Database Security and Auditing: Protecting Data Integrity and Accessibility

*Chapter 1 Security Architecture*

# Objectives

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

# Objectives (continued)

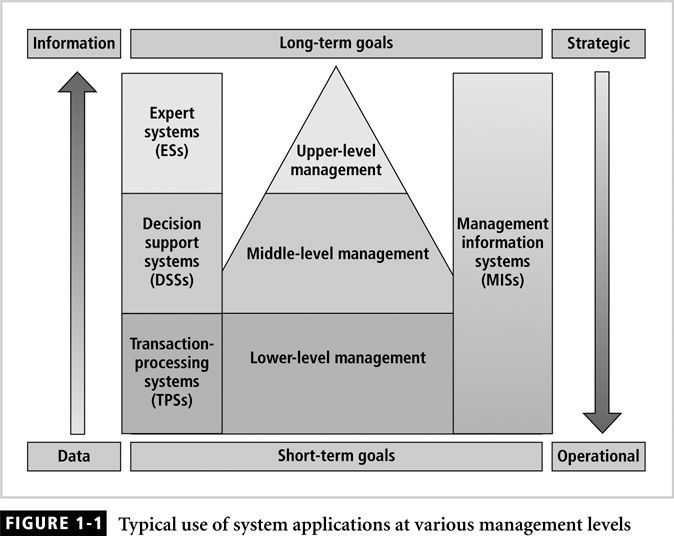
* Identify the major components of information security architecture
* Define database security
* List types of information assets and their values
* Describe security methods

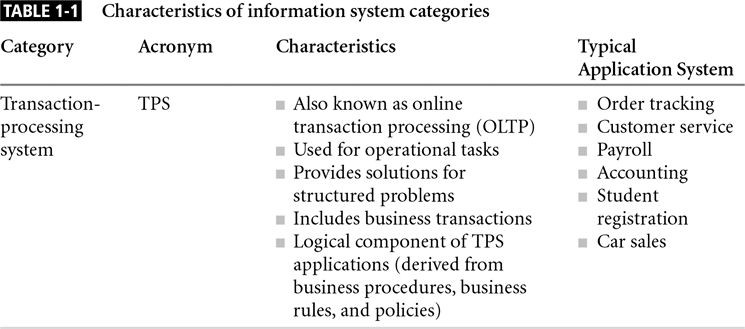
# Security

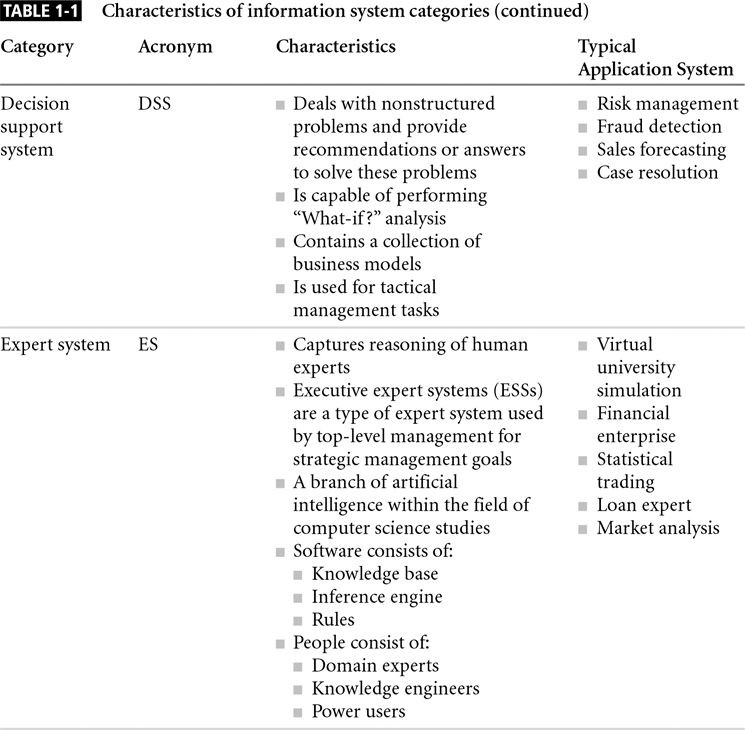
* Database security: degree to which data is fully protected from tampering or unauthorized acts
* Comprises information system and information security concepts

# Information Systems

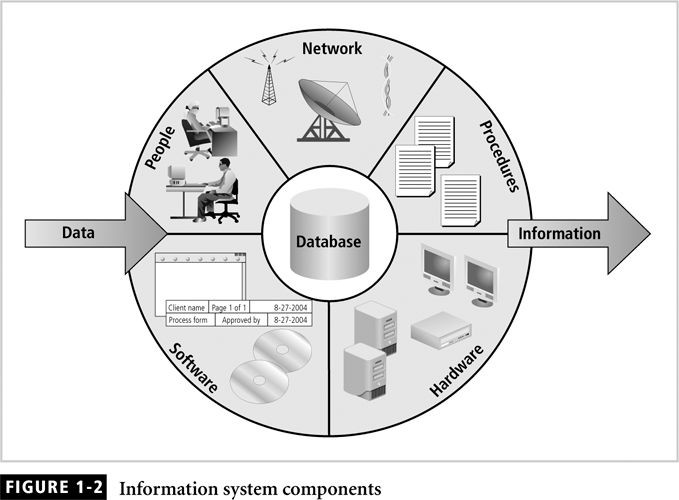
* Wise decisions require:
  + Accurate and timely information
  + Information integrity
* Information system: comprised of components working together to produce and generate accurate information
* Categorized based on usage



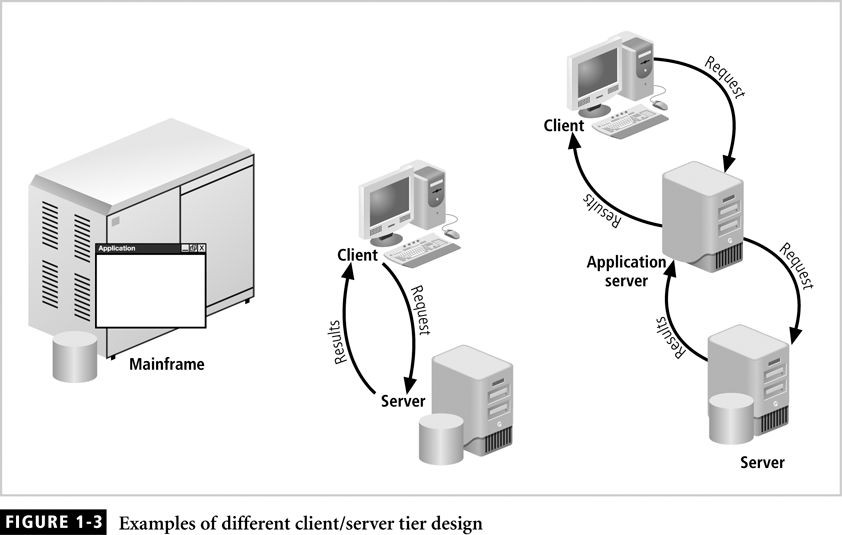




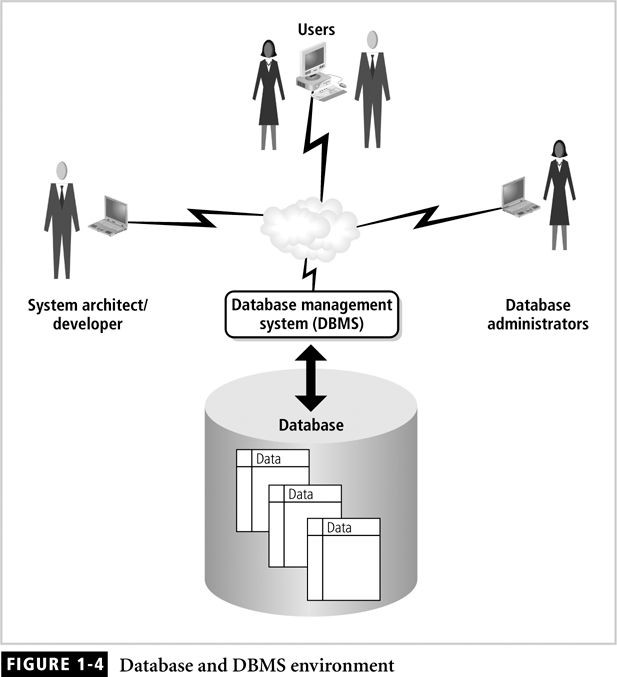
* Information system components include:
  + Data
  + Procedures
  + Hardware
  + Software
  + Network
  + People



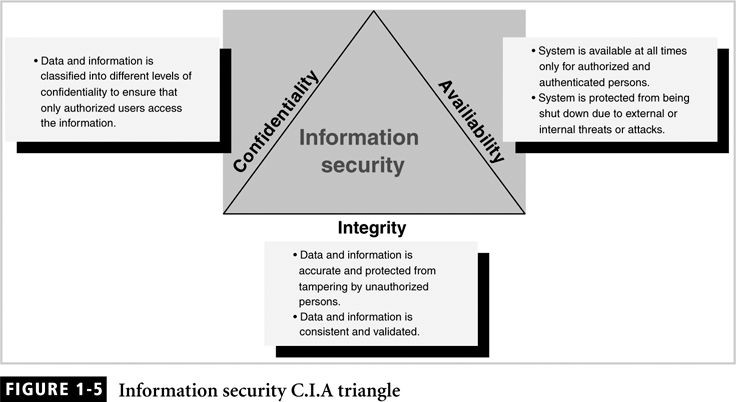
* Client/server architecture:
  + Based on the business model
  + Can be implemented as one-tier; two-tier; n-tier
  + Composed of three layers
* Tier: physical or logical platform
* Database management system (DBMS): collection of programs that manage database



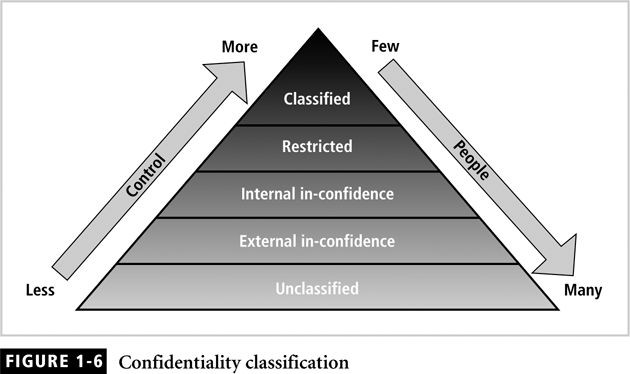
* Essential to success of information system
* DBMS functionalities:
  + Organize data
  + Store and retrieve data efficiently
  + Manipulate data (update and delete)
  + Enforce referential integrity and consistency
  + Enforce and implement data security policies and procedures
  + Back up, recover, and restore data
* DBMS components include:
  + Data
  + Hardware
  + Software
  + Networks
  + Procedures
  + Database servers



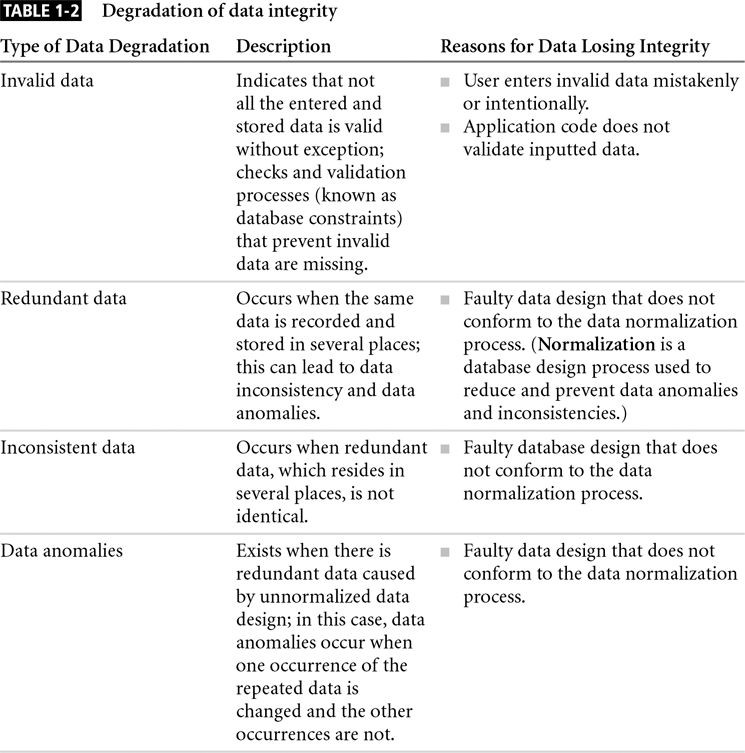
* Information is one of an organization’s most valuable assets
* Information security: consists of procedures and measures taken to protect information systems components
* C.I.A. triangle: confidentiality, integrity, availability
* Security policies must be balanced according to the C.I.A. triangle

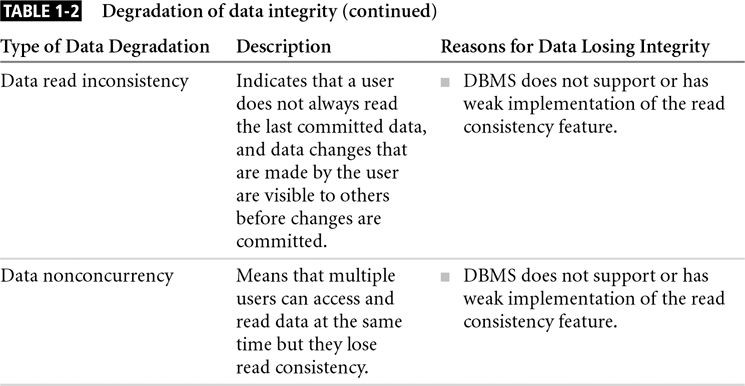


* Addresses two aspects of security:
  + Prevention of unauthorized access
  + Information disclosure based on classification
* Classify company information into levels:
  + Each level has its own security measures
  + Usually based on degree of confidentiality necessary to protect information

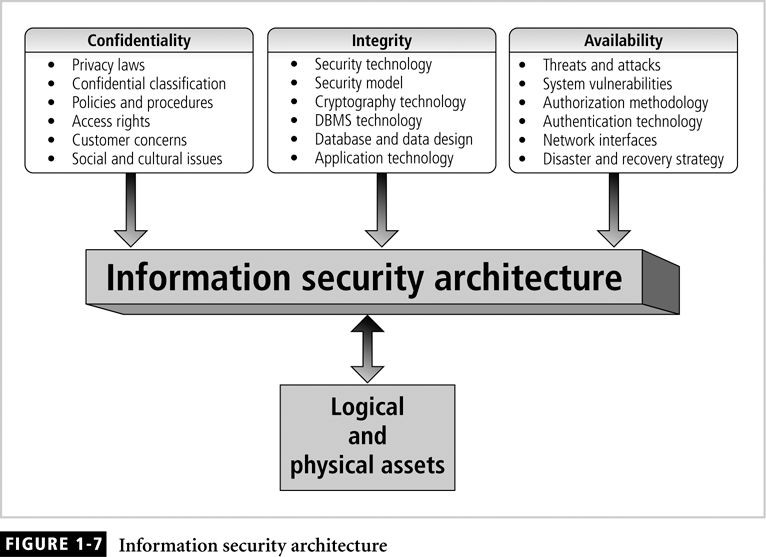


* Consistent and valid data, processed correctly, yields accurate information
* Information has integrity if:
  + It is accurate
  + It has not been tampered with
* Read consistency: each user sees only his changes and those committed by other users





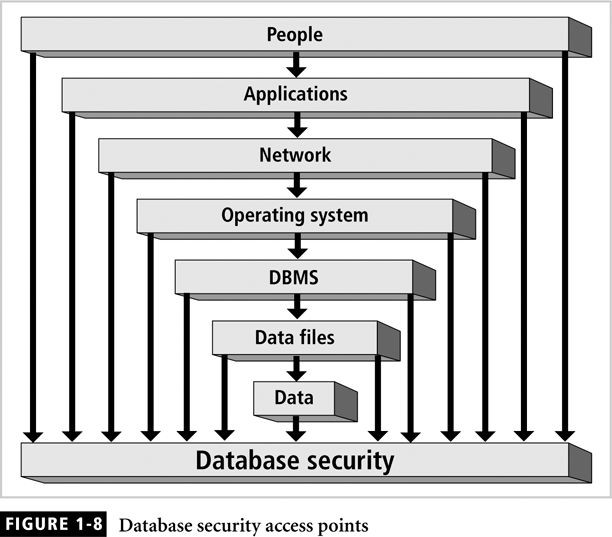
* Systems must be always available to authorized users
* Systems determines what a user can do with the information
* Reasons for a system to become unavailable:
  + External attacks and lack of system protection
  + System failure with no disaster recovery strategy
  + Overly stringent and obscure security policies
  + Bad implementation of authentication processes
* 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



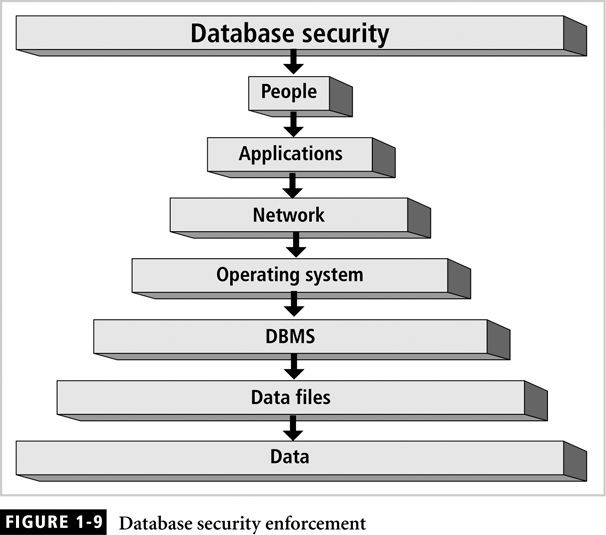
* Components include:
  + Policies and procedures
  + Security personnel and administrators
  + Detection equipments
  + Security programs
  + Monitoring equipment
  + Monitoring applications
  + Auditing procedures and tools

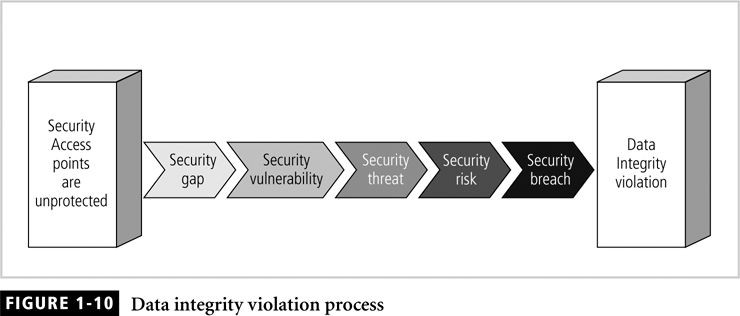
# Database Security

* 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

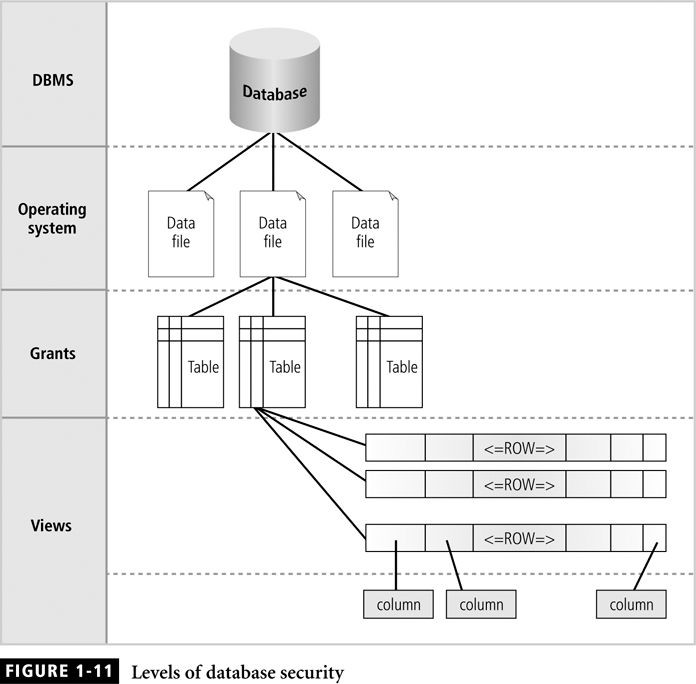


* Reducing access point size reduces security risks
* Security gaps: points at which security is missing
* Vulnerabilities: kinks in the system that can become threats
* Threat: security risk that can become a system breach

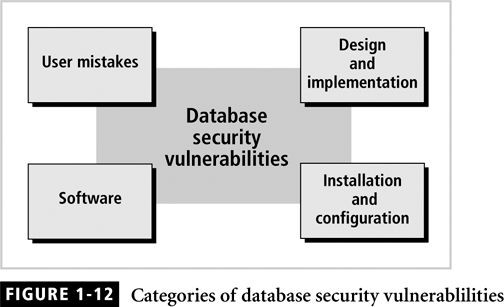




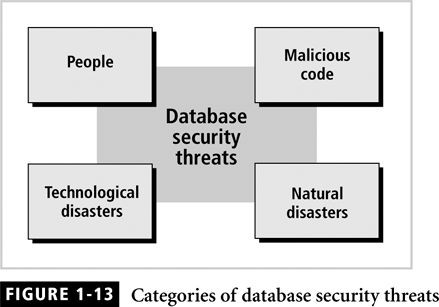
* Relational database: collection of related data files
* Data file: collection of related tables
* Table: collection of related rows (records)
* Row: collection of related columns (fields)



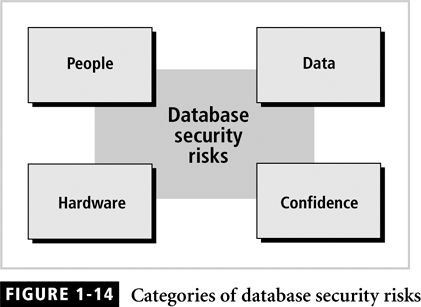
* Security vulnerability: a weakness in any information system component

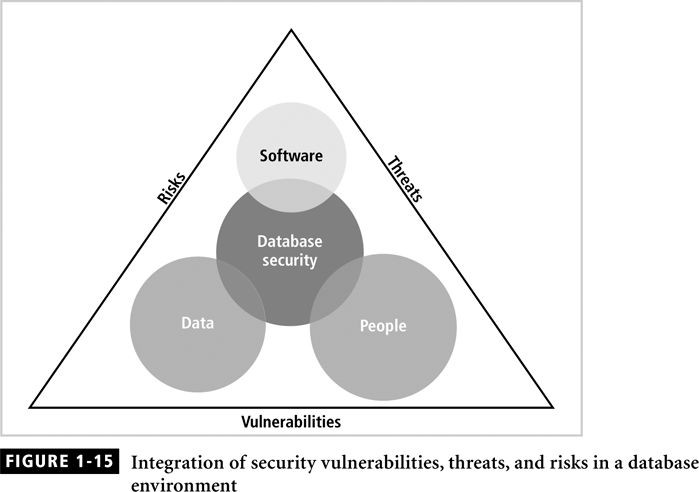


* Security threat: a security violation or attack that can happen any time because of a security vulnerability

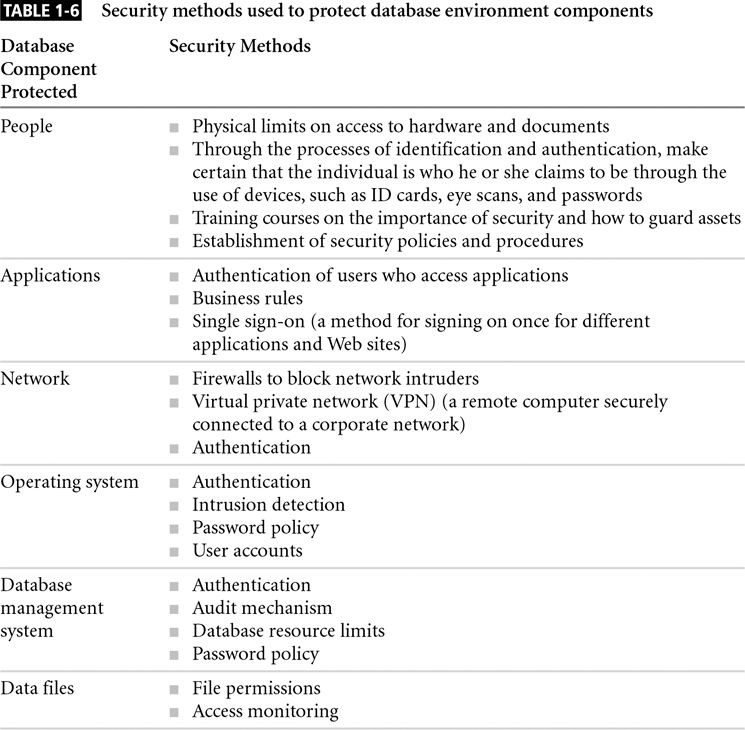


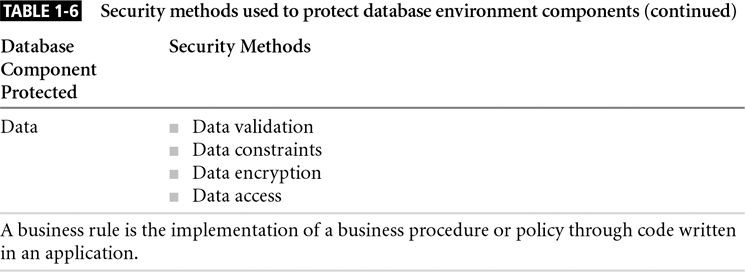
* Security risk: a known security gap intentionally left open

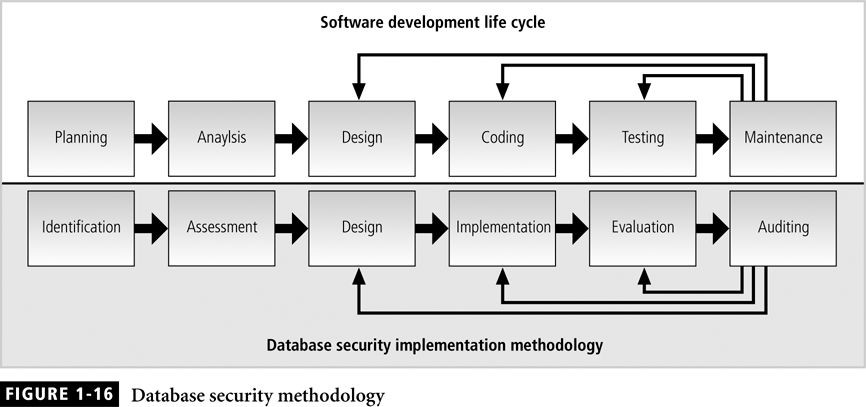




* Security measures are based on the value of each asset
* Types of assets include:
  + Physical
  + Logical
  + Intangible
  + Human







* 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
* 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