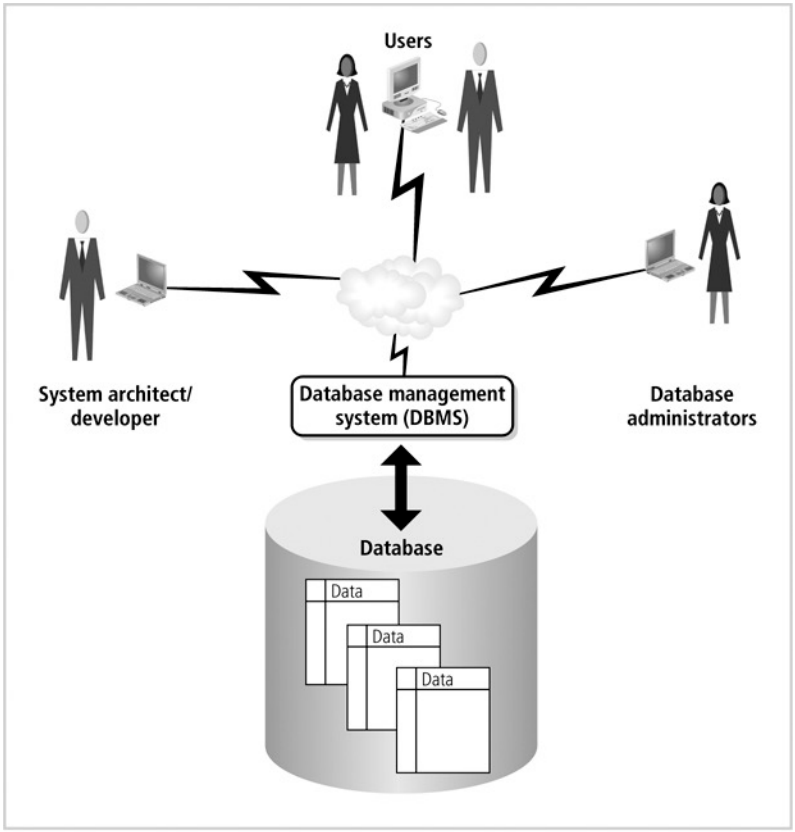

FIGURE 1-4 Database and DBMS environment

Information Security

- Information is one of an organization's most valuable assets
- Information security: consists of procedures and measures taken to protect information systems components
- C.I.A. triangle: confidentiality, integrity, availability
- Security policies must be balanced according to the C.I.A. triangle

Information Security (continued)

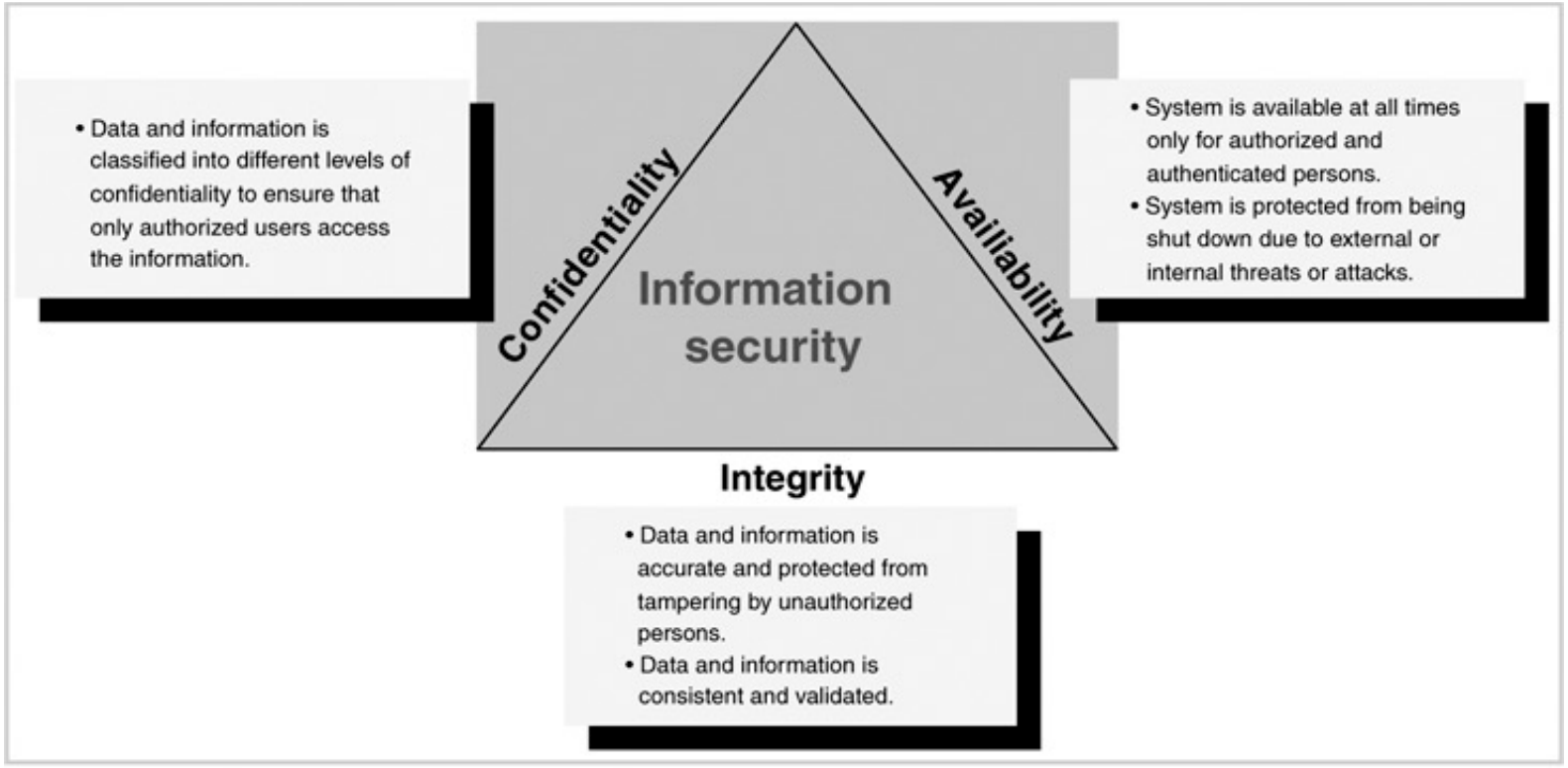

FIGURE 1-5 Information security C.I.A triangle

Confidentiality

- Addresses two aspects of security:
  - Prevention of unauthorized access
  - Information disclosure based on classification
- Classify company information into levels:
  - Each level has its own security measures
  - Usually based on degree of confidentiality necessary to protect information

Confidentiality (continued)

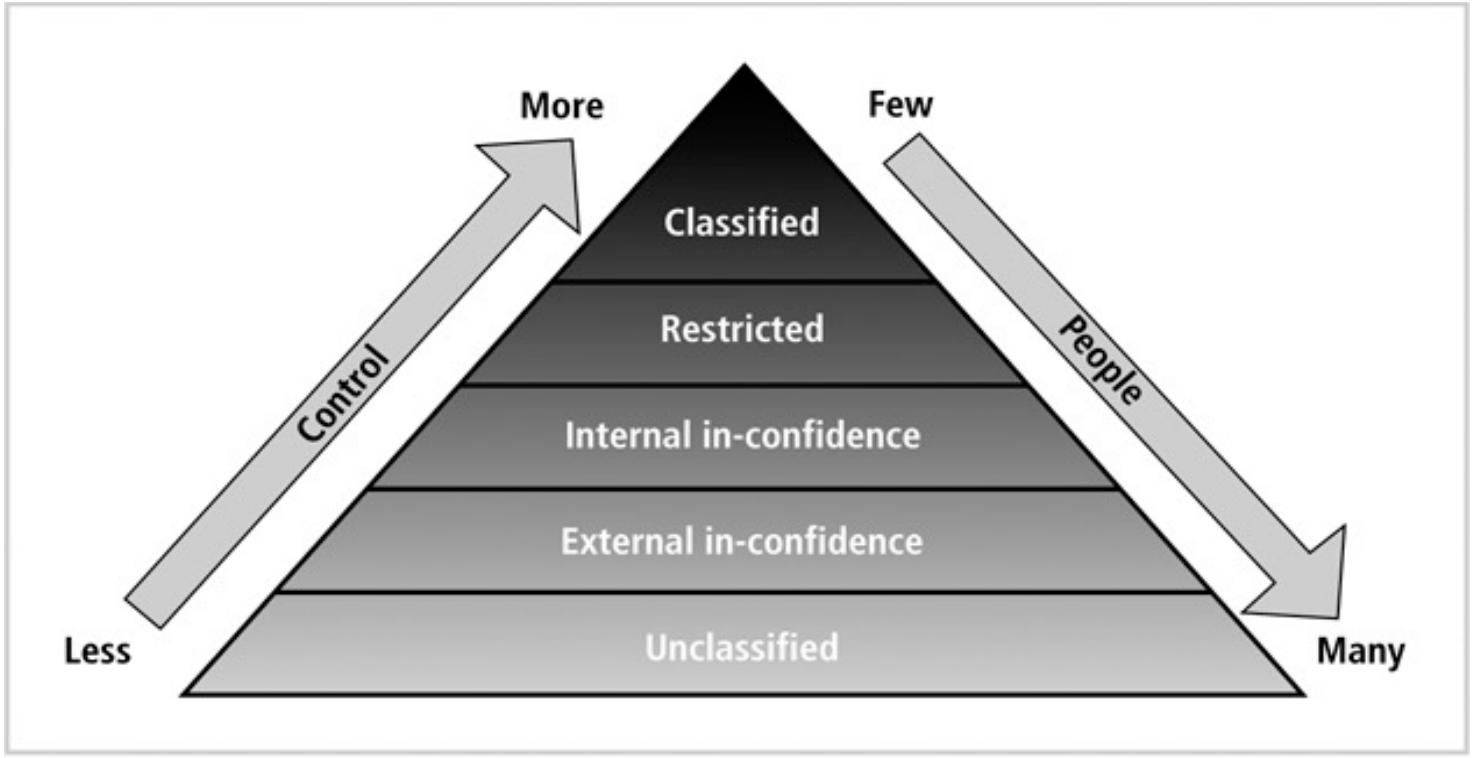

FIGURE 1-6 Confidentiality classification

Integrity

- Consistent and valid data, processed correctly, yields accurate information
- Information has integrity if:
  - It is accurate
  - It has not been tampered with
- Read consistency: each user sees only his changes and those committed by other users

Integrity -- Example

- Employee A learns that his adversarial coworker is earning higher salary then he is.
- A access an application program by accounting dept and manipulates the vacation hours and overtime hours of his colleague.
- Two security violations:
  - Confidential data is disclosed inappropriately
  - An application to modify data was access inappropriately.
- There should be a control to cross-check overtime hours against actual time cards, computes vacation hours, and verifies entered values. If they are different, the app requires override from another person. (data validation)

TABLE 1-2 Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Invalid data	Indicates that not all the entered and stored data is valid without exception; checks and validation processes (known as database constraints) that prevent invalid data are missing.	■ User enters invalid data mistakenly or intentionally. ■ Application code does not validate inputted data.
Redundant data	Occurs when the same data is recorded and stored in several places; this can lead to data inconsistency and data anomalies.	■ Faulty data design that does not conform to the data normalization process. (**Normalization** is a database design process used to reduce and prevent data anomalies and inconsistencies.)

Integrity (continued)

TABLE 1-2 Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Inconsistent data	Occurs when redundant data, which resides in several places, is not identical.	■ Faulty database design that does not conform to the data normalization process.
Data anomalies	Exists when there is redundant data caused by unnormalized data design; in this case, data anomalies occur when one occurrence of the repeated data is changed and the other occurrences are not.	■ Faulty data design that does not conform to the data normalization process.

Integrity (continued)

TABLE 1-2 Degradation of data integrity (continued)

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Data read inconsistency	Indicates that a user does not always read the last committed data, and data changes that are made by the user are visible to others before changes are committed.	■ DBMS does not support or has weak implementation of the read consistency feature.
Data nonconcurrency	Means that multiple users can access and read data at the same time but they lose read consistency.	■ DBMS does not support or has weak implementation of the read consistency feature.

Availability

- Systems must be always available to authorized users
- Systems determines what a user can do with the information

Availability (continued)

- Reasons for a system to become unavailable:
  - External attacks and lack of system protection
  - System failure with no disaster recovery strategy
  - Overly stringent and obscure security policies
  - Bad implementation of authentication processes

Information Security Architecture

- Protects data and information produced from the data
- Model for protecting logical and physical assets
- Is the overall design of a company's implementation of C.I.A. triangle

Information Security Architecture (continued)

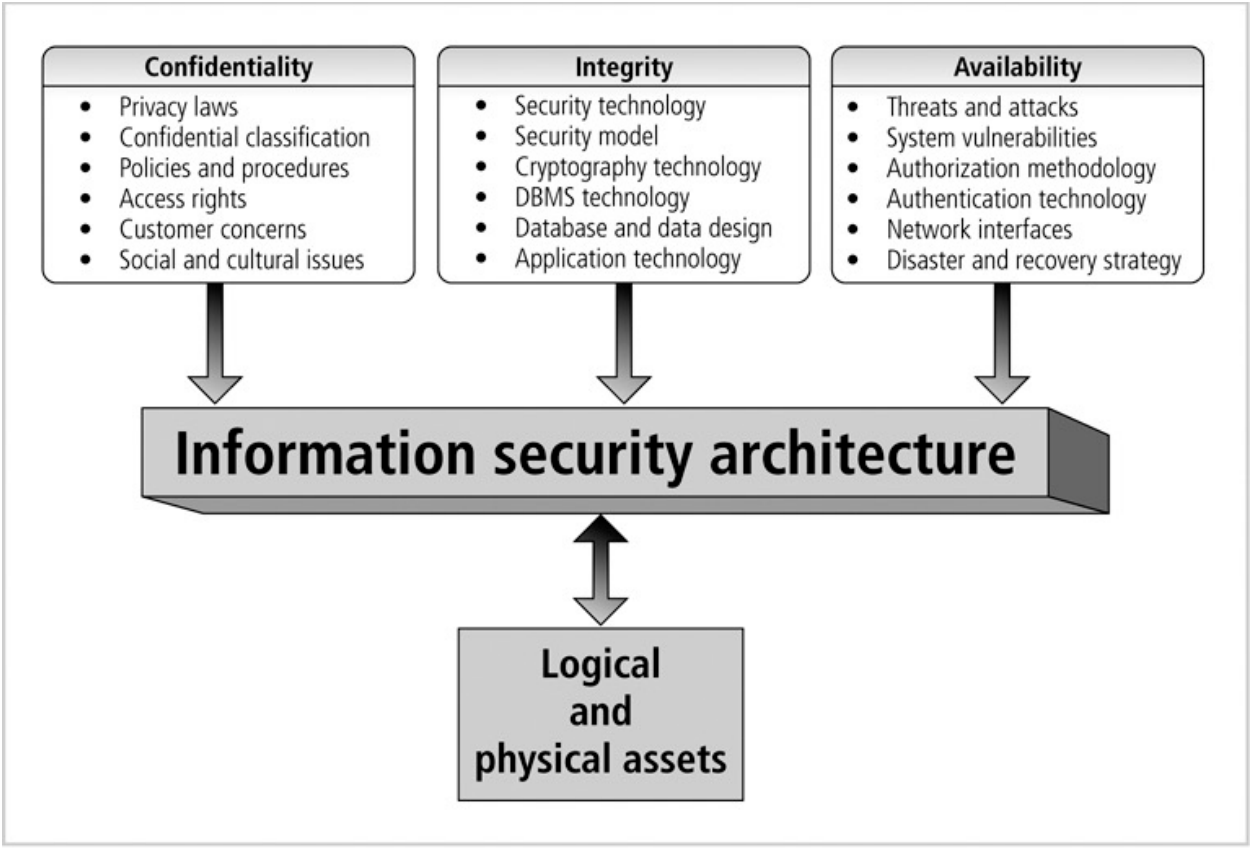

FIGURE 1-7 Information security architecture

Information Security Architecture (continued)

- Components include:
  - Policies and procedures
  - Security personnel and administrators
  - Detection equipments
  - Security programs
  - Monitoring equipment
  - Monitoring applications
  - Auditing procedures and tools

Database Security

- Enforce security at all database levels
- Security access point: place where database security must be protected and applied
- Data requires highest level of protection; data access point must be small

Database Security (continued)

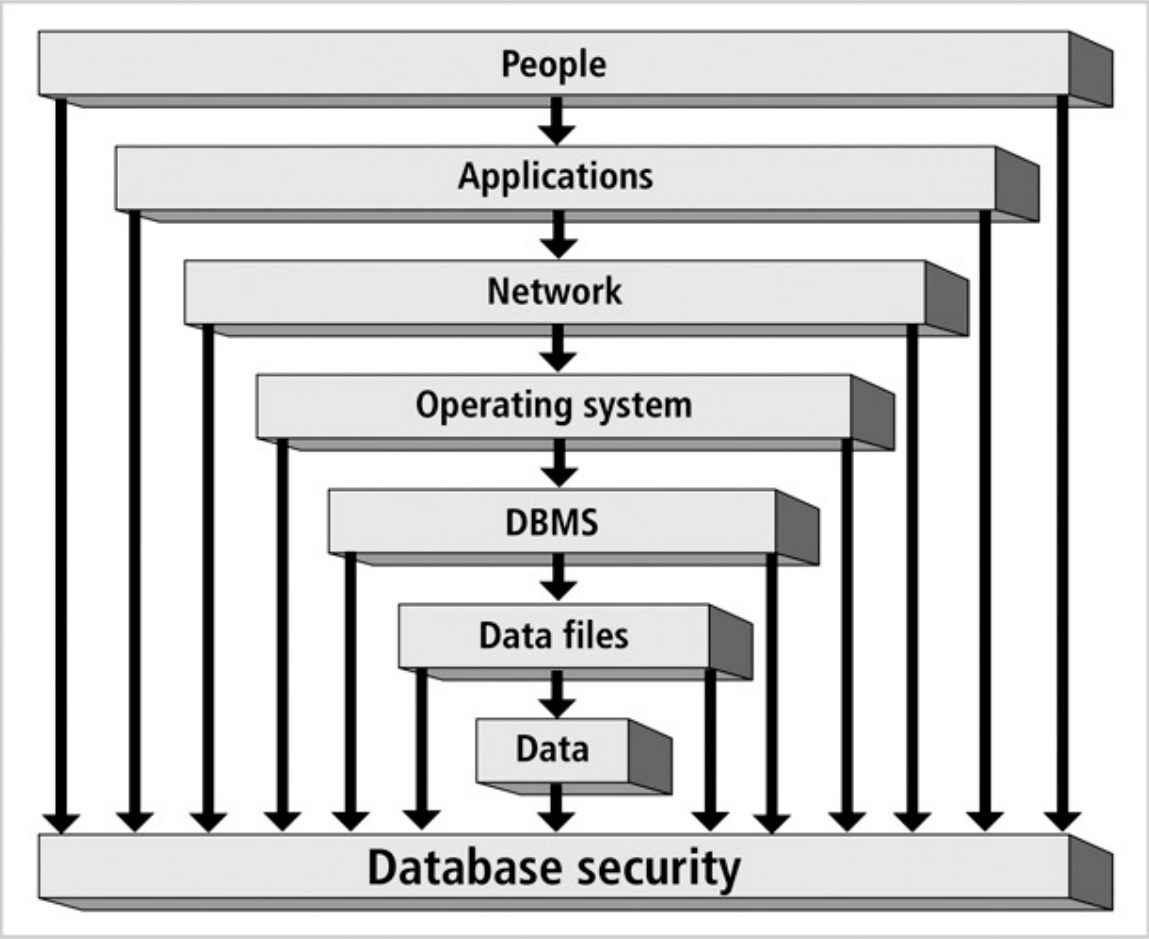

FIGURE 1-8 Database security access points

Database Security (continued)

- Reducing access point size reduces security risks
- Security gaps: points at which security is missing
- Vulnerabilities: kinks in the system that can become threats
- Threat: security risk that can become a system breach

Database Security (continued)

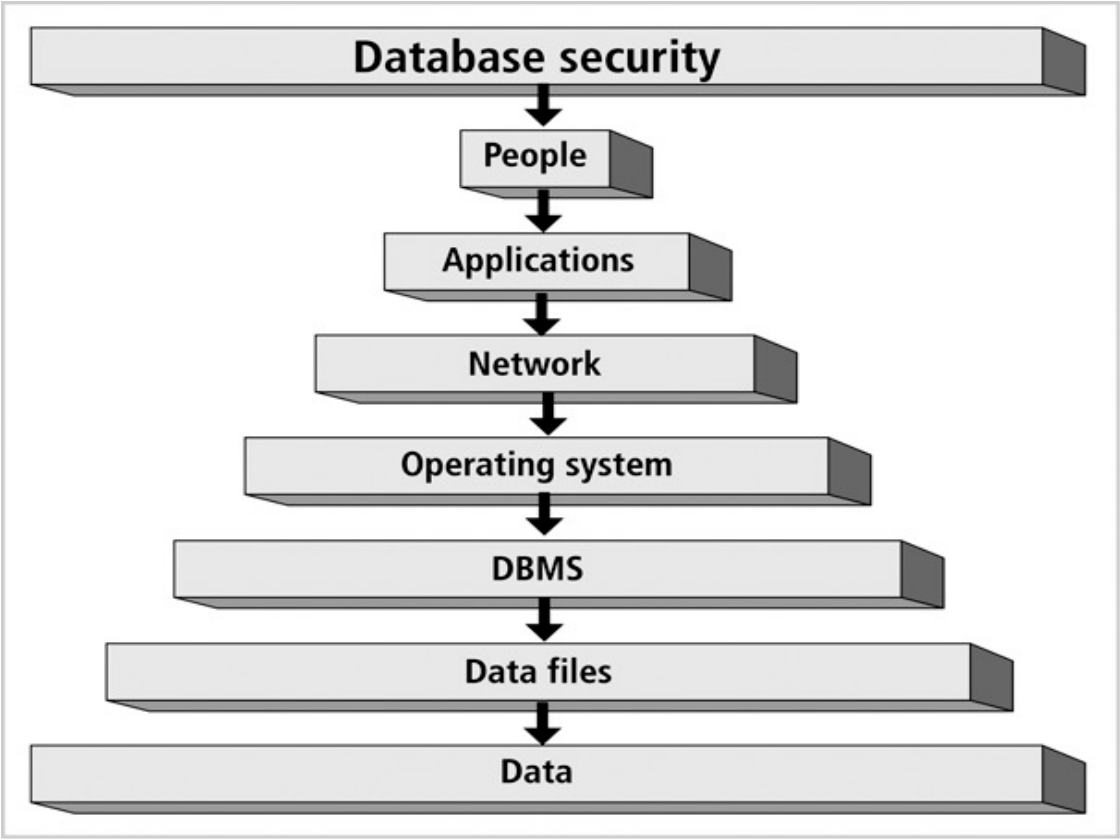

FIGURE 1-9 Database security enforcement

Database Security (continued)

- People: individuals who have been granted privileges and permissions to access applications, networks, servers, databases, data files and data.
- Applications: application design and implementation, which includes privileges and permissions granted to people. Be cautious because too loose permission results in violation of data access, and too strict permission compromises availability.
- Network is the most sensitive security access point. Use best effort to protect the network.

Database Security (continued)

- Operating system: the authentication to the system and the gateway to the data.
- DBMS: logical structure of the database, include memory, executables, and other binaries.
- Data files: to be protected through the use of permissions and encryption.
- Data: need to enforce data integrity, and necessary privileges.

Database Security (continued)

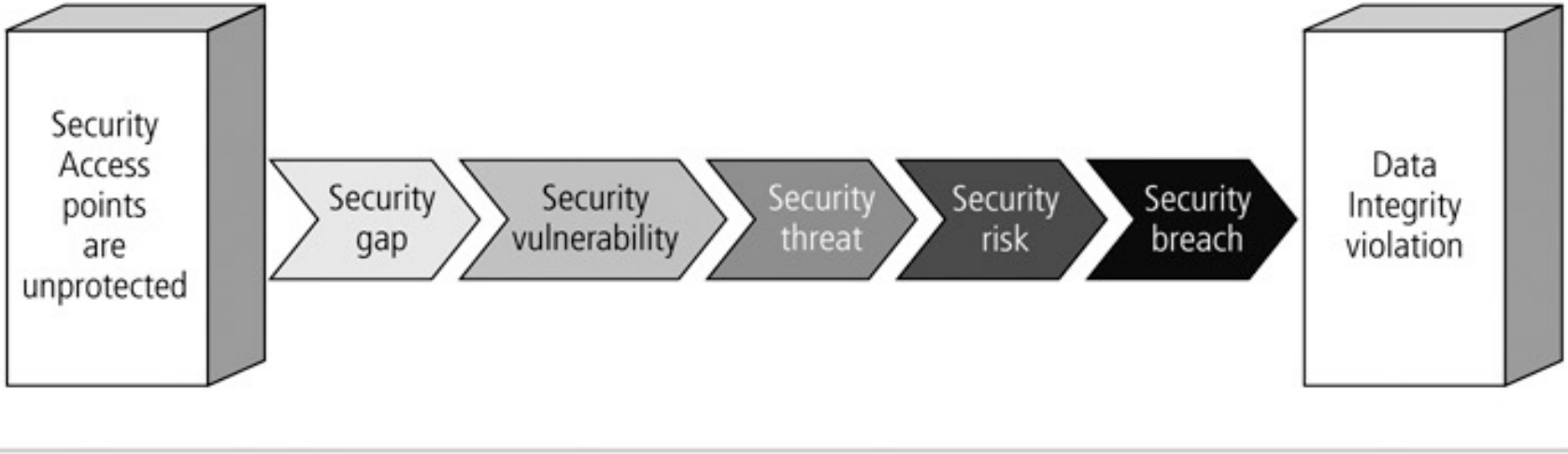

FIGURE 1-10 Data integrity violation process

Database Security Levels

- Relational database: collection of related data files
- Data file: collection of related tables
- Table: collection of related rows (records)
- Row: collection of related columns (fields)

Database Security Levels (continued)

By database management system through user accounts and password

Through file permission

Schema owners/security administrator grant or revoke privileges

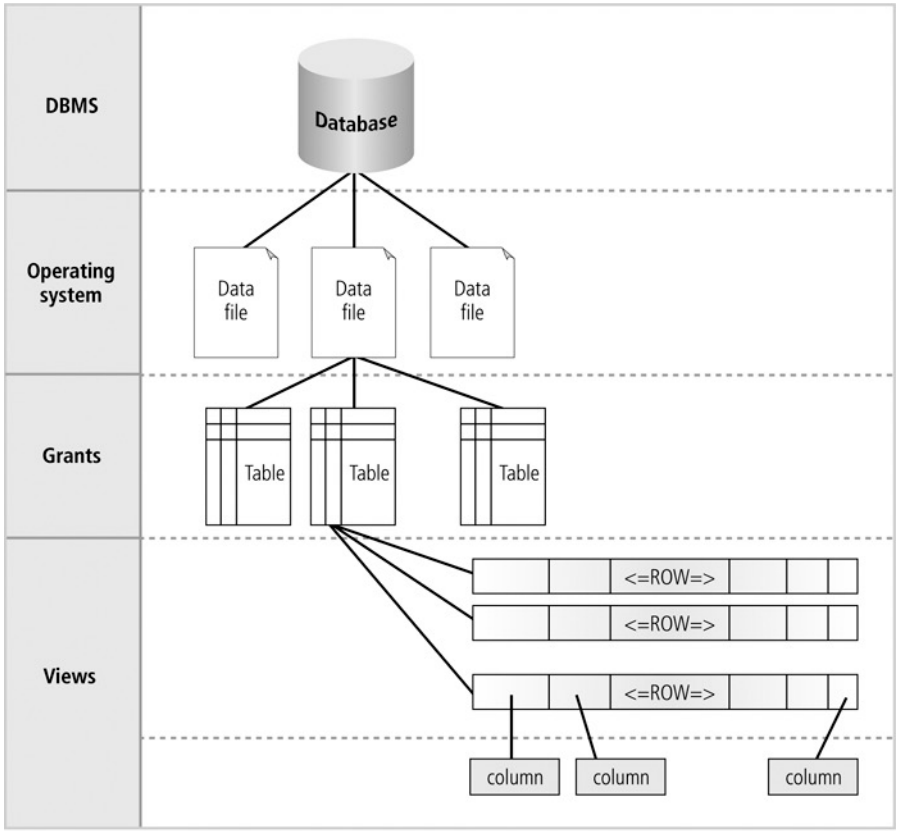

FIGURE 1-11 Levels of database security

Menaces to Databases

- Security vulnerability: a weakness in any information system component

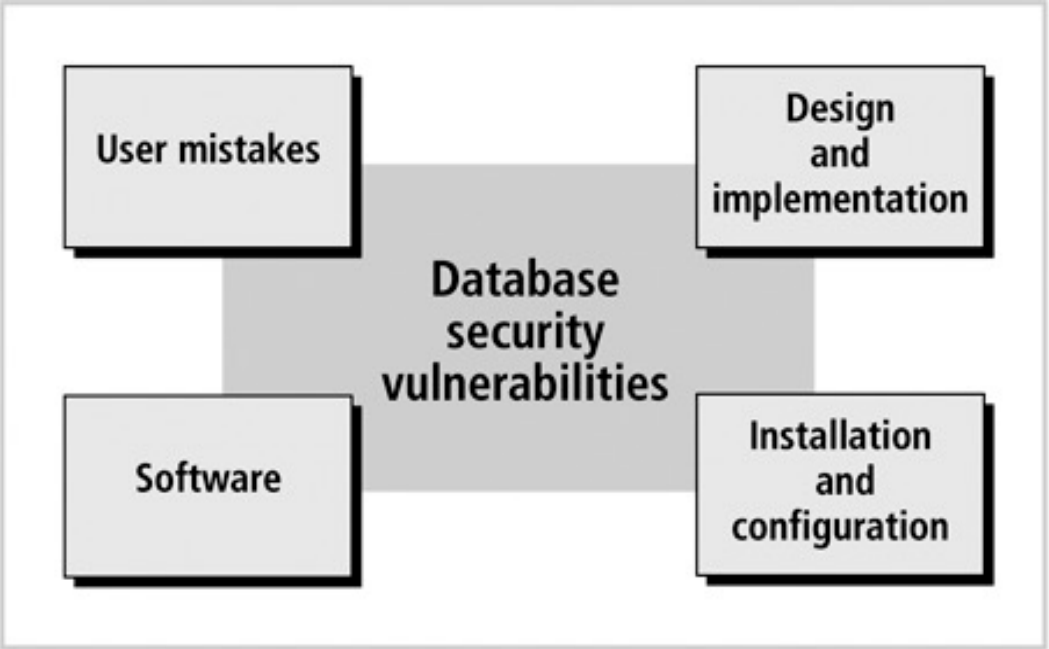

FIGURE 1-12 Categories of database security vulnerablilities

Menaces to Databases (continued)

- Security threat: a security violation or attack that can happen any time because of a security vulnerability.

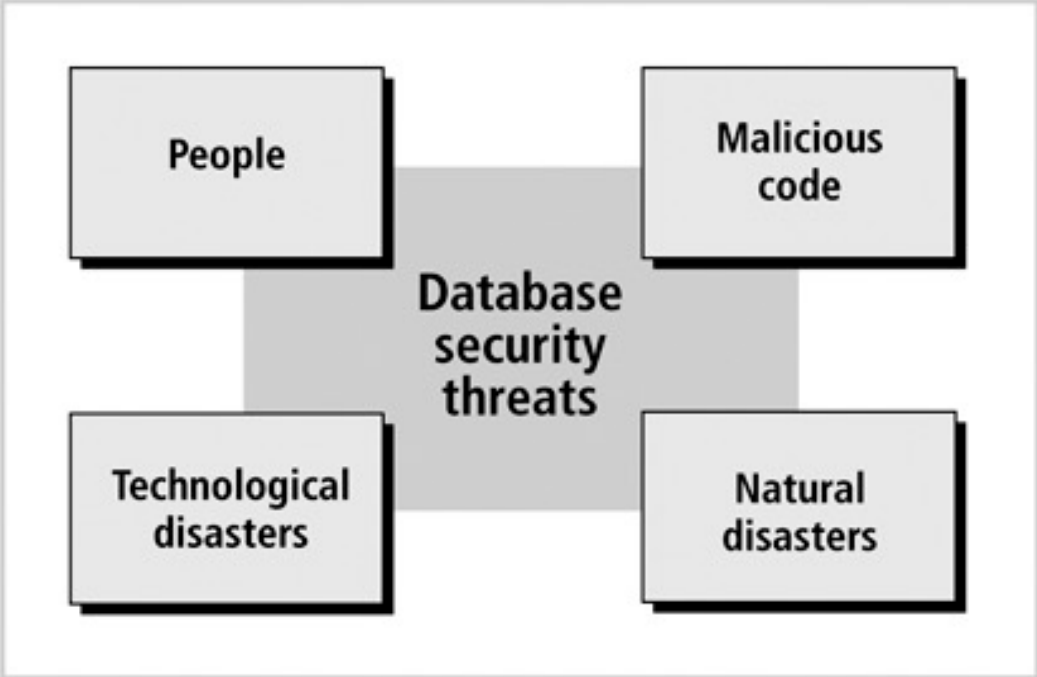

FIGURE 1-13 Categories of database security threats

Menaces to Databases (continued)

- Security risk: a known security gap left open.

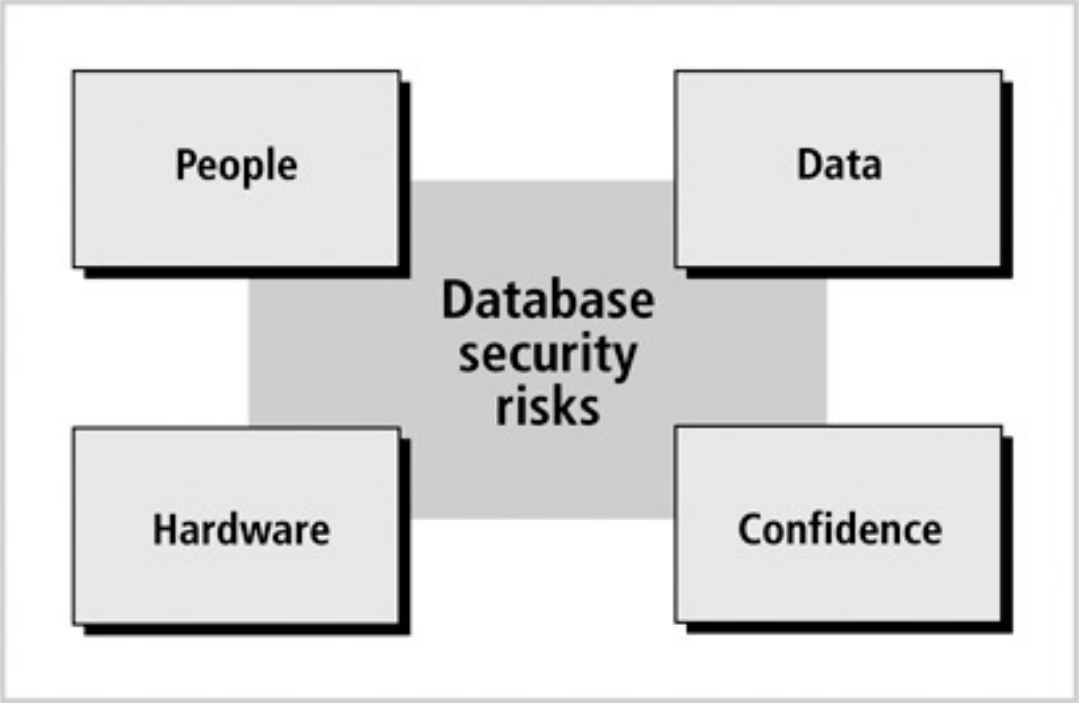

FIGURE 1-14 Categories of database security risks

Menaces to Databases (continued)

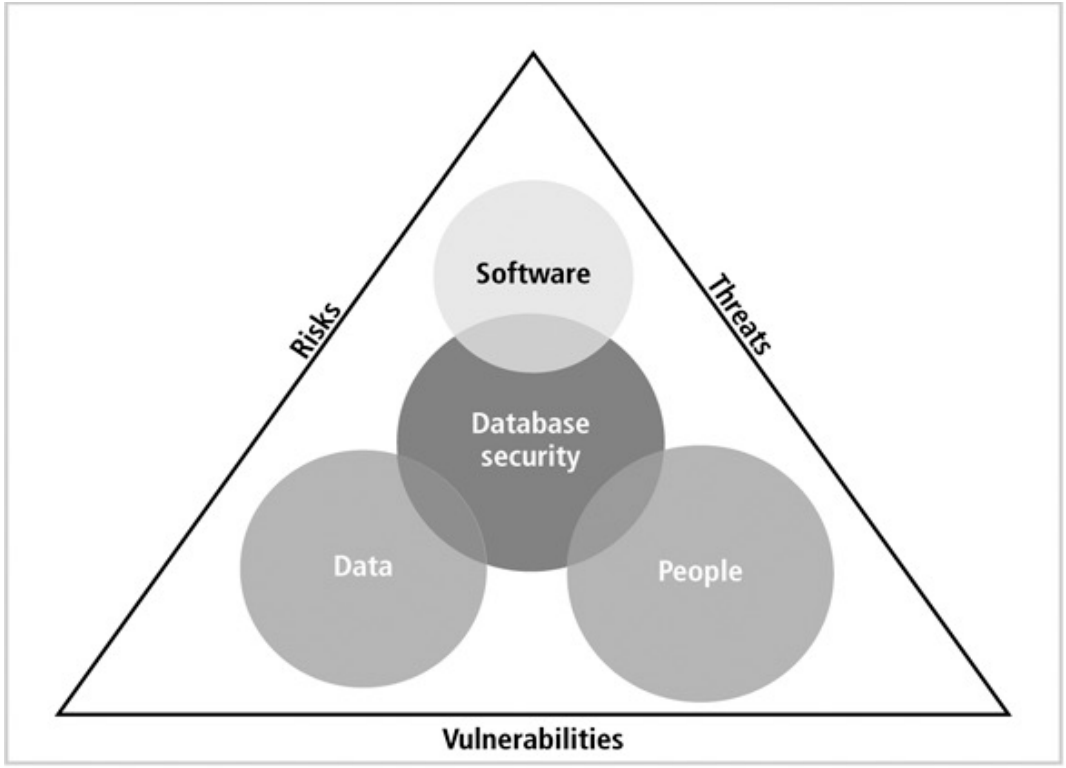

FIGURE 1-15 Integration of security vulnerabilities, threats, and risks in a database environment

Asset Types and Their Value

- Security measures are based on the value of each asset
- Types of assets include:
  - Physical: tangible assets including buildings, cars, hardware, …
  - Logical: such as business applications, in-house programs, purchased software, databases, …
  - Intangible: business reputation, public confidence, …
  - Human: human skills, knowledge, expertise, …

Security Methods

TABLE 1-6 Security methods used to protect database environment components

Database Component Protected	Security Methods
People	■ Physical limits on access to hardware and documents ■ Through the processes of identification and authentication, make certain that the individual is who he or she claims to be through the use of devices, such as ID cards, eye scans, and passwords ■ Training courses on the importance of security and how to guard assets ■ Establishment of security policies and procedures
Applications	■ Authentication of users who access applications ■ Business rules ■ Single sign-on (a method for signing on once for different applications and Web sites)

Security Methods

TABLE 1-6 Security methods used to protect database environment components

Database Component Protected	Security Methods
Network	■ Firewalls to block network intruders ■ Virtual private network (VPN) (a remote computer securely connected to a corporate network) ■ Authentication
Operating system	■ Authentication ■ Intrusion detection ■ Password policy ■ User accounts
Database management system	■ Authentication ■ Audit mechanism ■ Database resource limits ■ Password policy
Data files	■ File permissions ■ Access monitoring

Security Methods (continued)

TABLE 1-6 Security methods used to protect database environment components (continued)

Database Component Protected	Security Methods
Data	■ Data validation ■ Data constraints ■ Data encryption ■ Data access
A business rule is the implementation of a business procedure or policy through code written in an application.	

Database Security Methodology

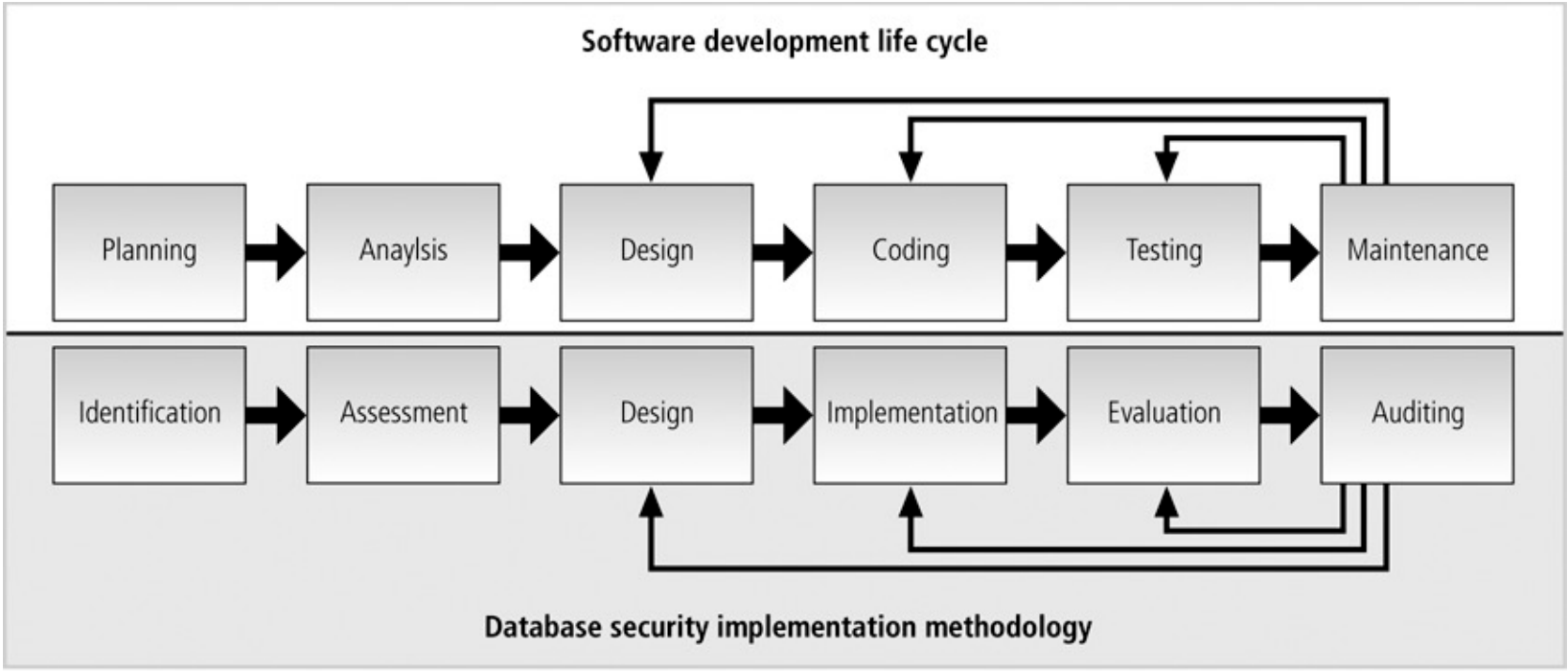

FIGURE 1-16 Database security methodology

Summary

- Security: level and degree of being free from danger and threats
- Database security: degree to which data is fully protected from unauthorized tampering
- Information systems: backbone of day-to-day company operations

Summary (continued)

- DBMS: programs to manage a database
- C.I.A triangle:
  - Confidentiality
  - Integrity
  - Availability
- Secure access points
- Security vulnerabilities, threats and risks
- Information security architecture
  - Model for protecting logical and physical assets
  - Company's implementation of a C.I.A. triangle
- Enforce security at all levels of the database

Databases

- Oracle 11g database:
  - Oracle Database Software Downloads is available at: http://www.oracle.com/technology/software/products/database/index.html
  - Oracle installation guide is available at: http://www.oracle.com/webfolder/technetwork/tutorials/obe/db/11g/r2/2day_dba/index.html
  - Tutorial of Installing Oracle Database 11g on Windows is available at:

http://st-curriculum.oracle.com/obe/db/11g/r2/2day_dba/install/install.htm

Quick Quiz (5 minutes)

- Data is processed or transformed by a collection of components working together to produce and generate accurate information. These components are known as a(n) _____.
  - information system
  - database
  - DBA
  - operating system
- The concept behind a(n) _____ application is based on the business model of a customer ordering a service or product and the representative of a business granting that request.
  - information system
  - C.I.A. triangle
  - DBMS
  - client/server
- _____ is a model for protecting logical and physical assets.

Quick Quiz (5 minutes)

- A _____ is a place where database security must be protected and applied.
  - Security gap
  - Security access point
  - Security threat
  - Security vulnerability
- A _____ is a security violation or attack that can happen any time because of a security vulnerability.
  - Security risk
  - Security privilege
  - Security policy
  - Security threat
- _____ is a collection of security policies and procedures, data constraints, security methods, and security tools blended together to implement all necessary measures to secure the integrity, accessibility, and confidentiality of every component of the database environment.

Hands-on Projects (10 minutes)

You are a security officer working for a medium-sized research company. You have been assigned to guard a back entrance checkpoint. One day, a well-known manager walks out with a box of papers. A day after you are summoned to the security office by your manager and the security director for questioning about the manager who had been terminated the day before. The manager had walked out with highly confidential information.

1. Outline briefly what types of security measures were violated and how to avoid those violations.
2. Describe how this incident may result in security violations.

Hands-on Projects (10 minutes)

You are an employee of a company responsible for the administration of ten production databases. Lately, you have noticed that your manager is asking you frequent questions about the data used by one of the top researchers of the Engineering department. For two days, while conducting routine database tasks, you notice your manager exporting data from the database the top researchers are using.

1. What type of security threat is the exportation of data? How can your prevent it?
2. To what type of security risk could exporting data lead?
3. Explain briefly how you would react to this incident.

Preparation lab: Install Oracle database Project 1: Exercise SQL in Oracle Database

- Create the database schema (you can use the script from the textbook), refer to Figure 4-20 for details.
- Fill in the data (you can use the script from the textbook)
- Use SQL commands to manipulate the data, such as query, insert and delete.
- Submit a written report including above activities.