Faculty of Informatics Engineering

الجامعة السورية الخاصة
SYRIAN PRIVATE UNIVERSITY

DATABASE SYSTEMS SECURITY

CHAPTER 1:

SECURITY ARCHITECTURE

DR. CHRISTINE ZENIEH

INTRODUCTION

- The **cost of data loss** is rising progressively every year.
- Companies are losing data due to **malicious attacks** and **improper implementation of database security and auditing**.
- **Data must be protected** in order to ensure the company operability.

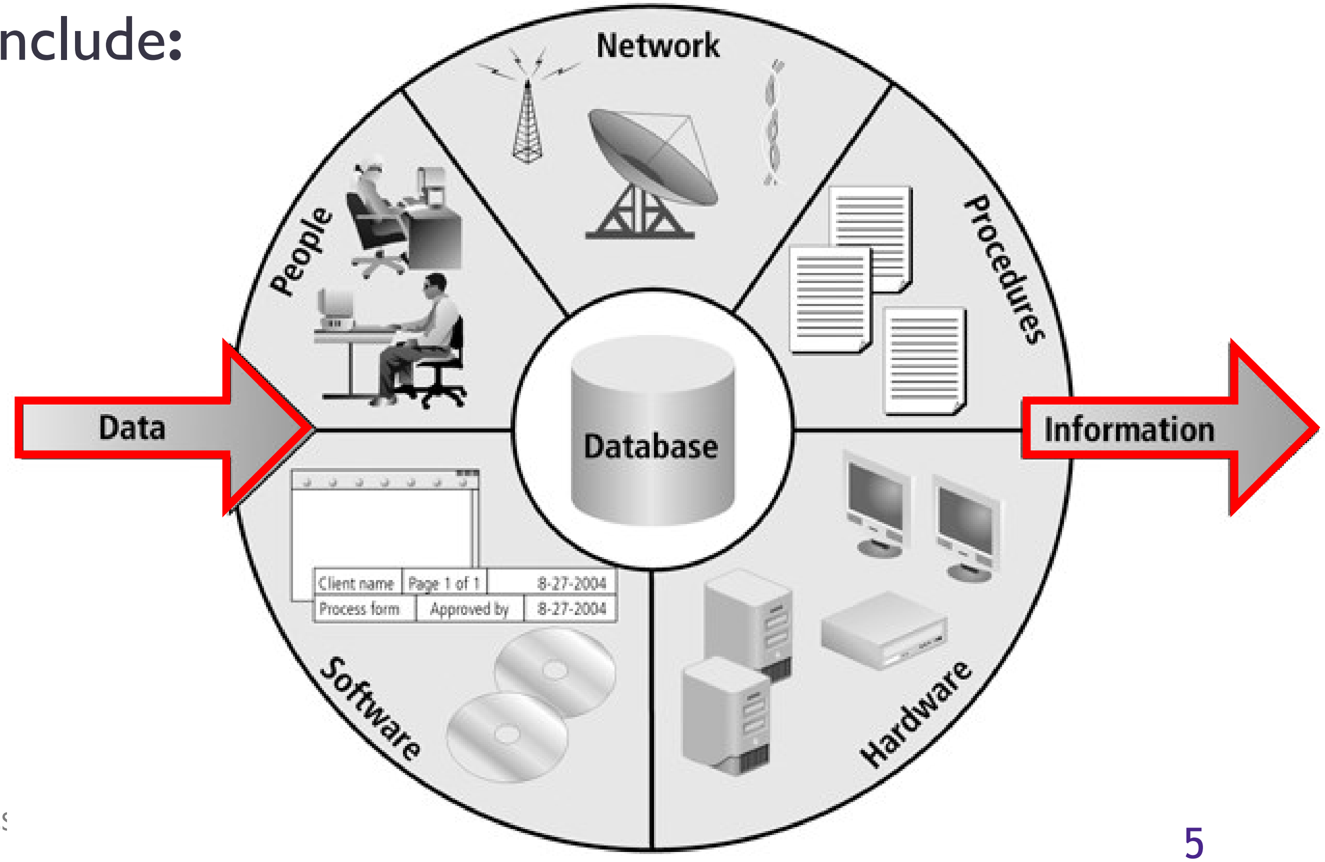
SECURITY

- **Database security:**
  Degree to which **data** is fully **protected** from **tampering** or **unauthorized acts**. (incomplete definition)
- To understand Database security, you need to understand:
  - Various **information systems**
  - **Information security concepts**

INFORMATION SYSTEMS

INFORMATION SYSTEMS

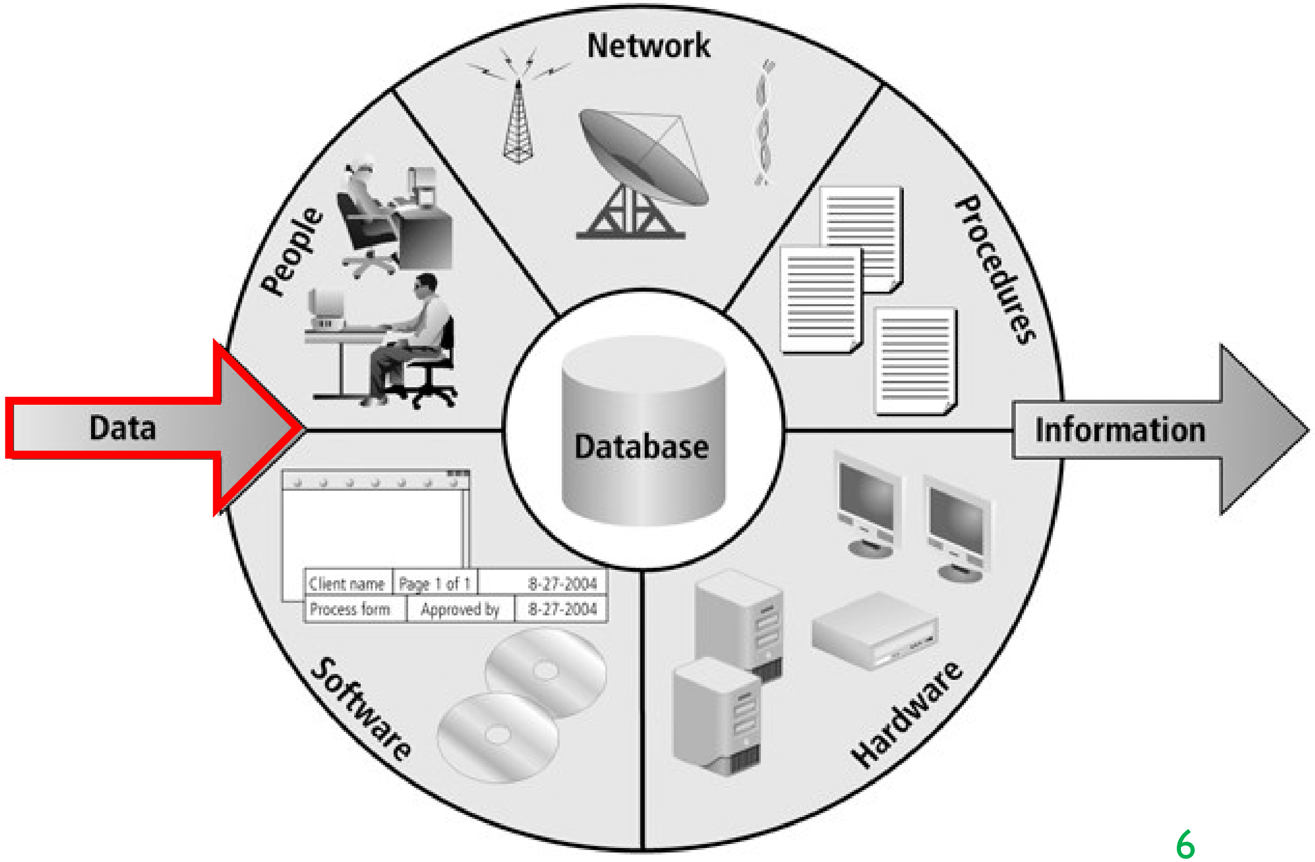
- A collection of **components working together** to produce **accurate information**
- **Information system components** include:
  - Data
  - Procedures
  - Hardware
  - Software
  - Network
  - People



INFORMATION SYSTEMS COMPONENTS

Data:

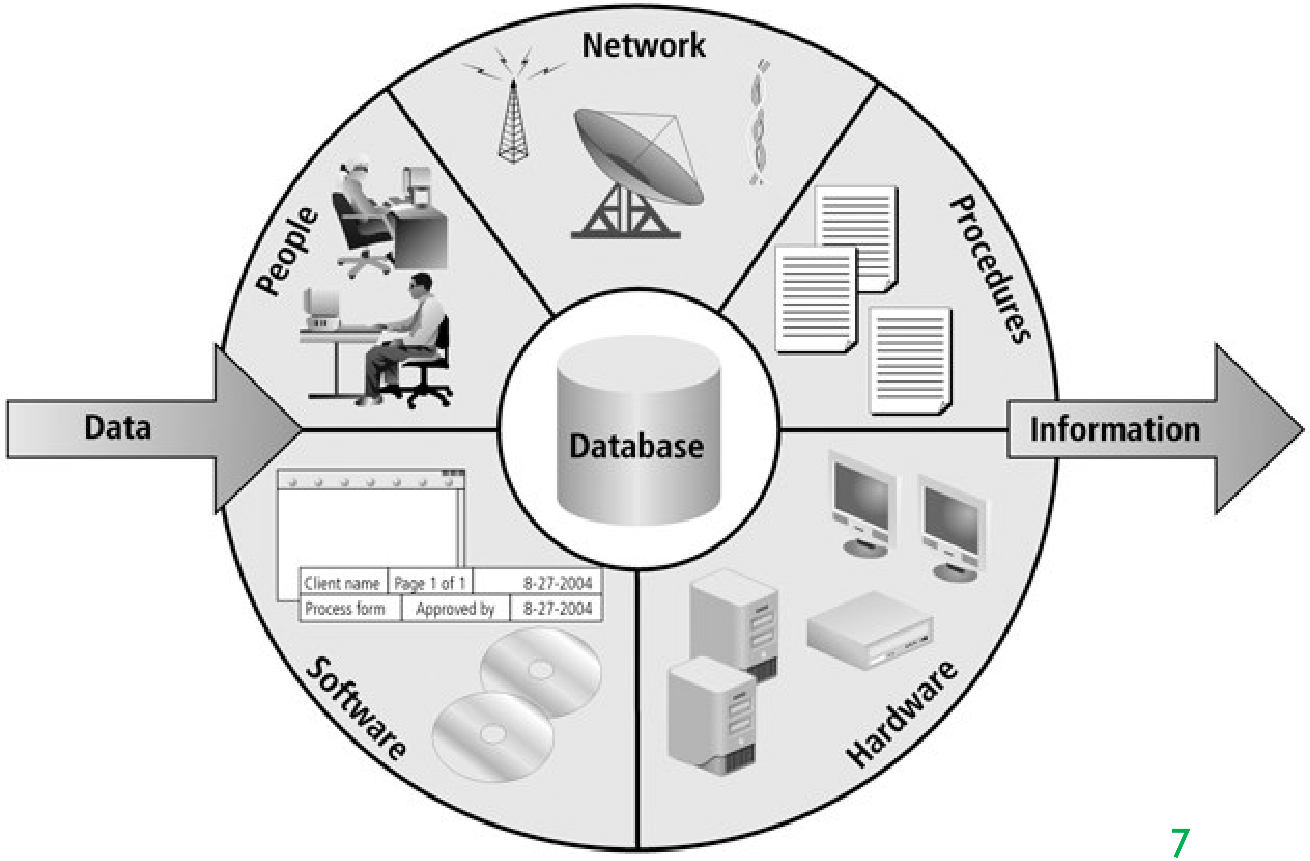
- Collected **data** and **facts** used as **input** for system processing
- Data **stored** in the database for future **reference** or **processing**.



INFORMATION SYSTEMS COMPONENTS

Procedures:

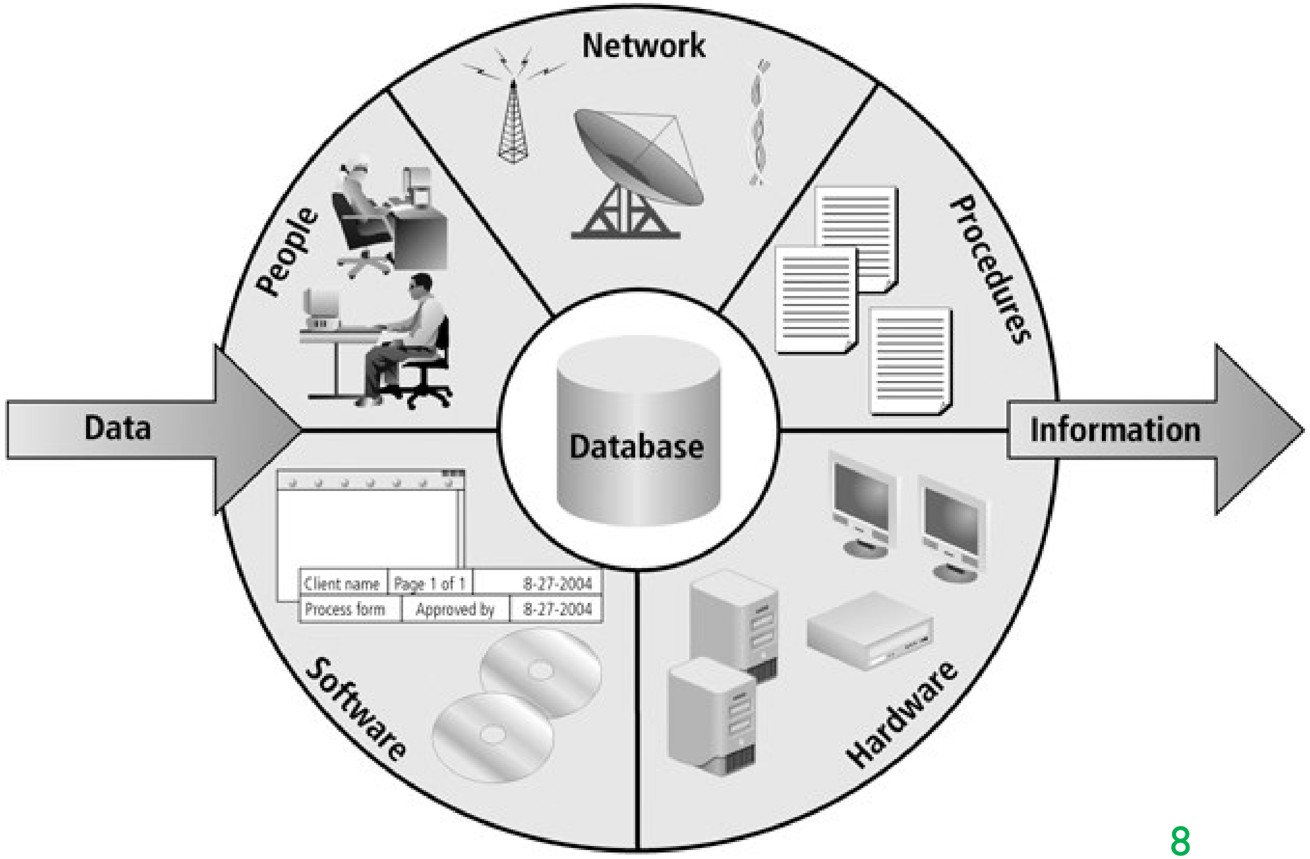
- Manual procedures
- Guidelines
- Business rules
- Policies



INFORMATION SYSTEMS COMPONENTS

Hardware:

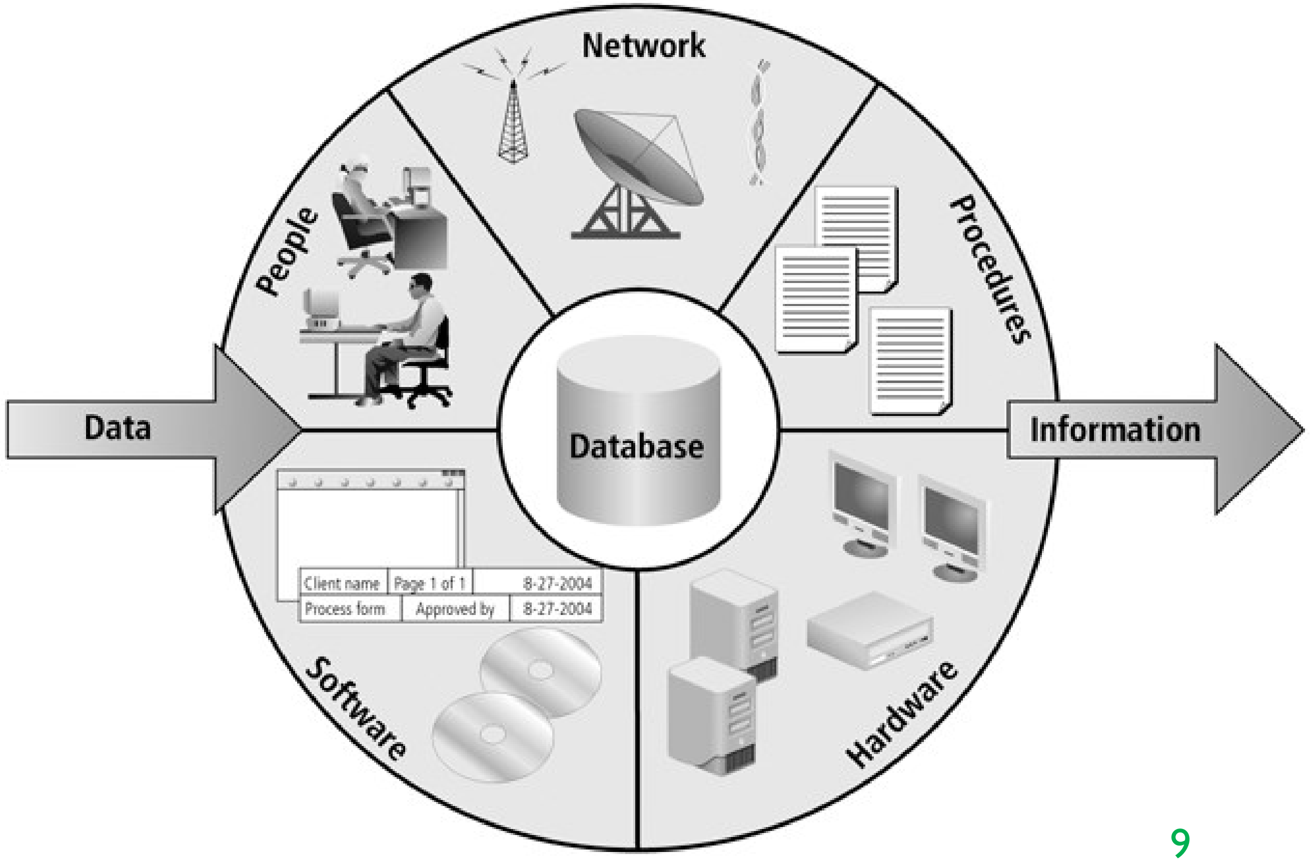
- Computer systems
- Devices
- etc.



INFORMATION SYSTEMS COMPONENTS

Software:

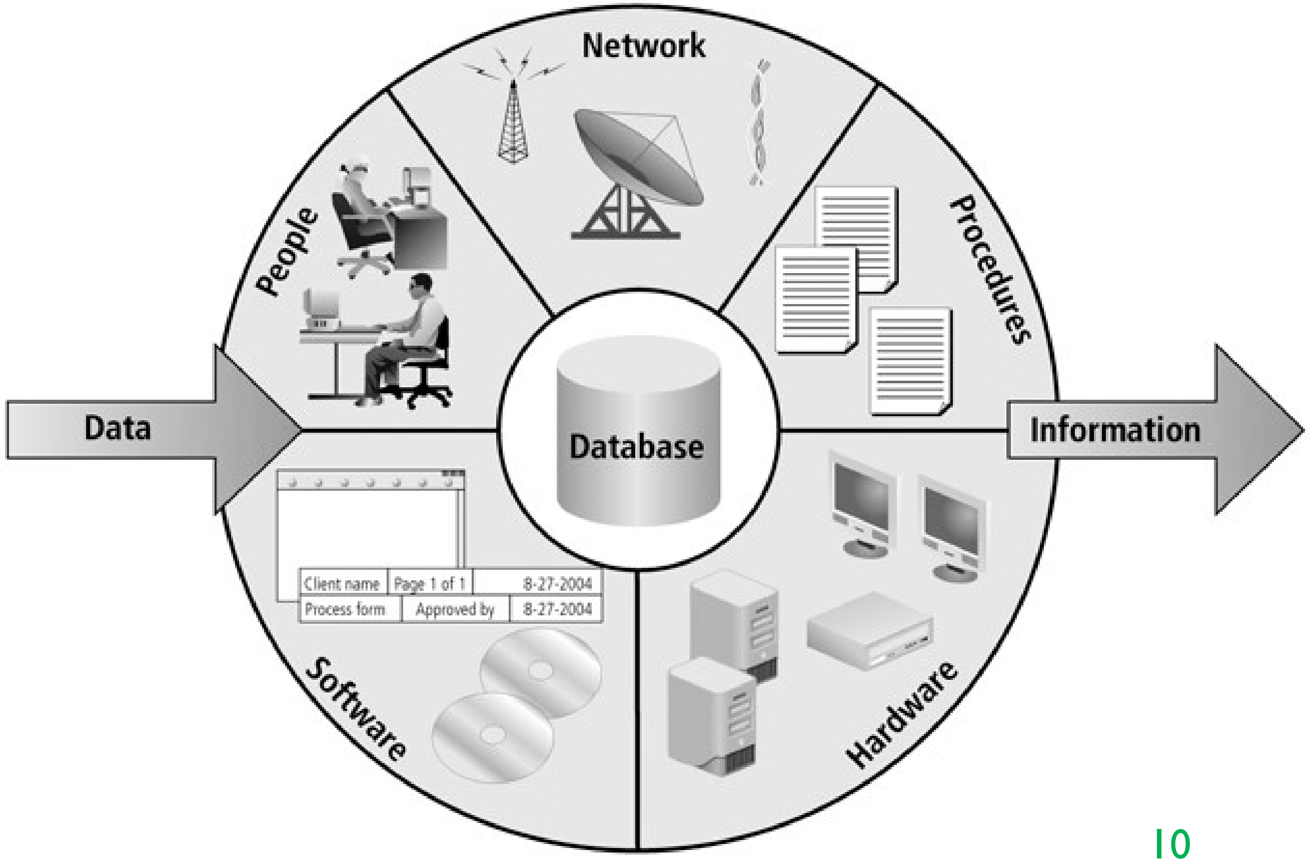
- Application code
- Database management system
- Operating system
- etc.



INFORMATION SYSTEMS COMPONENTS

Network:

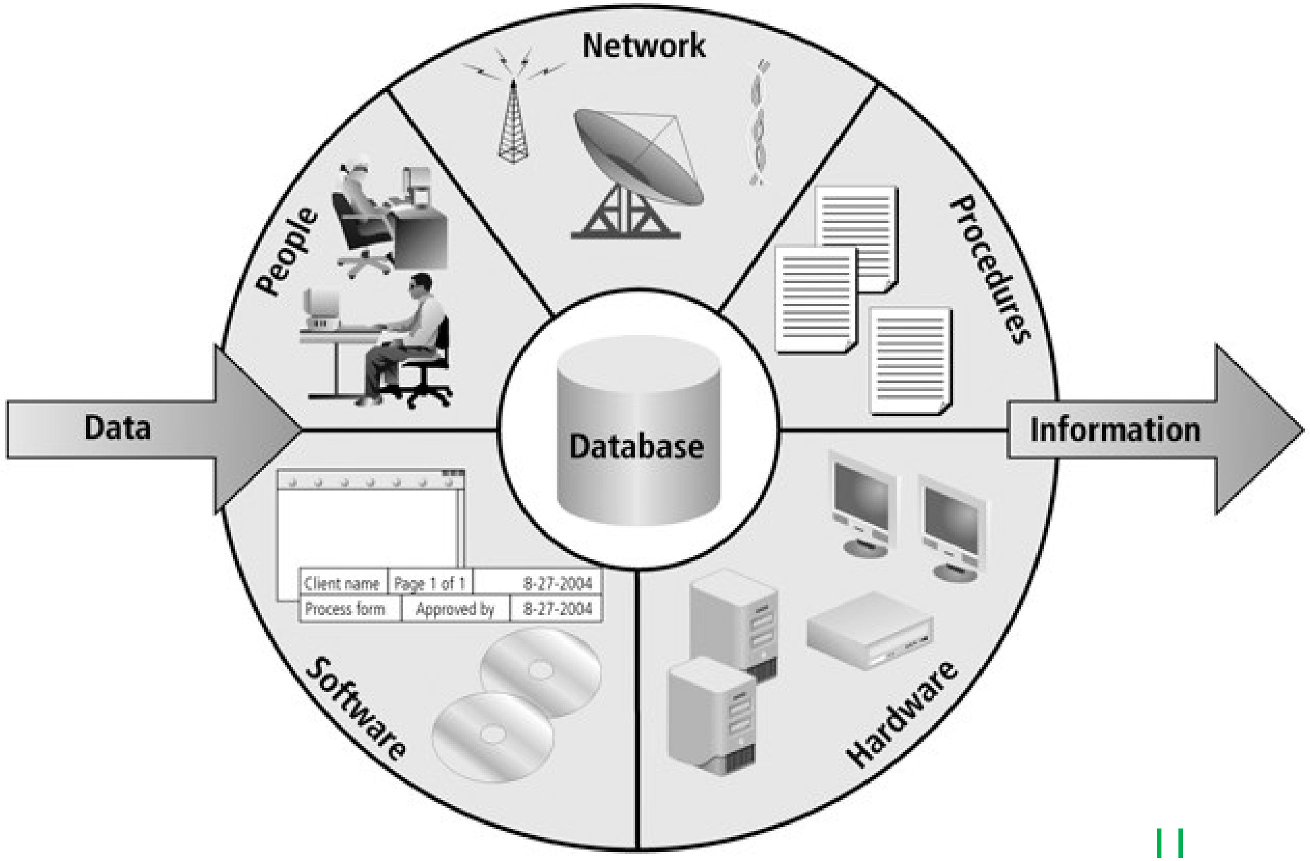
- A communication infrastructure



INFORMATION SYSTEMS COMPONENTS

People:

- Users
- Managers
- Programmers
- Database administrators
- System administrators
- etc.



CLIENT/SERVER ARCHITECTURE

- The **database** is a **core component** in client/server architecture.
- This **client/server architecture** is composed of **three layers**:
  - **Layer 1:** User interface (Client)
  - **Layer 2:** Network layer
  - **Layer 3:** Which responds to all requests submitted by the client (Database server).
- All applications use some sort of a database server.

DATABASE MANAGEMENT SYSTEMS

DATABASE MANAGEMENT SYSTEMS (DBMS)

- A collection of **programs** whose main purpose is to **allow users to store**, **manipulate**, and **retrieve data efficiently**.
- **Examples:** Oracle, MySQL, Microsoft SQL Server, etc.
- **DBMS functionalities:**
  - **Organize data**
  - **Store** and **retrieve** data efficiently
  - Manipulate data (**update** and **delete**)
  - Enforce referential **integrity and consistency** (relationship between tables)
  - Enforce and implement **data security policies and procedures**
  - **Back up**, **recover**, and **restore data**

DATABASE MANAGEMENT SYSTEMS (DBMS)

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

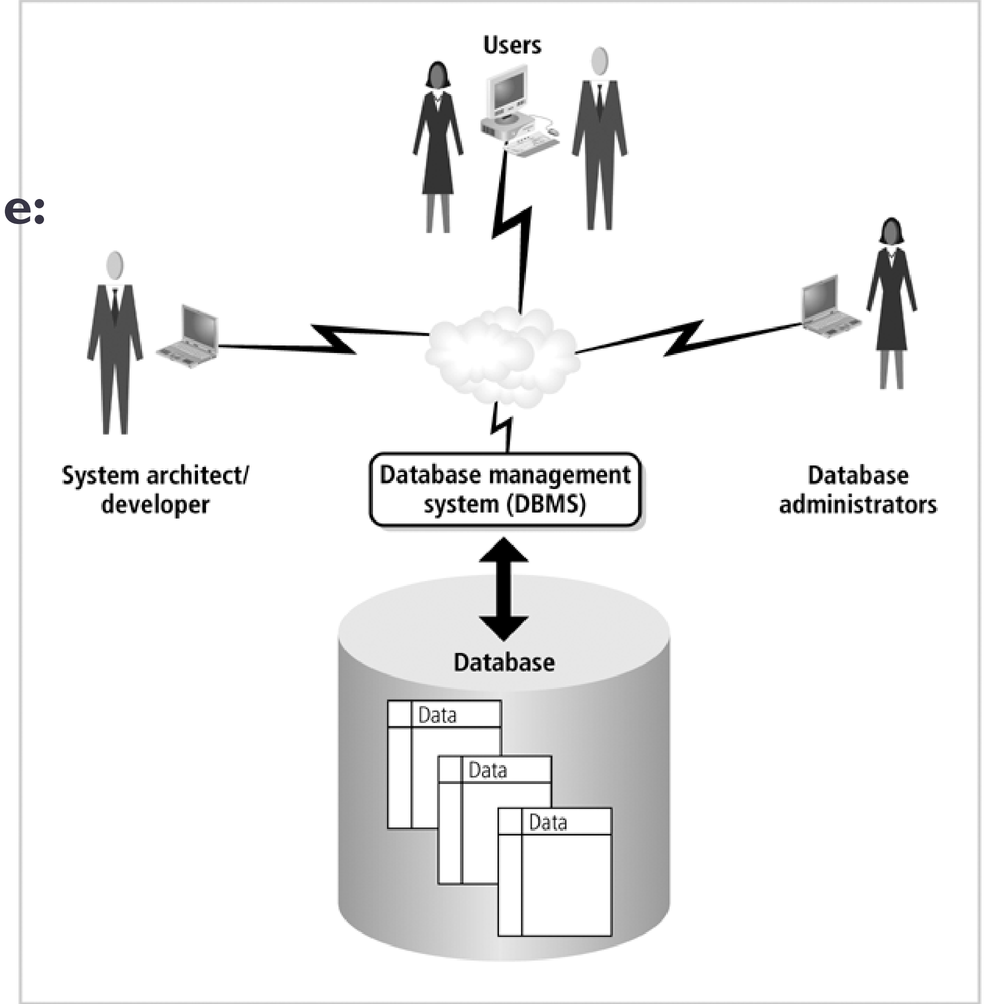

Users
System architect/ developer
Database management system (DBMS)
Database administrators
Database
Data
Data
Data

FIGURE 1-4 Database and DBMS environment

INFORMATION SECURITY

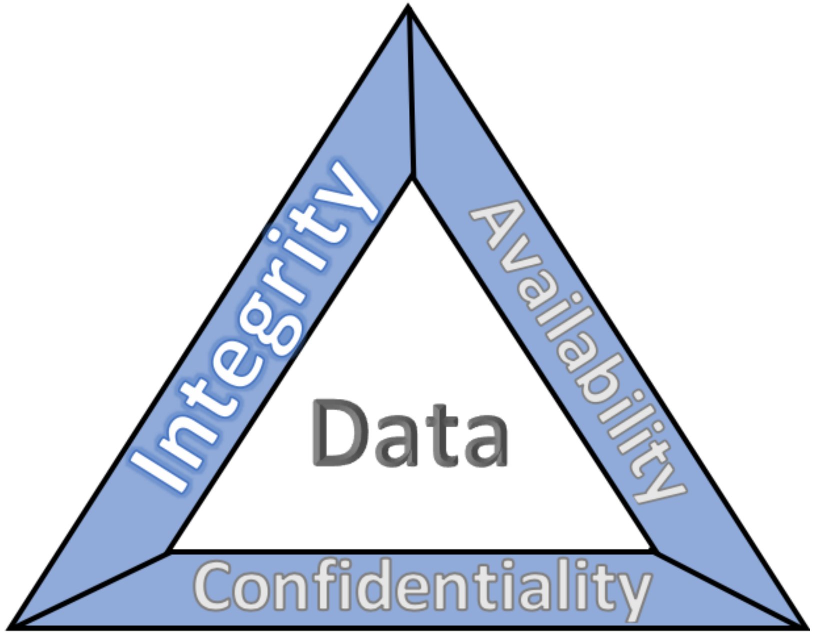
INFORMATION SECURITY

- **Information** is one of an organization's **most valuable assets**
- Information is **safe** if it is **protected from access by unauthorized users**.
- **At the same time** (to be useful) information **must be accessible at all times to authorized users**.

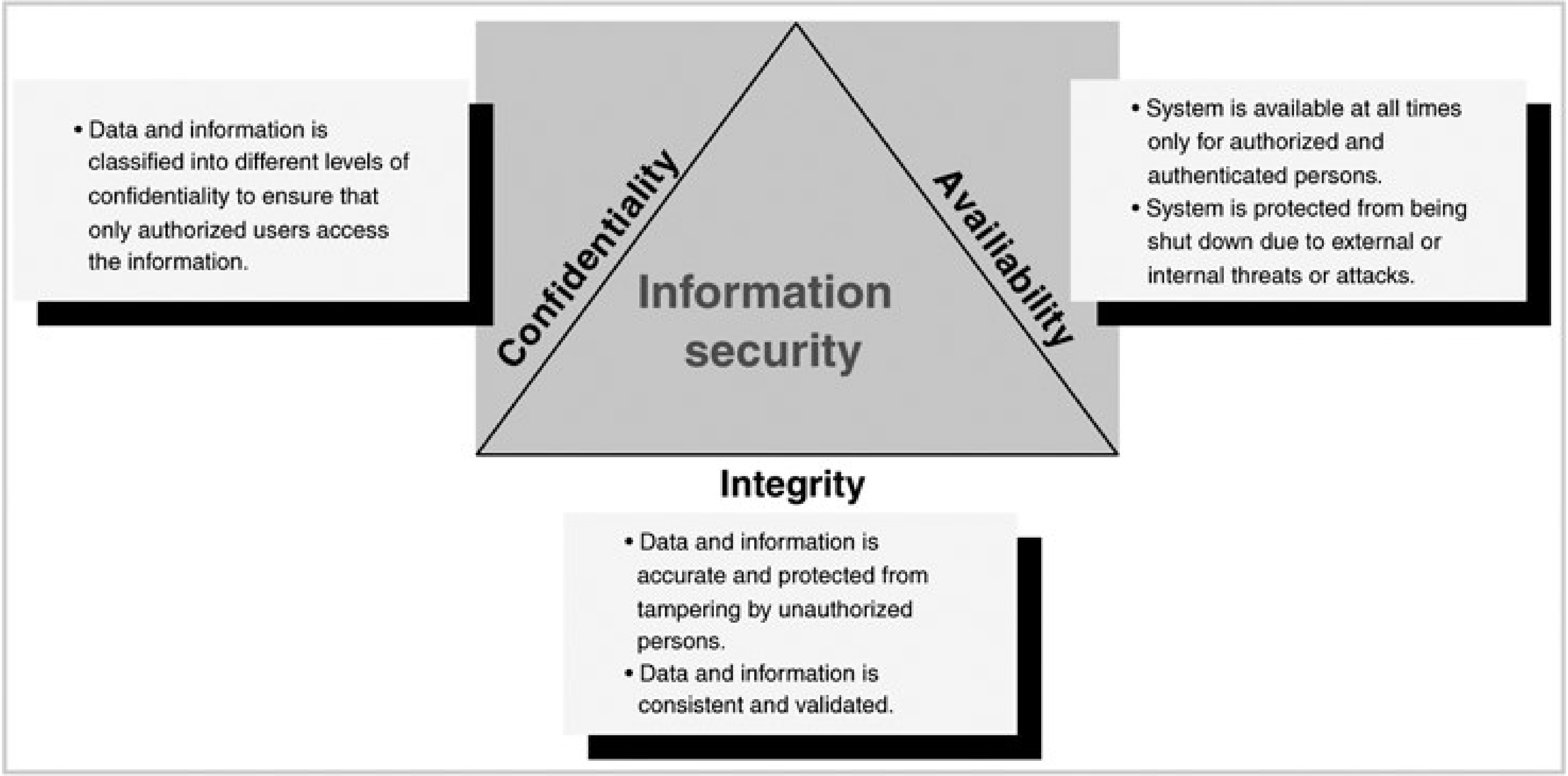
Information security consists of **procedures** and **measures** taken to **protect information systems components**.

C.I.A. TRIANGLE

- The concept of information security is **based on** the **C.I.A. triangle** according to the National Security Telecommunications and Information Systems Security Committee (NSTISSC)
- **C.I.A. triangle:**
  - Confidentiality
  - Integrity
  - Availability



C.I.A. TRIANGLE



Confidentiality

- Data and information is classified into different levels of confidentiality to ensure that only authorized users access the information.

Availability

- System is available at all times only for authorized and authenticated persons.
- System is protected from being shut down due to external or internal threats or attacks.

Information security

Integrity

- Data and information is accurate and protected from tampering by unauthorized persons.
- Data and information is consistent and validated.

CONFIDENTIALITY

- Confidentiality is the **prevention** of **unauthorized individuals** from knowing or accessing **secret information**.
- Company information should be **classified into different levels**:
  - Information are classified **based on the degree of confidentiality**
  - Each level has **its own security measures**

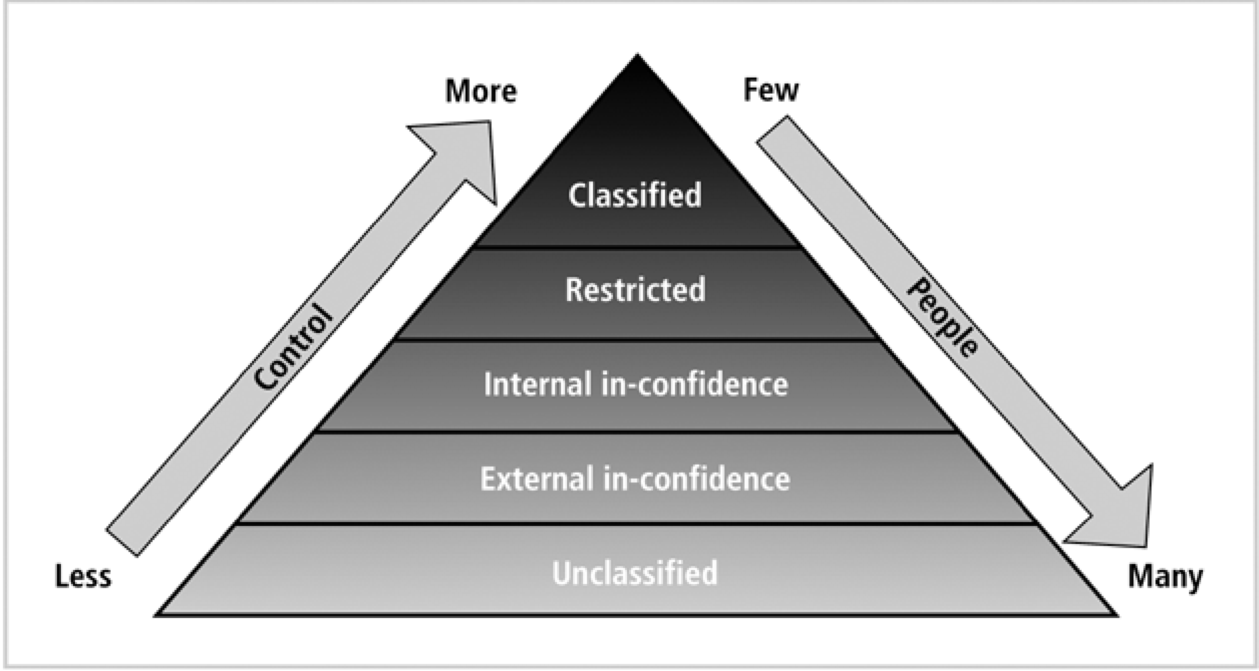


FIGURE 1-6 Confidentiality classification

INTEGRITY

- **Data is considered to have integrity** if it is **accurate** and has not been tampered with **intentionally** or **accidentally**.
- Data must be protected at **all levels** to achieve full integrity.
- Consistent and **valid data**, processed correctly, yields **accurate information**
- **Example of a violation of data integrity**

INTEGRITY

Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Invalid data	Not all the entered and stored data is valid. Checks and validation processes that prevent invalid data are missing.	User enters invalid data mistakenly or intentionally. Application code does not validate inputted data.
Redundant data	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.
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.

INTEGRITY

Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Data anomalies	Exists when there is redundant data and 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.
Data read inconsistency	The user does not always read the last committed data. 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	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

- The systems should be **always available to authorized users**
- The systems should determine **what a user can do with the information**
- **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
- **How is availability related to security?**

INFORMATION SECURITY ARCHITECTURE

INFORMATION SECURITY ARCHITECTURE

- **Information Security Architecture** is the company's **implementation of C.I.A. triangle**
- Information Security Architecture **components** range from **physical equipment** to **logical tools and utilities**.

THE COMPONENTS OF INFORMATION SECURITY ARCHITECTURE

- **Policies and procedures:** Documented procedures and policies that elaborate on how security is to be carried out
- **Security personnel and administrators:** People who enforce and keep security in order
- **Detection equipment:** Devices that authenticate employees and detect equipment that is prohibited by the company
- **Security programs:** Tools that protect computer systems' servers from malicious code such as viruses
- **Monitoring equipment:** Devices that monitor physical properties, employees, and other important assets
- **Monitoring applications:** Utilities and applications used to monitor network traffic and Internet activities, downloads, uploads, and other network activities
- **Auditing procedures and tools:** Checks that security measures are working

DATABASE SECURITY

DATABASE SECURITY

- The database **administrator** have to implement security at **all levels of the database**.
- To protect data stored in the database, the various **security access points** that can make your database vulnerable **must be known**.

DATABASE SECURITY ACCESS POINTS

- **Security access point:**
  Place where database security must be applied (implemented, enforced, and audited)

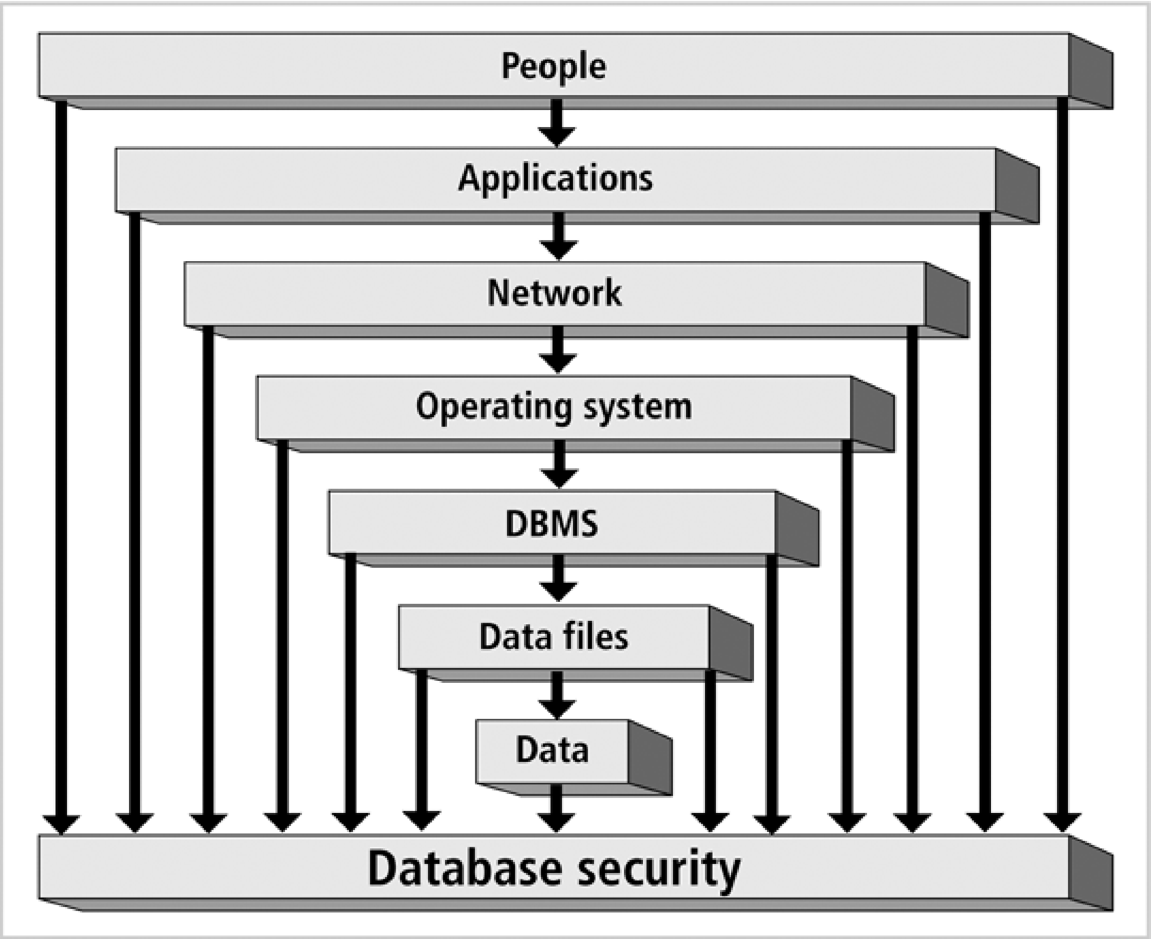


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

- The **major access points** within a database environment where security measures must be applied:
  - People
  - Applications
  - Networks
  - Operating system
  - Database management system
  - Data files
  - Data

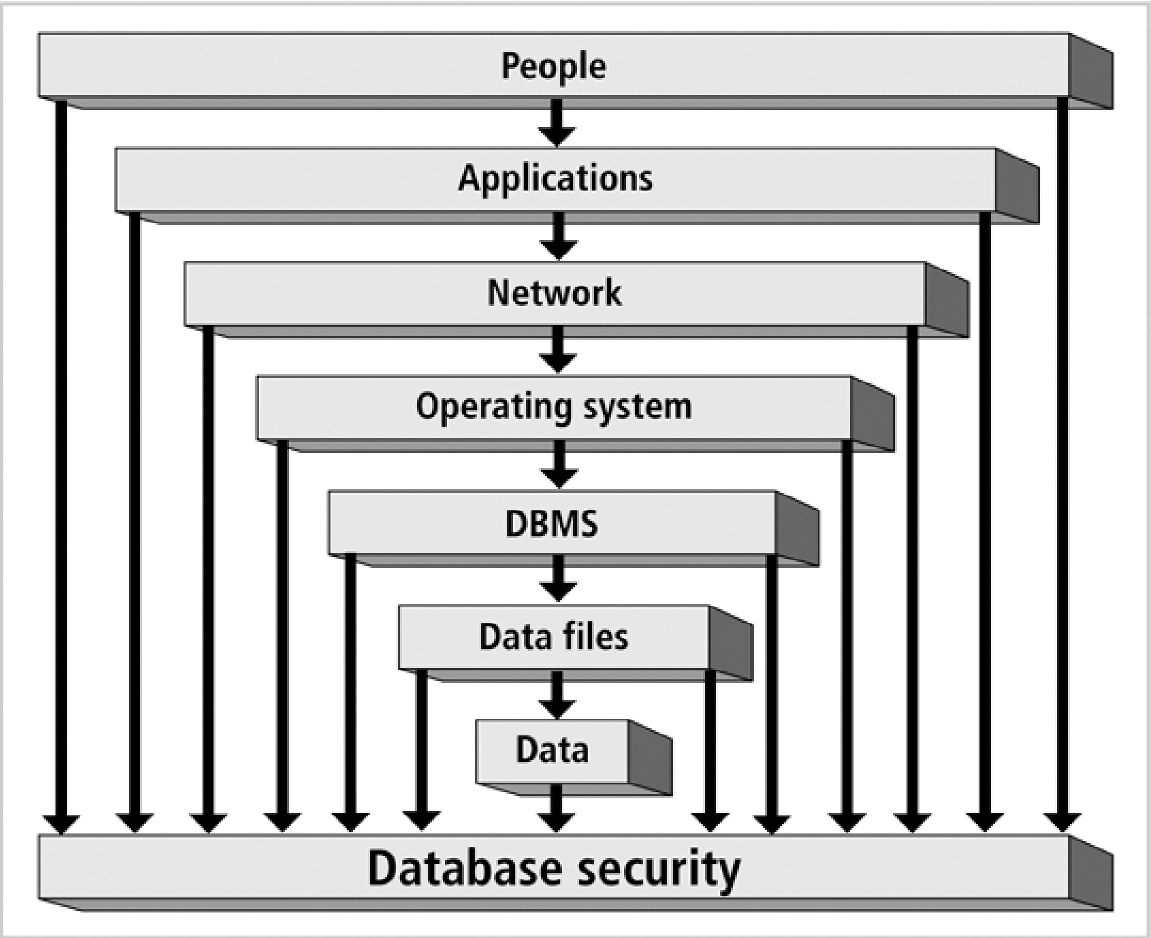


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

People:

- **Individuals** who have **permissions** to access applications, networks, servers, databases, data files, and data.
- People represent a **risk** of database security violations.
- Database security **must secure the data against violations caused by people**.

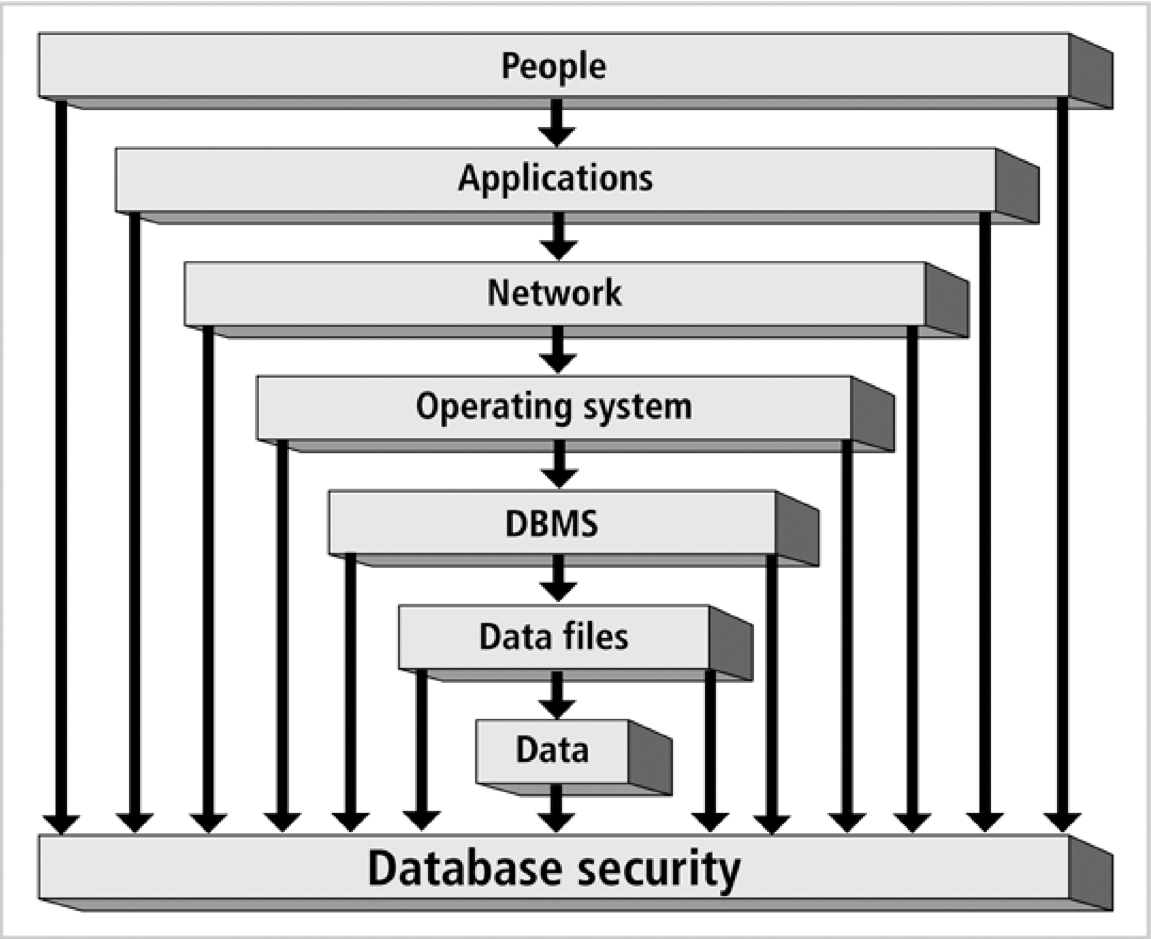


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Applications:

- Application which includes **permissions granted to people**.
- If these permissions are **too loose**, individuals can access and violate data.
- Extreme caution should be exercised when granting **security privileges to applications**.

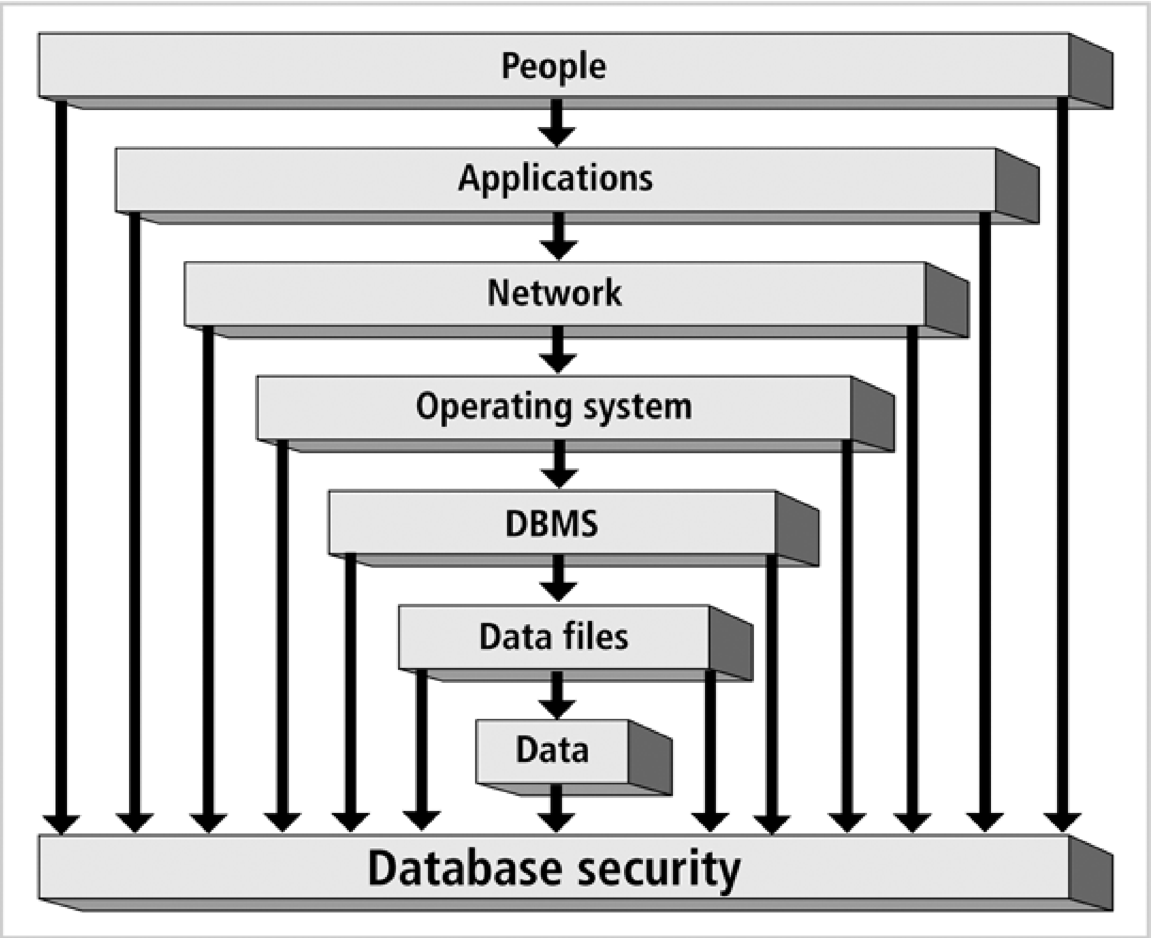


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Network:

- One of the most **sensitive** security access points.
- The network should be protected with the best efforts

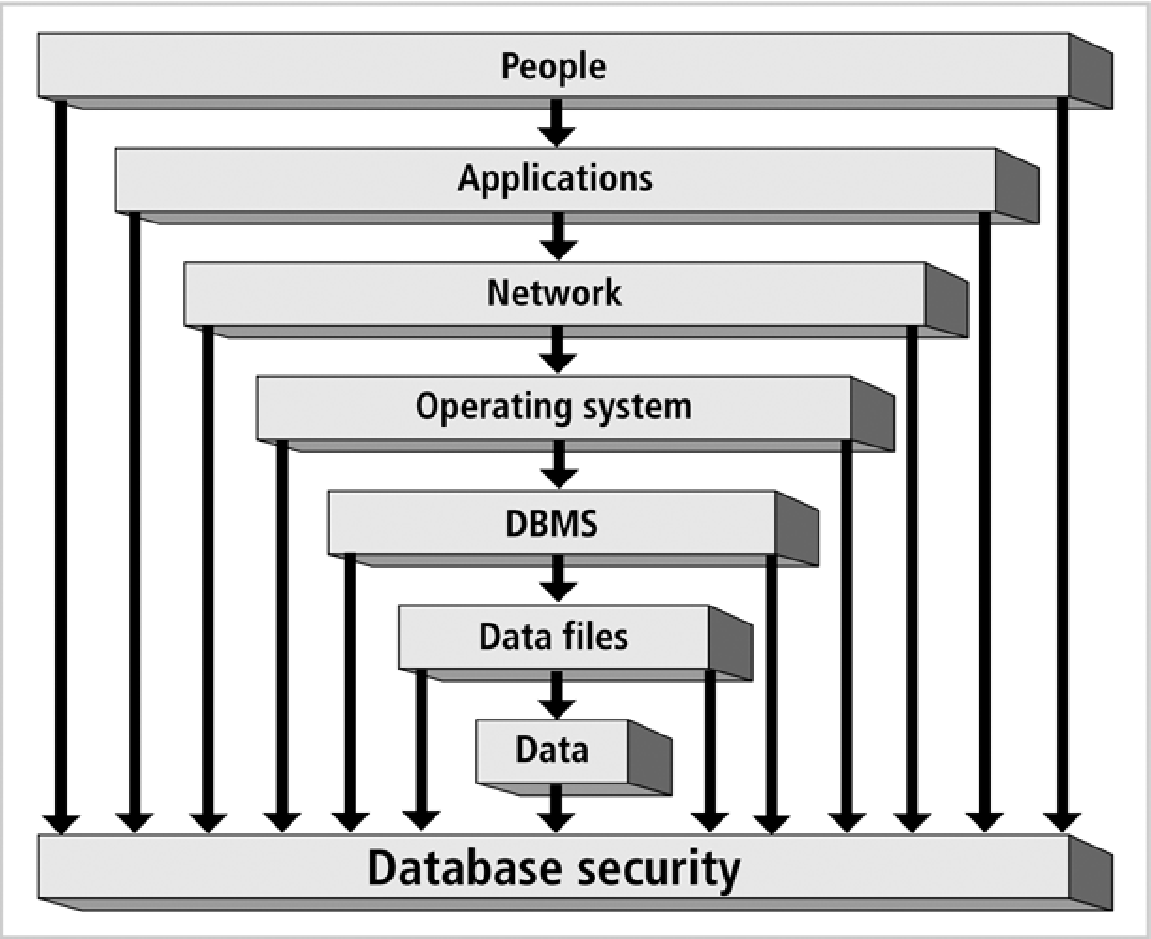


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Operating system:

- The operating system access point consists of the **authentication mechanism** for logging into the system, which acts as the **gateway to access the data**. (to access the data residing in a system, you must log on and your security credentials must be verified).
- The absence of good security measures at this access point is the cause of **most security violations**.

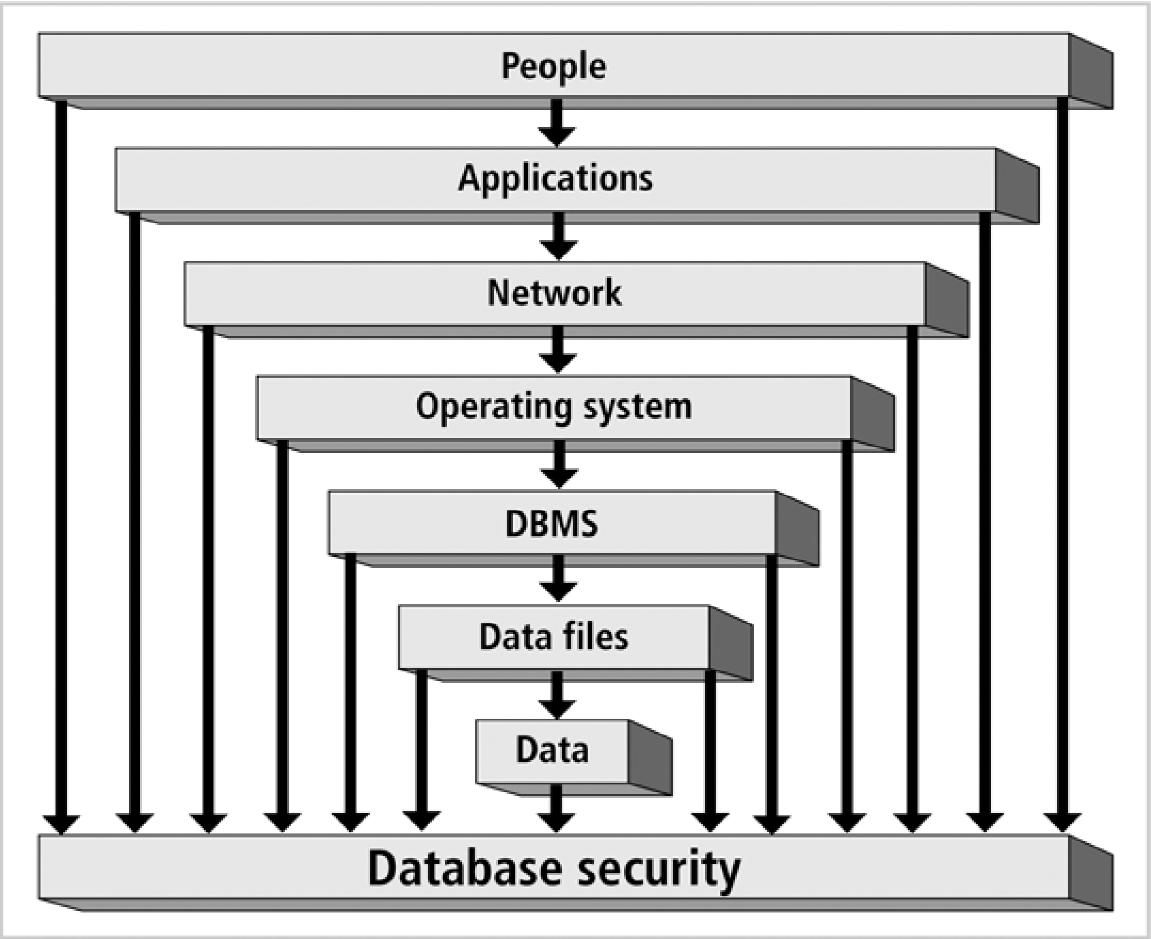


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

DBMS:

- The **logical structure of the database**, which includes **memory**, **executables**, and other **binaries**.

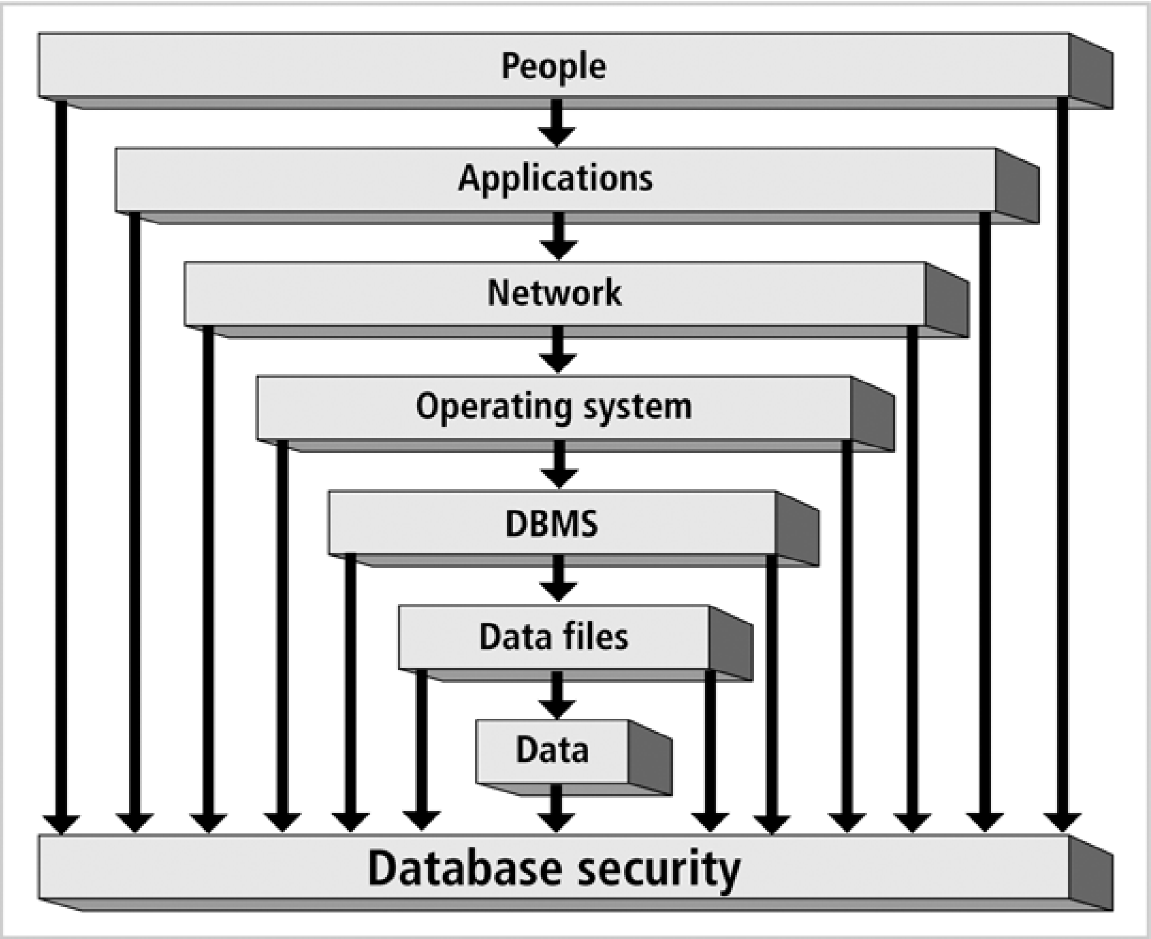


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Data files:

- Access to data files where data resides.
- Data files belonging to the database must be **protected from being accessed by unauthorized individuals** through the use of **permissions** and **encryption**.

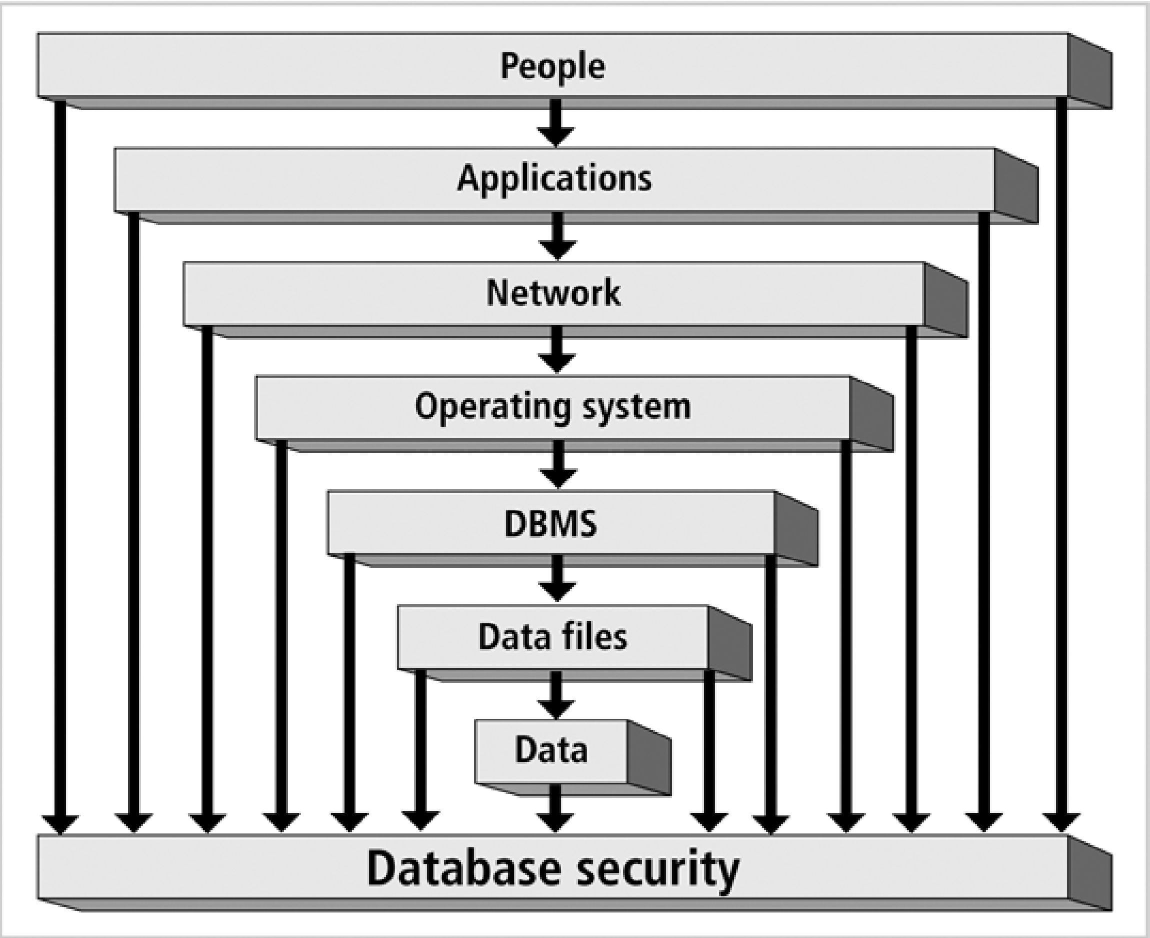


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Data:

- **The data access point deals with:**
  - the data **design** needed to enforce data **integrity**,
  - the **application** implementation needed to ensure **data validity**,
  - the **privileges** necessary to **access data.**

Data requires **highest** level of protection.
Data access point must be **small.**

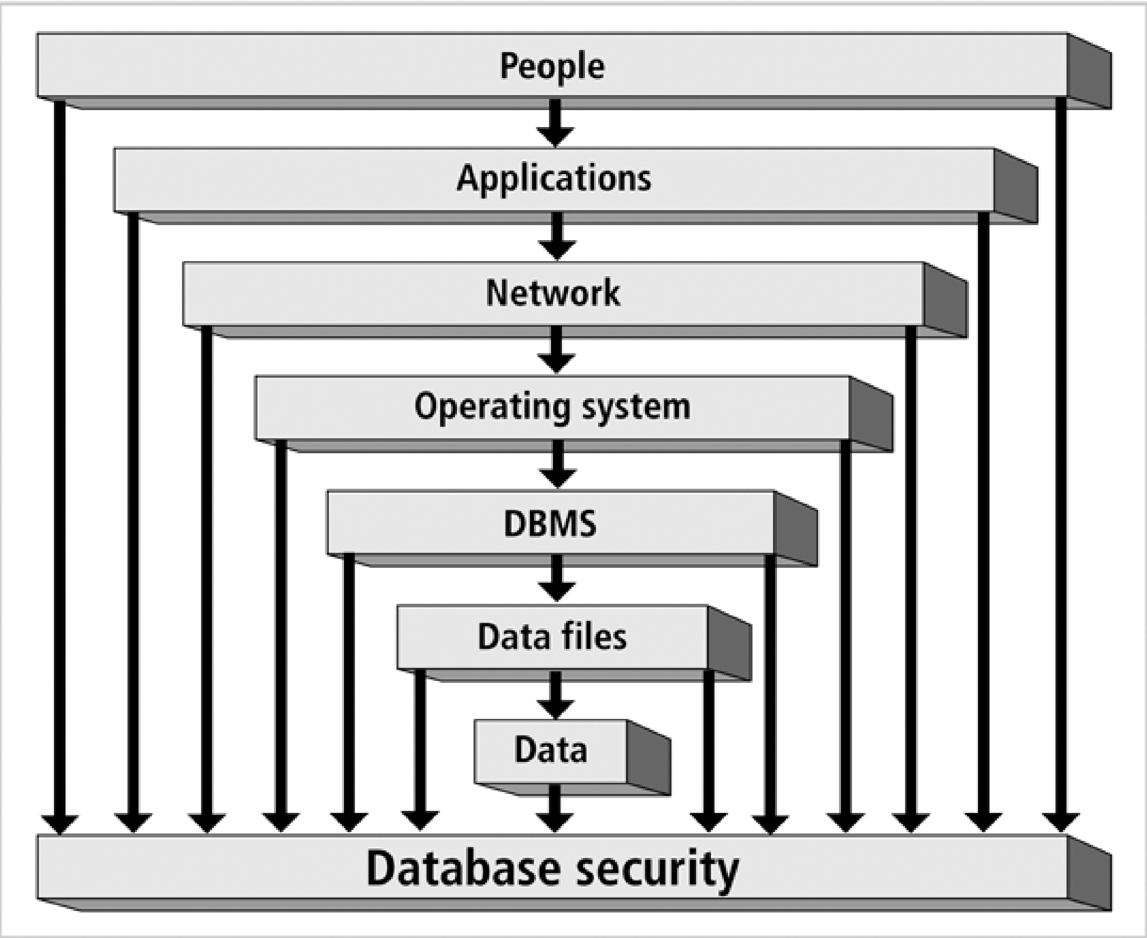


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Notes:

- The proximity of **database security** to the access point indicates **the proximity to database security violations.**
- The **area** of the access point indicates the **security risk**.
- The **people** is the **largest** area because there is a **huge community** of individuals who access data.
- The **data file** access point is smaller than any of the points above it, which means that the **security risks for data files is not as high as at DBMS access points**.

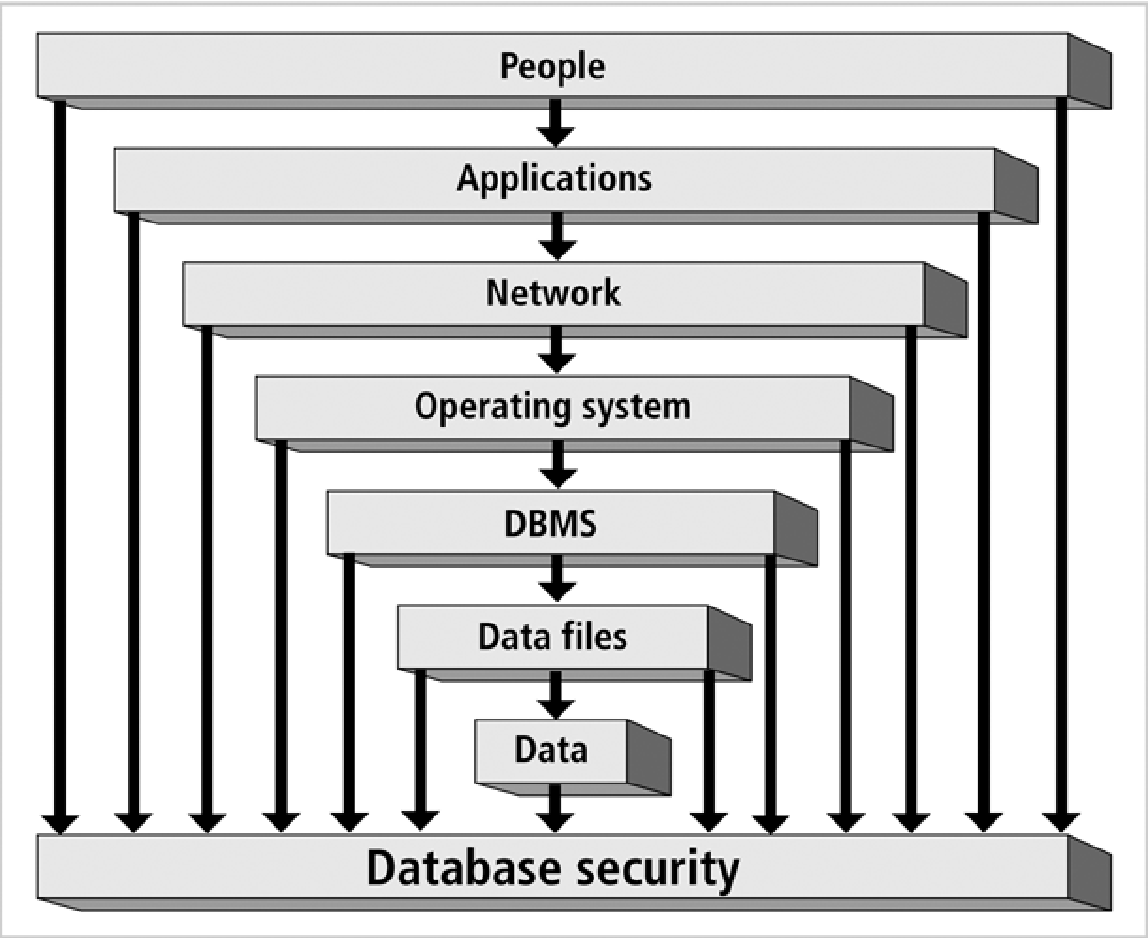


FIGURE 1-8 Database security access points

DATABASE SECURITY ACCESS POINTS

Notes:

- Reducing **DBMS** access points makes the **data files** access point even **less accessible**.
- The **database must be secured**, **starting with** the access points of **people**, followed by applications, and so on.

Reducing access point size reduces security risks, which in turn **increases database security**.

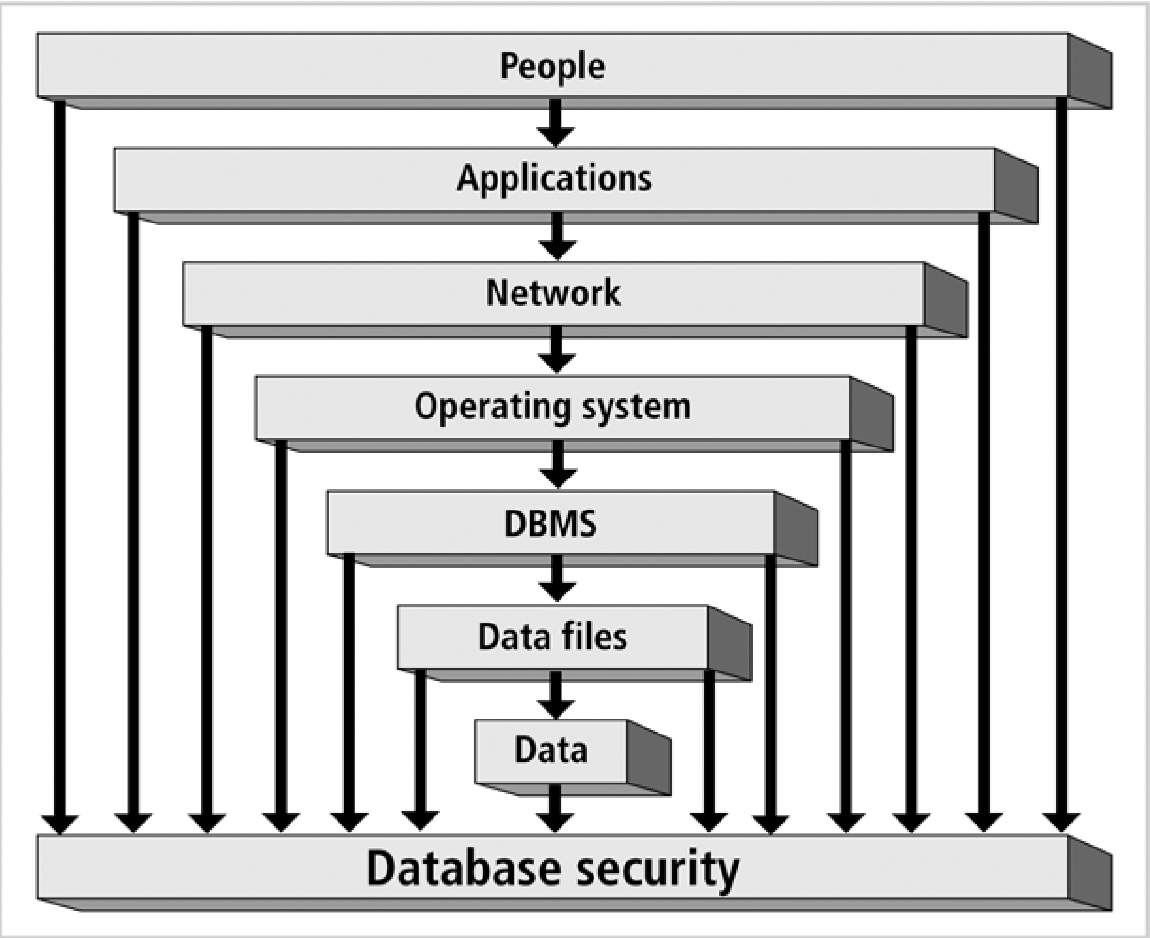
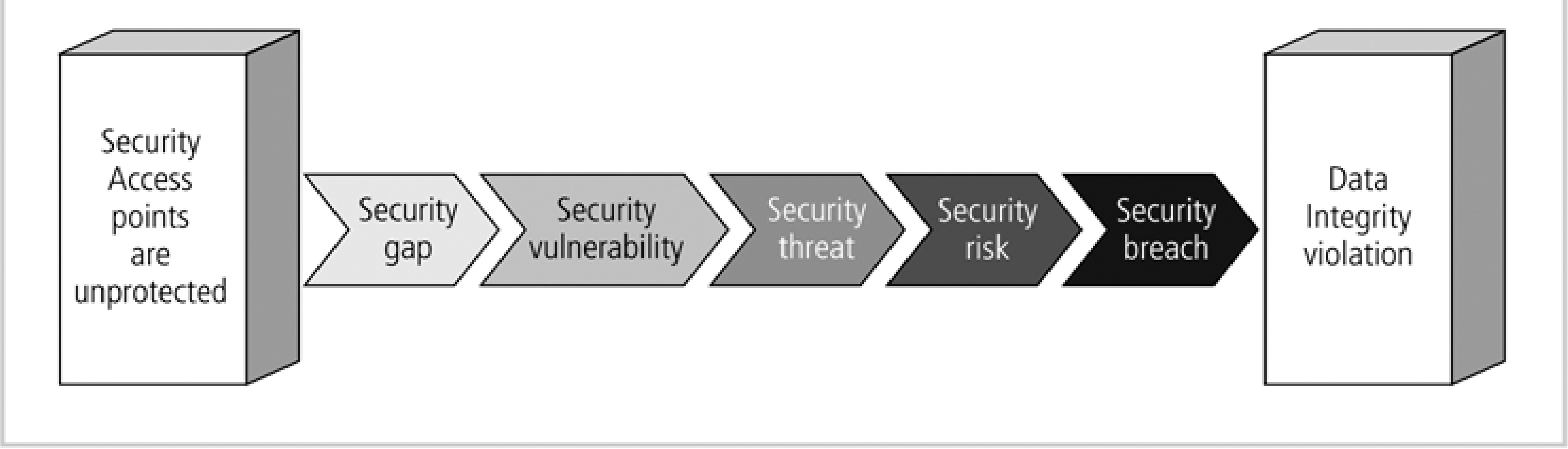


FIGURE 1-8 Database security access points

DATA INTEGRITY VIOLATION PROCESS



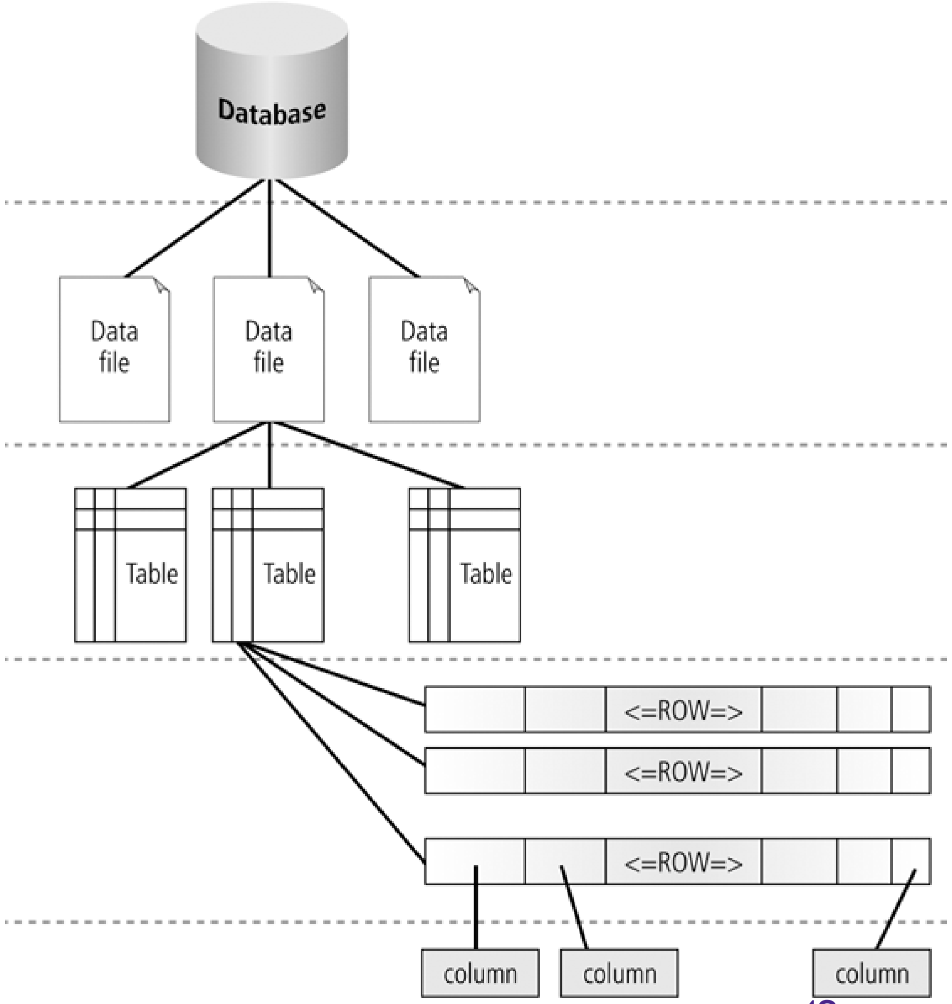
The process of a **security gap eventually resulting in a security breach:**

- **Security access point** is a point at which **security measures are needed** to prevent access that can involve unauthorized actions.
- **Security gaps** are **points** at which **security is missing,** and thus the system is vulnerable.
- **Vulnerabilities** are **kinks in the system** that must be watched because they can become threats.
- **A threat** is defined as a **security risk** that can become a system breach.
- **The breach** can be caused by either intentional or unintentional actions.

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)

- The structure of the database is organized in **levels**
- Each level can be **protected** by a different **security mechanism.**



DATABASE SECURITY LEVELS

- A **column** can be protected by using a **VIEW** object.
- A **table** is protected through the functionality of the database system, which allows schema owners to **grant or revoke privileges**.
- The **data files** are protected by the database and that protection is enforced by **operating system file permissions**.

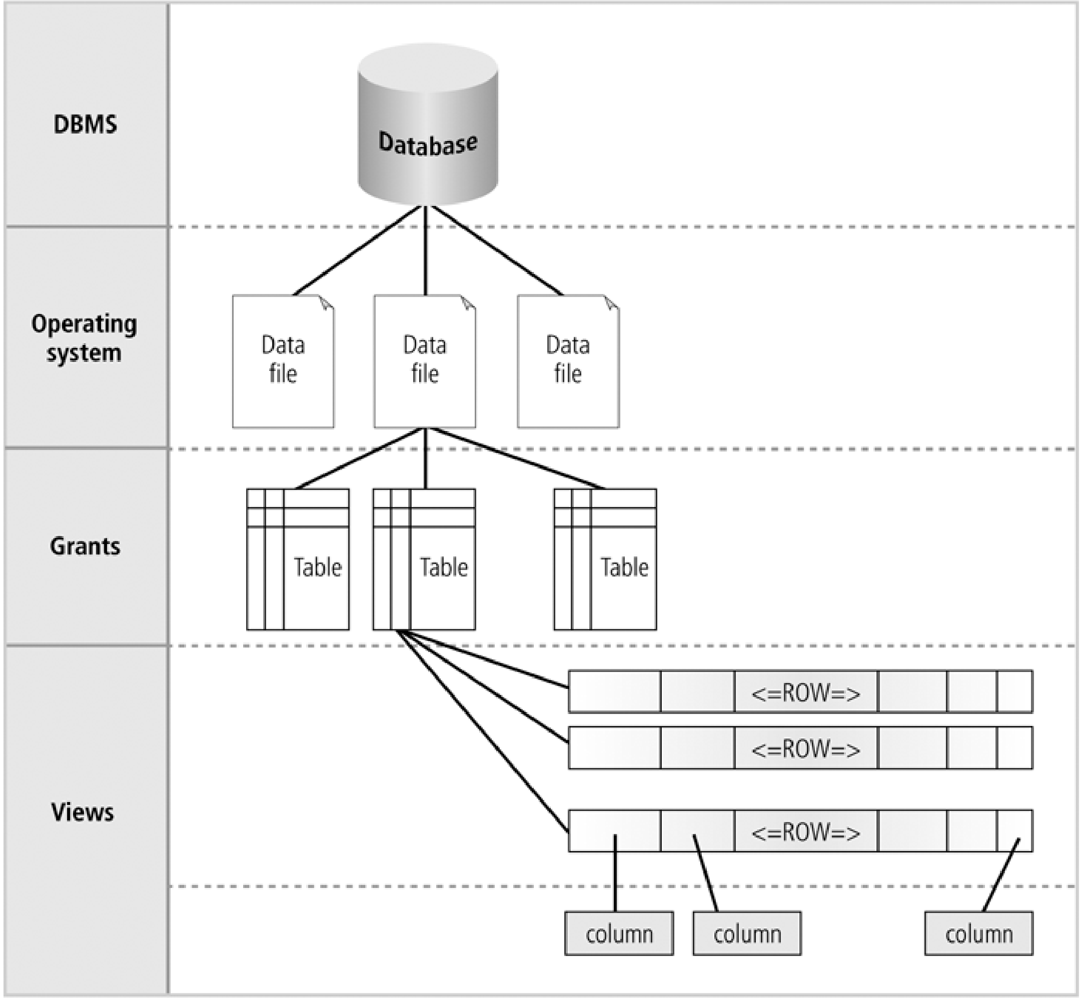


FIGURE 1-11 Levels of database security

DATABASE SECURITY LEVELS

- The **database** is secured by the **database management system** through:
  - the use of **user accounts and passwords**
  - the **privileges and permissions** of the main database **functions**
  - database **backup** and **recovery**
  - etc.

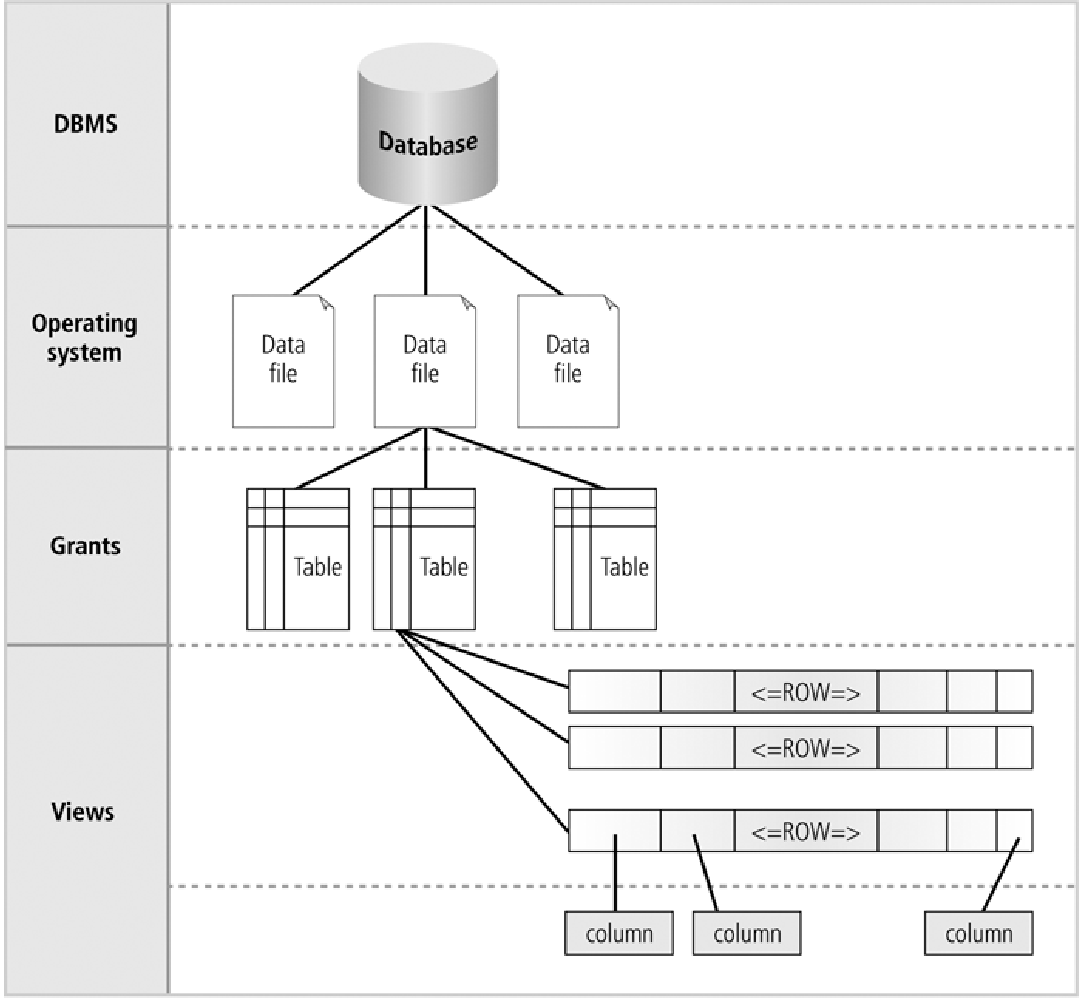


FIGURE 1-11 Levels of database security

MENACES TO DATABASES

The kinds of menaces to database security are:

- **Security vulnerability**
- **Security threat**
- **Security risk**

SECURITY VULNERABILITY

- Security vulnerability is a **weakness** in any of the information system **components** that can be exploited to violate the **integrity**, **confidentiality**, or **accessibility** of the system
- Intruders and attackers exploit vulnerabilities in the environment to start their attacks.
- Hackers **explore the weak points** of a system until they **gain entry** through a **gap** in protection and then they do their attacks on the system.

TYPES OF VULNERABILITIES

Installation and configuration

- Results from:
  - using a default installation and configuration that is known publicly and does not enforce any security measures.
  - improper configuration or installation.
- **Examples:**
  - Failure to change default passwords
  - Failure to change default permissions and privileges

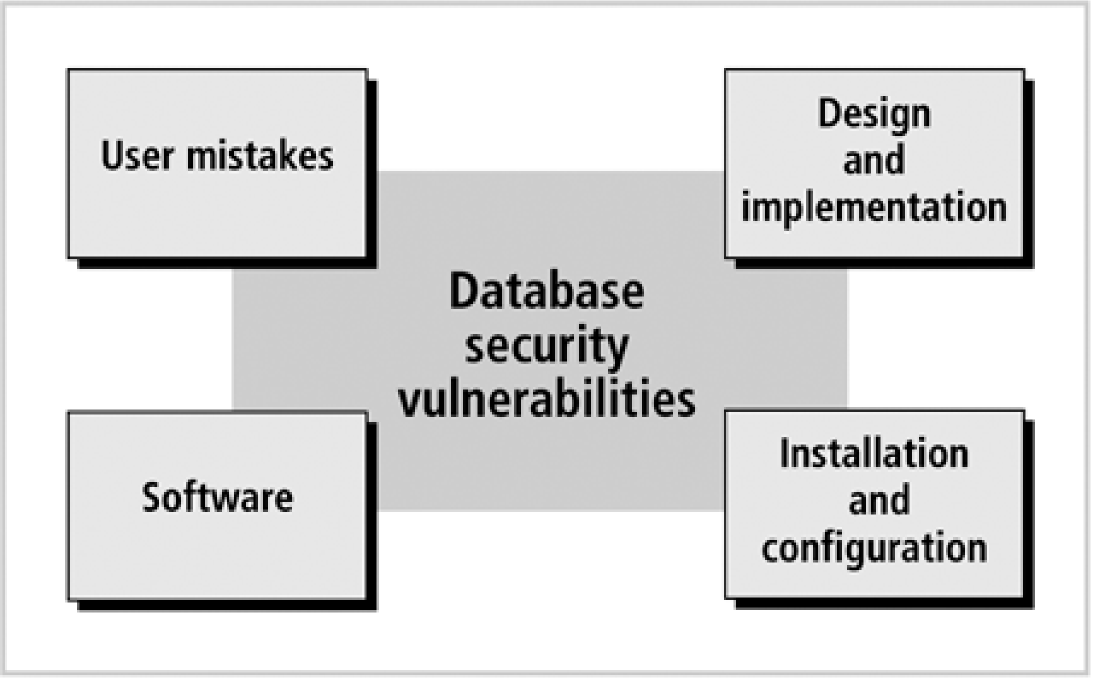

User mistakes
Design and implementation
Database security vulnerabilities
Software
Installation and configuration

FIGURE 1-12 Categories of database security vulnerablilities

TYPES OF VULNERABILITIES

User mistakes:

- Carelessness in implementing procedures and failure to follow through
- Accidental errors

- **Examples:**
  - Lack of auditing controls
  - Untested disaster recovery plan
  - Lack of activity monitoring malicious code
  - Bad authentication
  - Lack of protection against Social Engineering

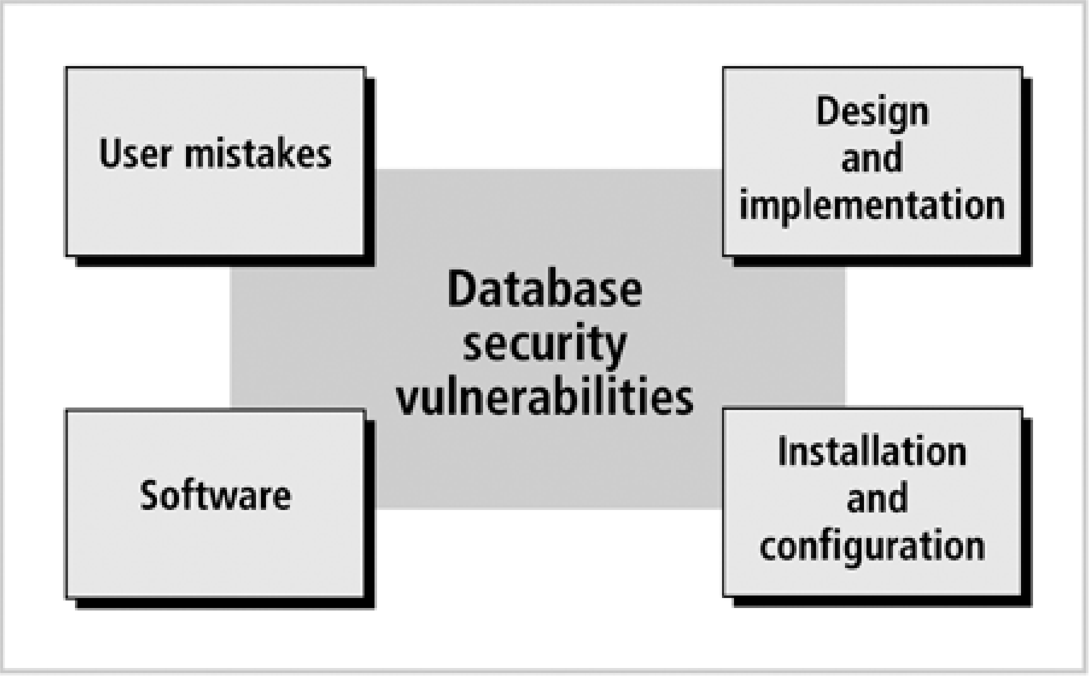

User mistakes
Design and implementation
Database security vulnerabilities
Software
Installation and configuration

FIGURE 1-12 Categories of database security vulnerablilities

TYPES OF VULNERABILITIES

Software:

- Vulnerabilities found in software for all types of programs (applications, operating systems, database management systems, and other programs).

- **Examples:**
  - Software contains bugs
  - System administrators do not keep track of patches

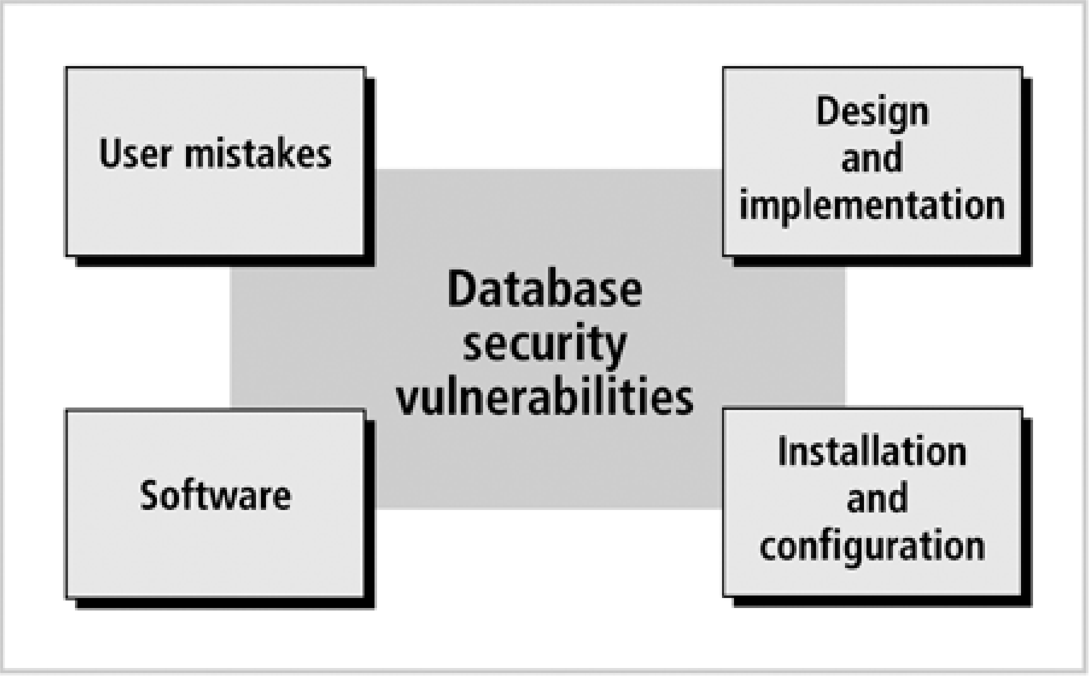

User mistakes
Design and implementation
Database security vulnerabilities
Software
Installation and configuration

FIGURE 1-12 Categories of database security vulnerablilities

TYPES OF VULNERABILITIES

Design and implementation

- Improper software analysis and design as well as coding problems.

- **Examples:**
  - System design errors
  - Exceptional conditions and errors are not handled
  - Input data is not validated

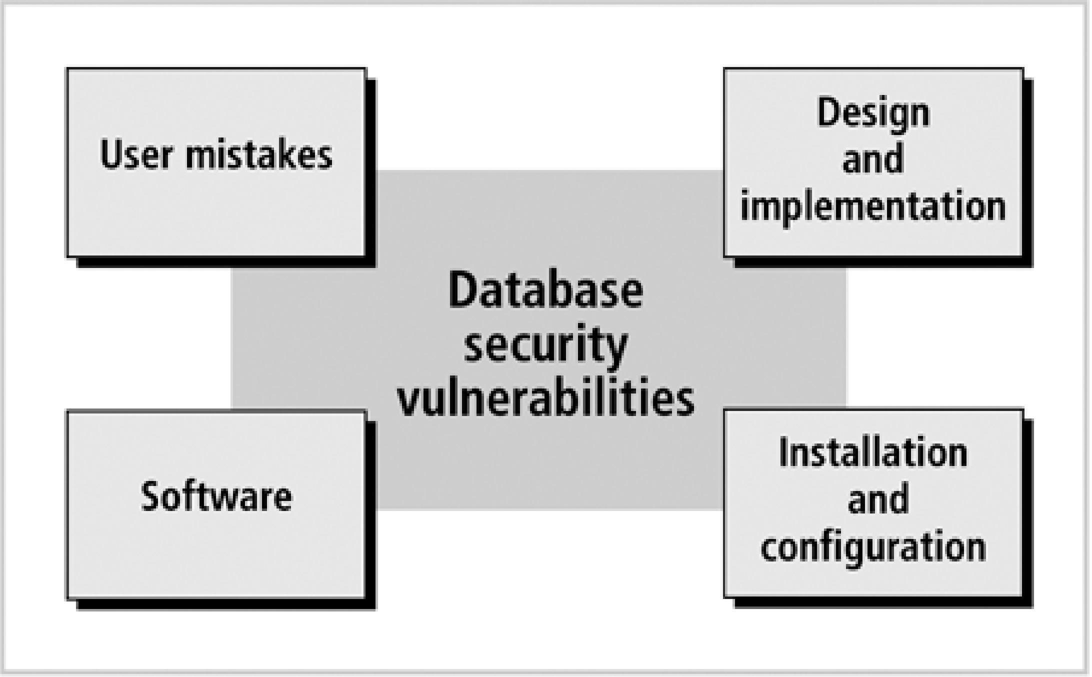

User mistakes
Design and implementation
Database security vulnerabilities
Software
Installation and configuration

FIGURE 1-12 Categories of database security vulnerablilities

SECURITY THREAT

- Security threat is a **security violation or attack** that **can happen** any time **because of a security vulnerability**
- Vulnerabilities can escalate into threats.

TYPES OF THREATS

People:

- People inflict damage, violation, or destruction to all or any of the database environment components.

- **Examples:**
  - Employees
  - Visitors
  - Hackers
  - Social engineers

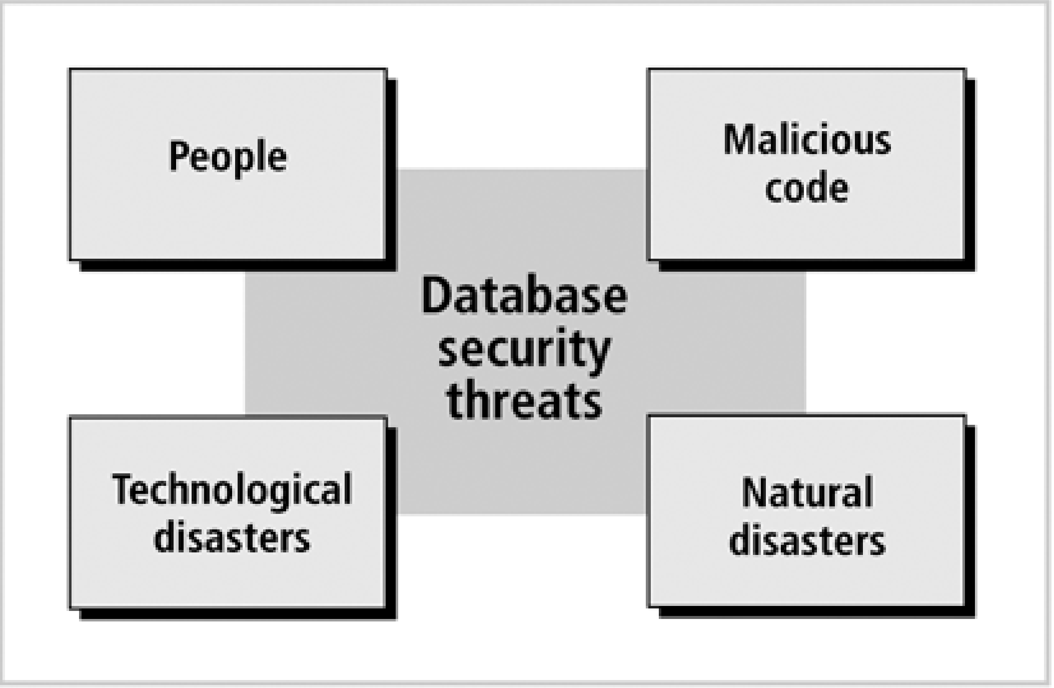


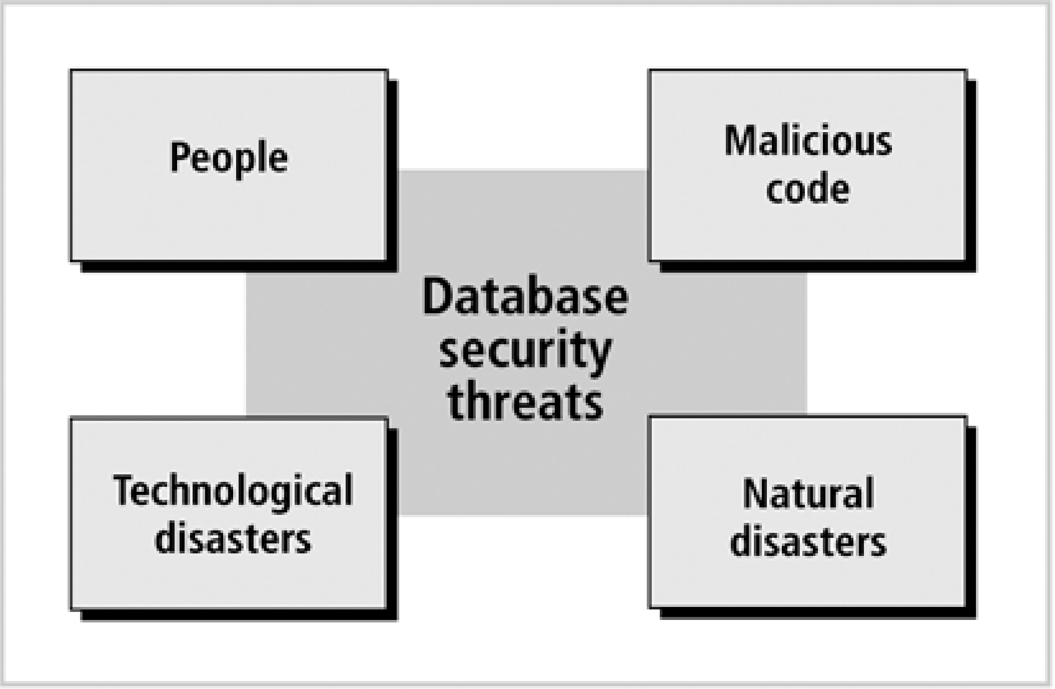
FIGURE 1-13 Categories of database security threats

TYPES OF THREATS

Malicious code

- Software code that is written to damage or violate one or more of the database environment.

- **Examples:**
  - Viruses
  - Trojan horses
  - Spoofing code
  - Denial-of-service flood



People

Malicious code

Database security threats

Technological disasters

Natural disasters

FIGURE 1-13 Categories of database security threats

TYPES OF THREATS

Natural disasters:

- Calamities caused by nature, which can destroy any or all of the database environment components.

- **Examples:**
  - Tornados
  - Earthquakes
  - Fire

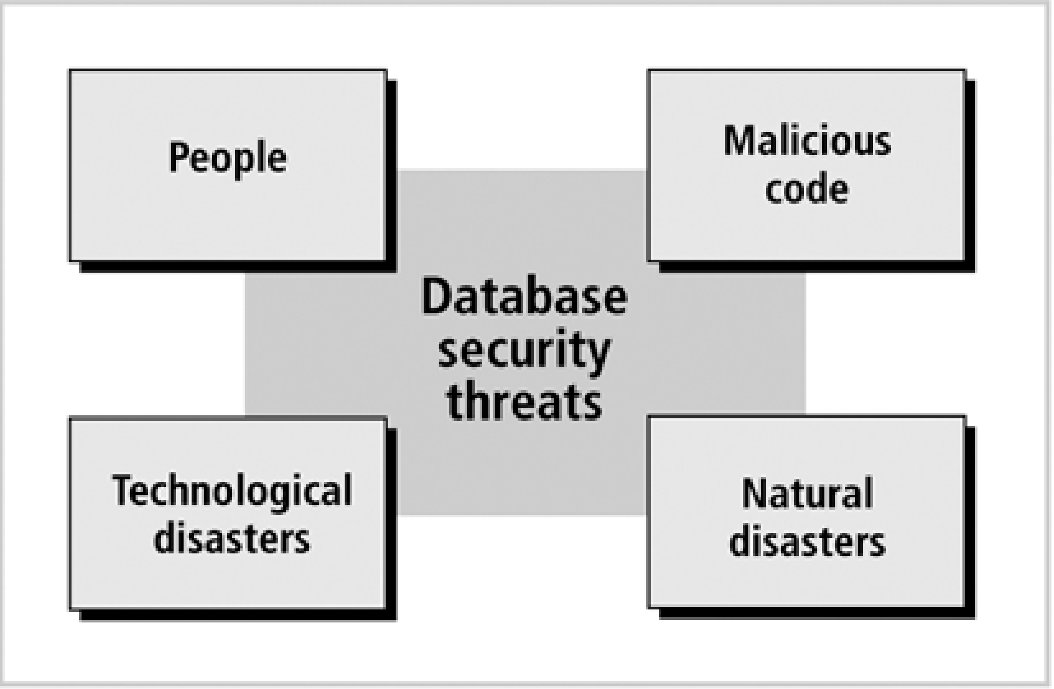


FIGURE 1-13 Categories of database security threats

TYPES OF THREATS

Technological disasters:

- Often caused by some sort of malfunction in equipment or hardware. Technological disasters can inflict damage to networks, operating systems, database management systems, data files, or data.

- **Examples:**
  - Power failure
  - Media failure
  - Hardware failure
  - Network failure

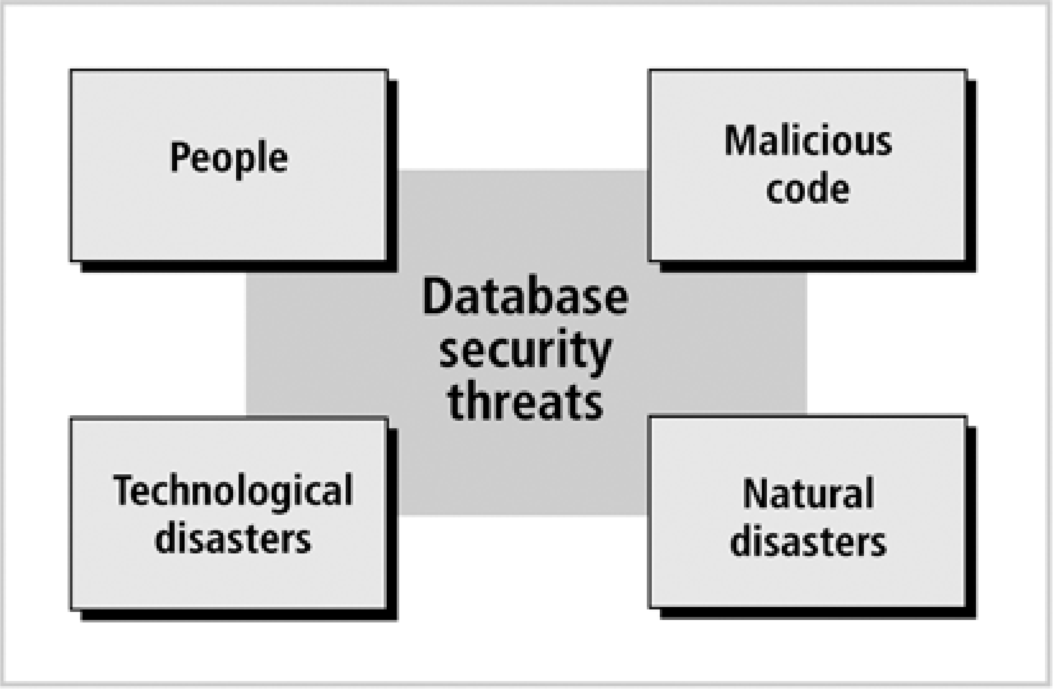


FIGURE 1-13 Categories of database security threats

SECURITY RISK

- **Security risk** is a **known security gap** that a company **leaves open.**
- The **probability** of these threats occurring should be diminished.

TYPES OF RISKS

People

- The loss of people who know critical information about the environment can create risks.

- **Examples:**
  - Loss of key persons (resignation, migration, health problems)
  - Key person downtime due to sickness, personal or family problems, or burnout

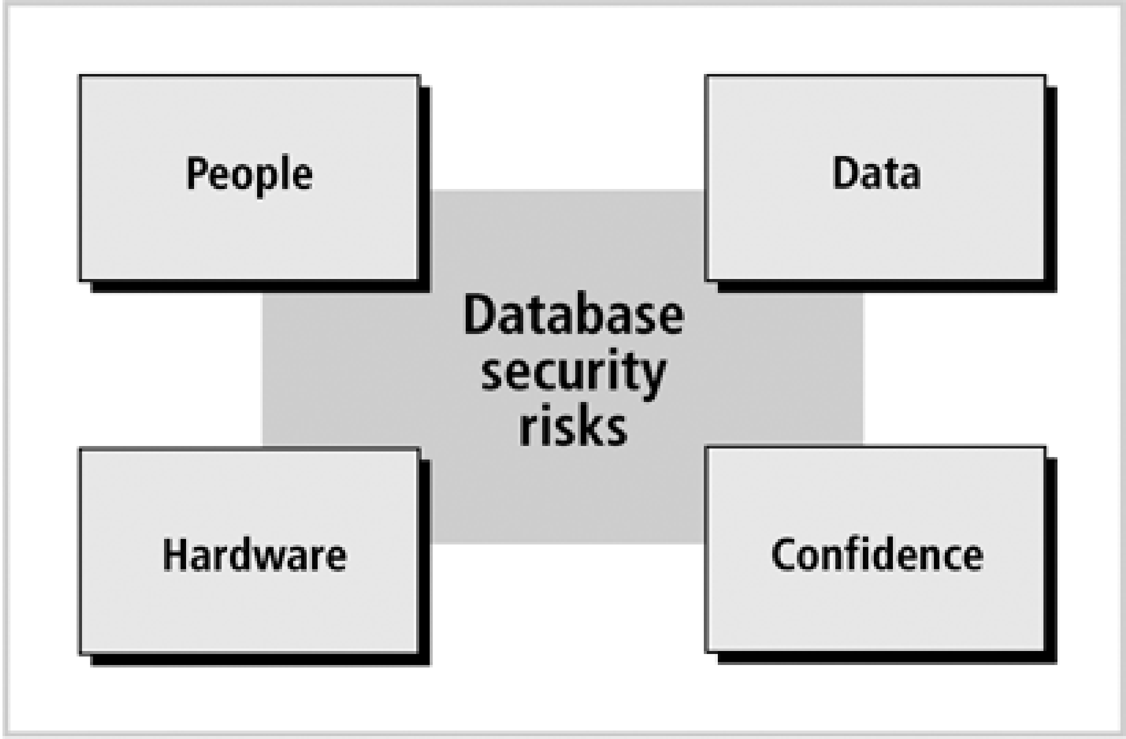


FIGURE 1-14 Categories of database security risks

TYPES OF RISKS

Hardware

- A risk that mainly results in hardware unavailability or inoperability.

- **Example:**
  - Downtime due to hardware failure, malfunction, or inflicted damage
  - Failure due to unreliable or poor-quality equipment

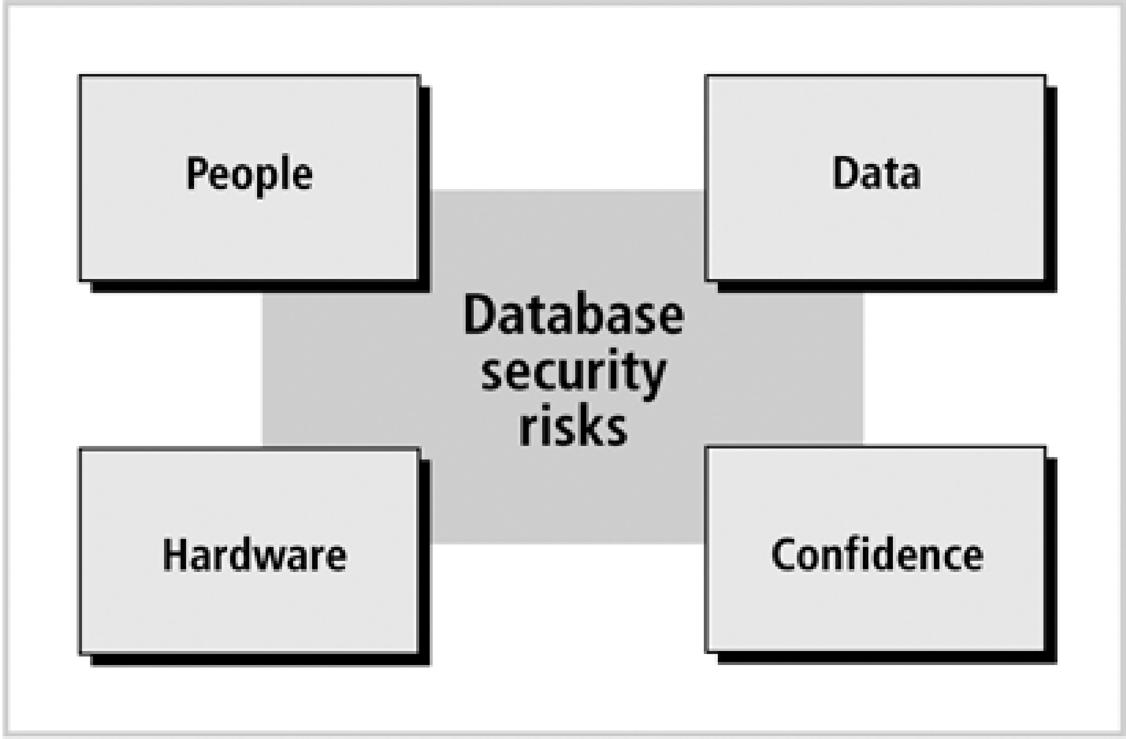


FIGURE 1-14 Categories of database security risks

TYPES OF RISKS

Data:

- Data loss and data integrity loss is a major concern of the database administrators and management

- **Examples:**
  - Data loss
  - Data corruption
  - Data privacy loss

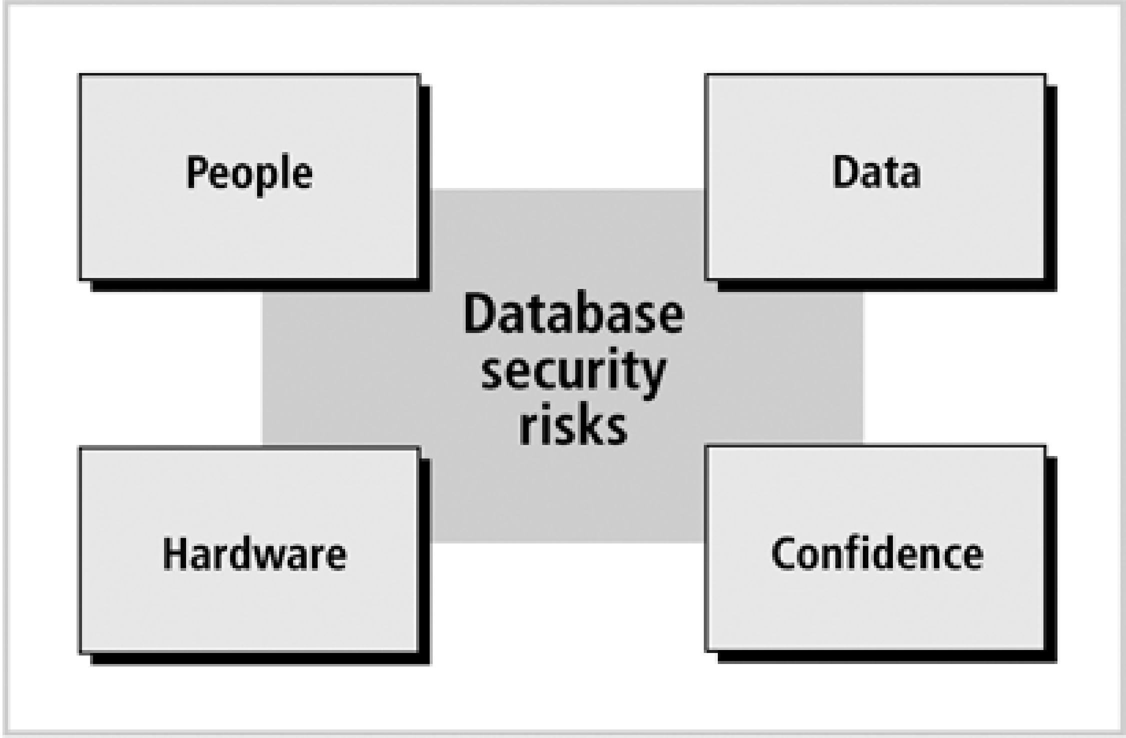


FIGURE 1-14 Categories of database security risks

TYPES OF RISKS

Confidence

- The loss of public confidence in the data produced by the company causes a loss of public confidence in the company itself.

- **Examples:**
  - Loss of procedural and policy documents
  - Database performance degradation
  - Fraud
  - Confusion and uncertainty about database information

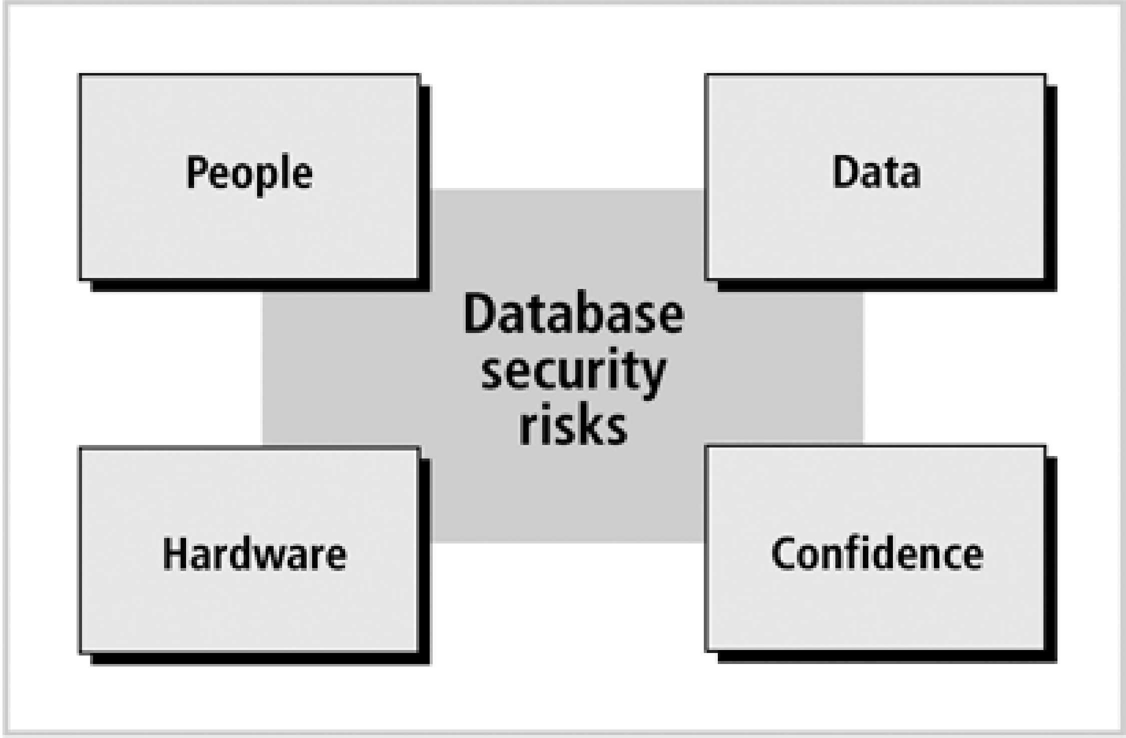


FIGURE 1-14 Categories of database security risks

INTEGRATION OF SECURITY VULNERABILITIES, THREATS, AND RISKS IN A DATABASE ENVIRONMENT

- **Three key factors** are considered when rating vulnerabilities, threats, and risks :
  - **People**
  - **Software**
  - **Data**
- Database security involves the protection of these factors.

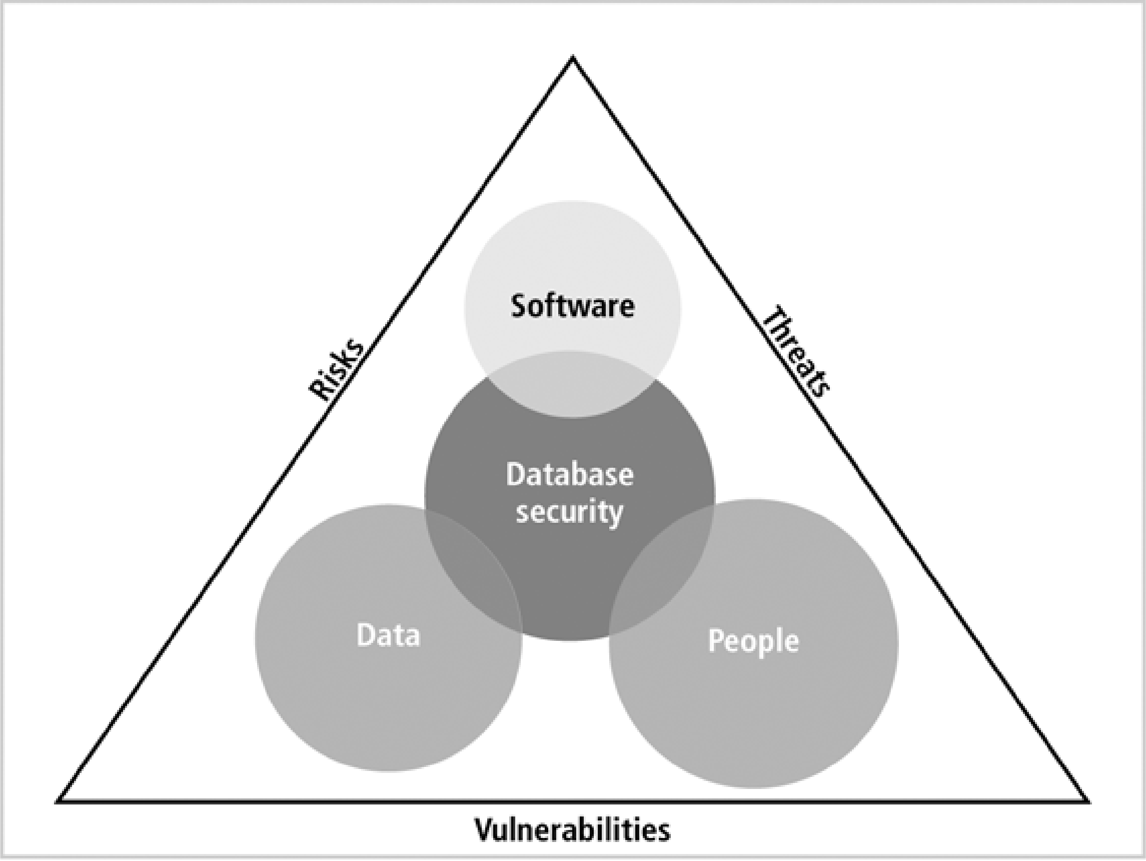


FIGURE 1-15 Integration of security vulnerabilities, threats, and risks in a database environment

SECURITY METHODS

SECURITY METHODS

- **Security technology** comprises a variety of **methods** that protect **specific aspects of security architecture**.

METHODS FOR PROTECTING COMPONENTS OF A DATABASE ENVIRONMENT

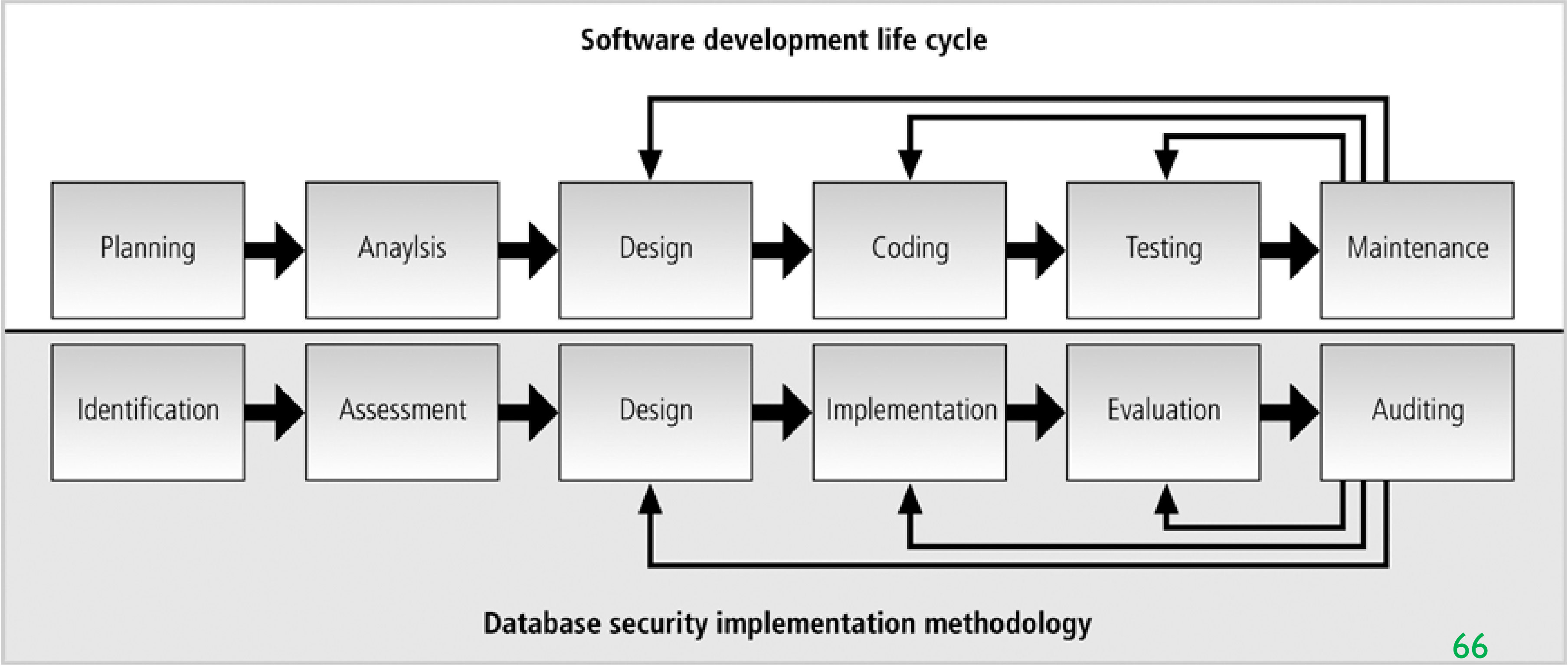
Database Component Protected	Examples of Security Methods
People	▪ Physical limits on access to hardware and documents ▪ Processes of identification and authentication ▪ Use of devices, such as ID cards, eye scans, and passwords to make certain that the individual is who he claims to be ▪ Training courses on the importance of security
Applications	▪ Authentication of users who access applications ▪ Business rules
Network	▪ Firewalls to block network intruders ▪ Virtual private network (VPN) (a remote computer securely connected to a corporate network) ▪ Authentication

METHODS FOR PROTECTING COMPONENTS OF A DATABASE ENVIRONMENT

Database Component Protected	Examples of Security Methods	
Operating system	▪ User accounts ▪ Authentication	▪ Password policy ▪ Intrusion detection
Database management system	▪ Authentication ▪ Audit mechanism	▪ Database resource limits ▪ Password policy
Data files	▪ File permissions ▪ Access monitoring	
Data	▪ Data validation ▪ Data constraints	▪ Data encryption ▪ Data access

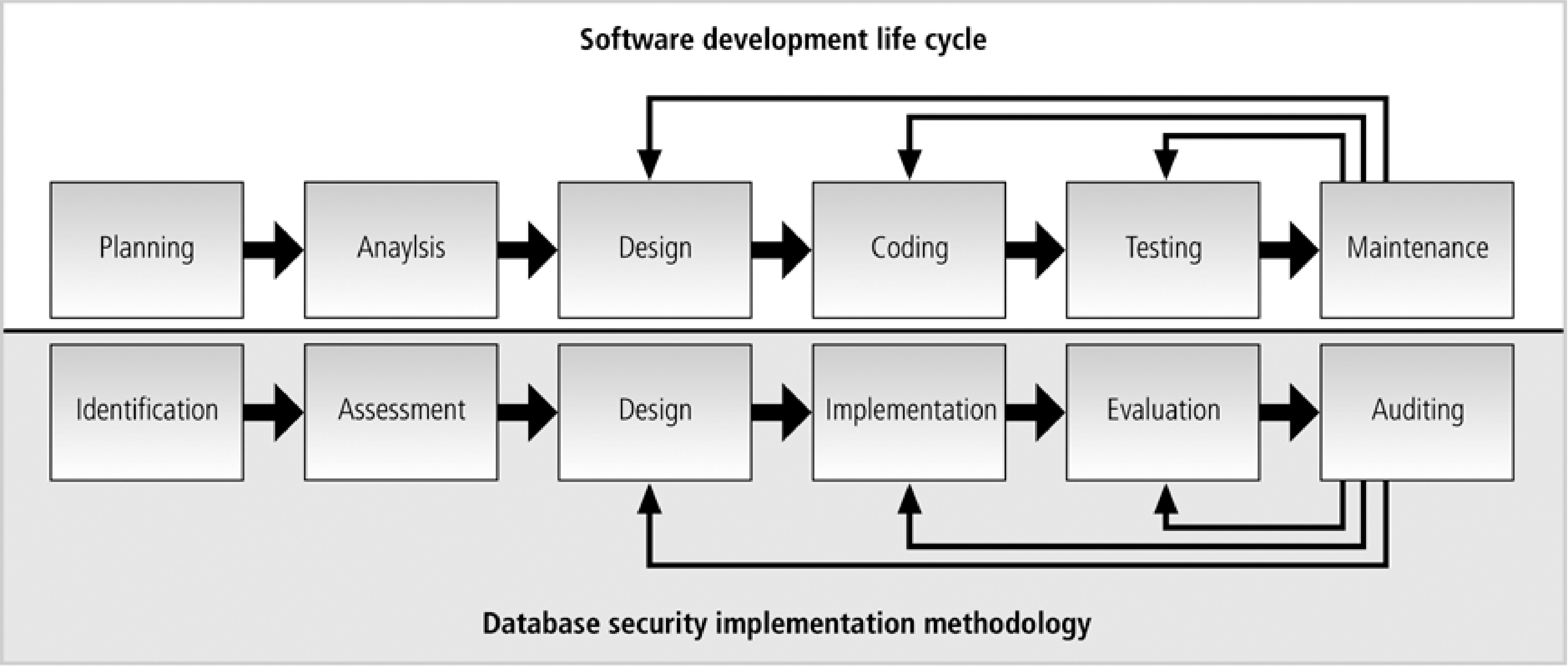
DATABASE SECURITY METHODOLOGY

- **Phases in the database security methodology** correspond to those of the **Software Development Life Cycle** (SDLC).
- **Phases of the database security methodology:**
  - Identification
  - Assessment
  - Design
  - Implementation
  - Evaluation
  - Auditing



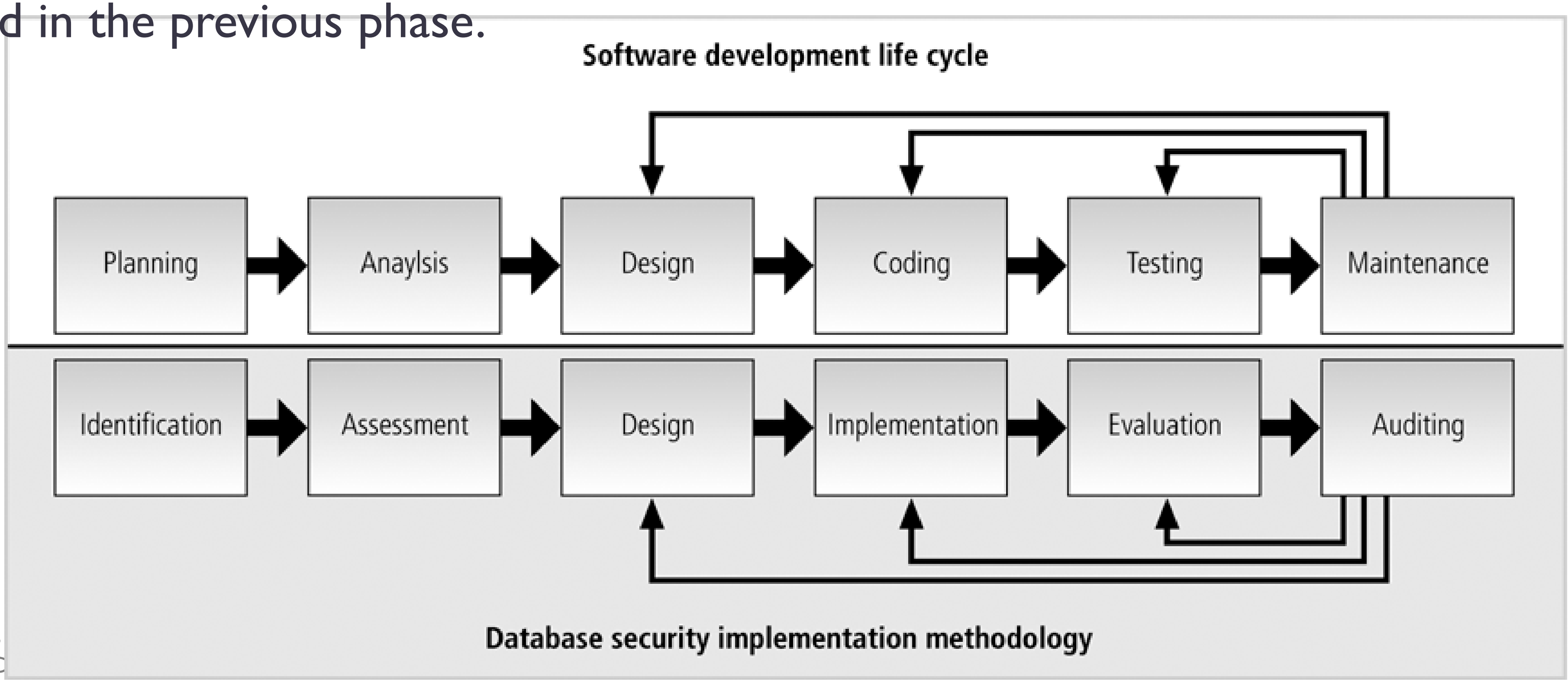
DATABASE SECURITY METHODOLOGY

- **Identification:** Identification and investigation of **resources required** and **policies** to be adopted.
- **Assessment: Analysis of vulnerabilities**, **threats**, and **risks** for both aspects of database security: **physical** (data files and data) and **logical** (codes).



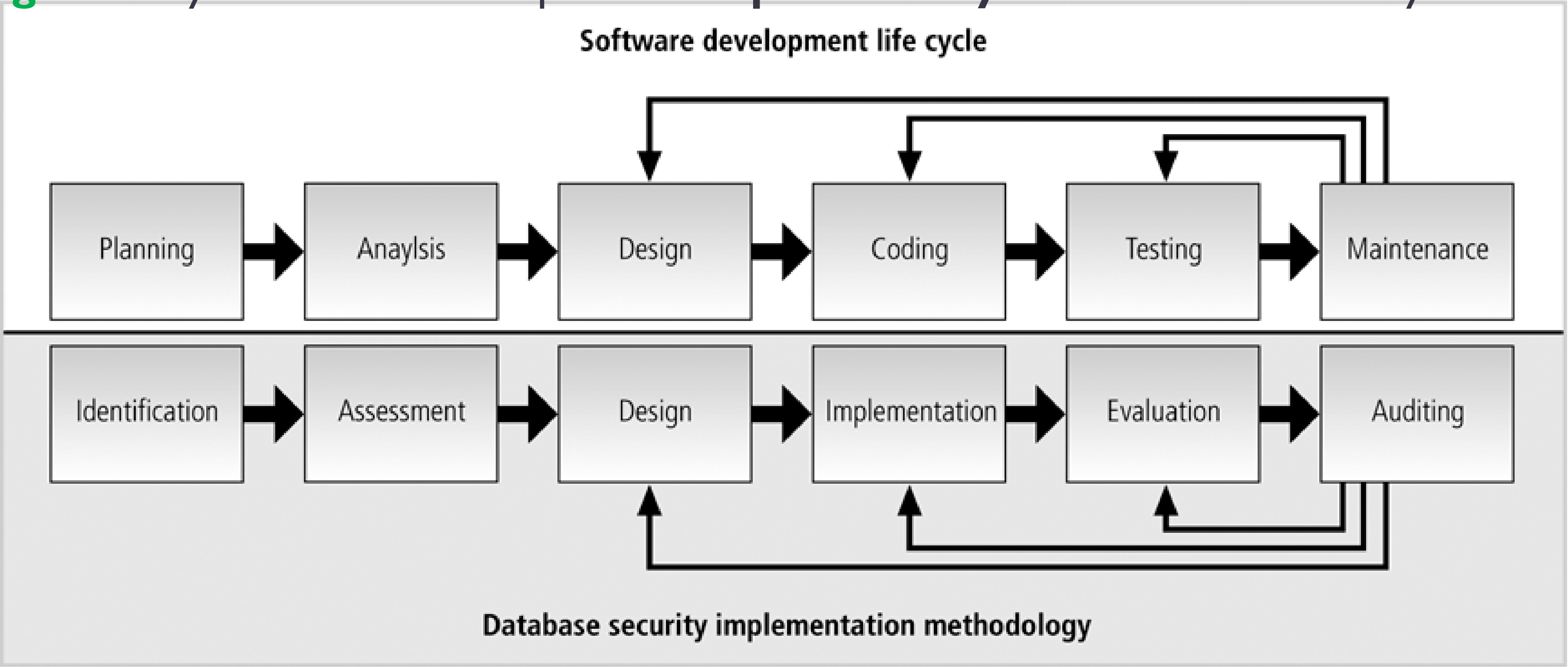
DATABASE SECURITY METHODOLOGY

- **Design:** This phase results in a blueprint of the **adopted security model** that is used to enforce security (**how security measures are implemented**).
- **Implementation:** **Code** is developed or **tools** are purchased to implement the blueprint outlined in the previous phase.



DATABASE SECURITY METHODOLOGY

- **Evaluation:** Evaluate the security implementation by **testing system against software attacks**, **hardware failures**, **natural disasters**, and **human errors** (determination of the system's **degree of security**).
- **Auditing:** Security audits should be performed **periodically** to ensure the security state of the system.



DATABASE SECURITY DEFINITION

Database security 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. These components include people, applications, networks, operating systems, database management systems, data files, and data.

REFERENCES

- Hassan, A. Afyouni. *Database security and auditing: Protecting data integrity and accessibility*.