Security

- Database security:
  - degree to which data is fully protected from tampering or unauthorized acts
  - Full understanding requires viewing it within information systems/information security environment

Information Systems

- Success of companies
  - By wise decisions of management
    - Accurate and timely information
    - Information integrity
- Information system:
  - comprised of components working together to produce and generate accurate information
  - Categorized based on usage

Information Systems (continued)

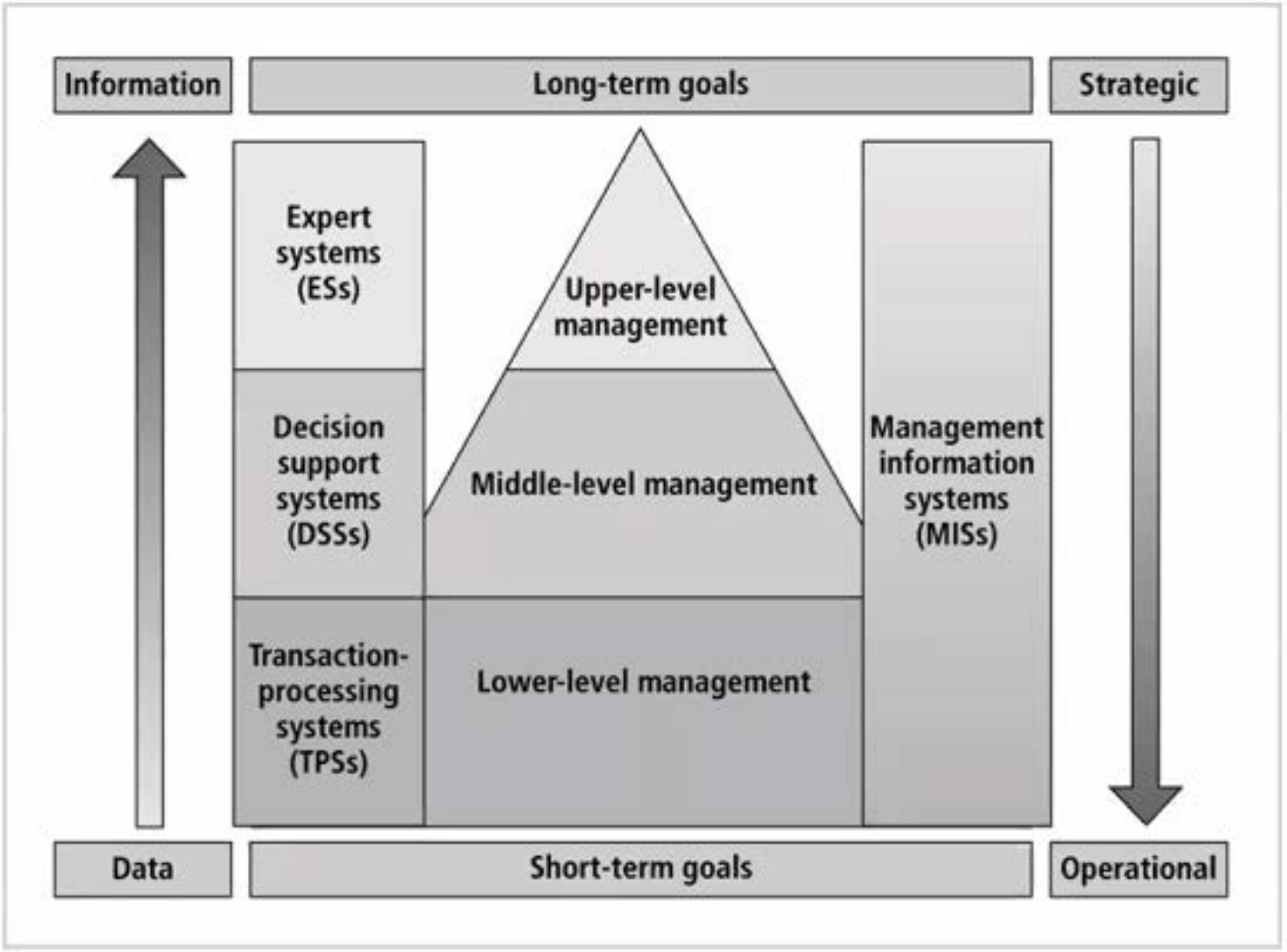

FIGURE 1-1 Typical use of system applications at various management levels

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 Components

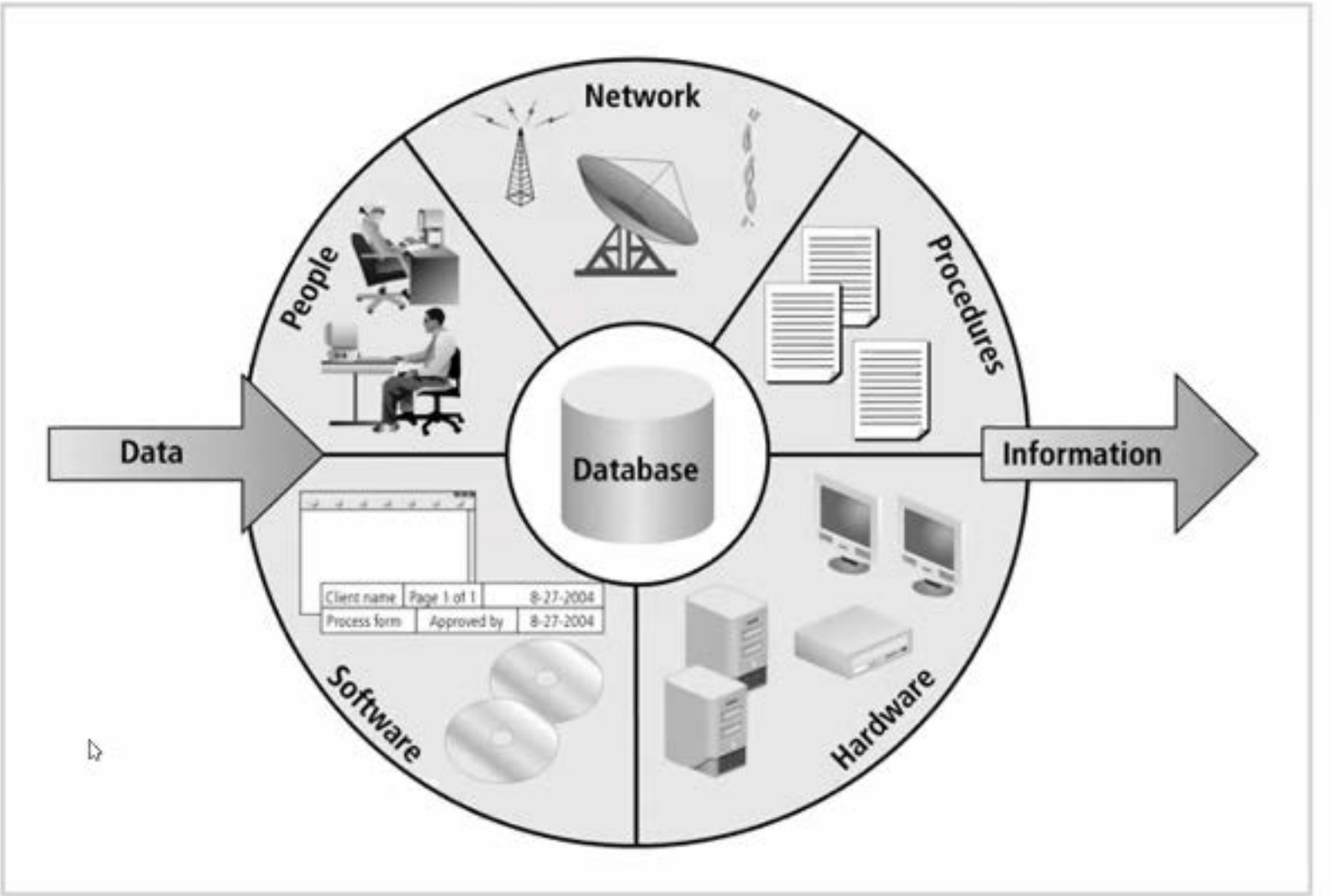

FIGURE 1-2 Information system components

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)

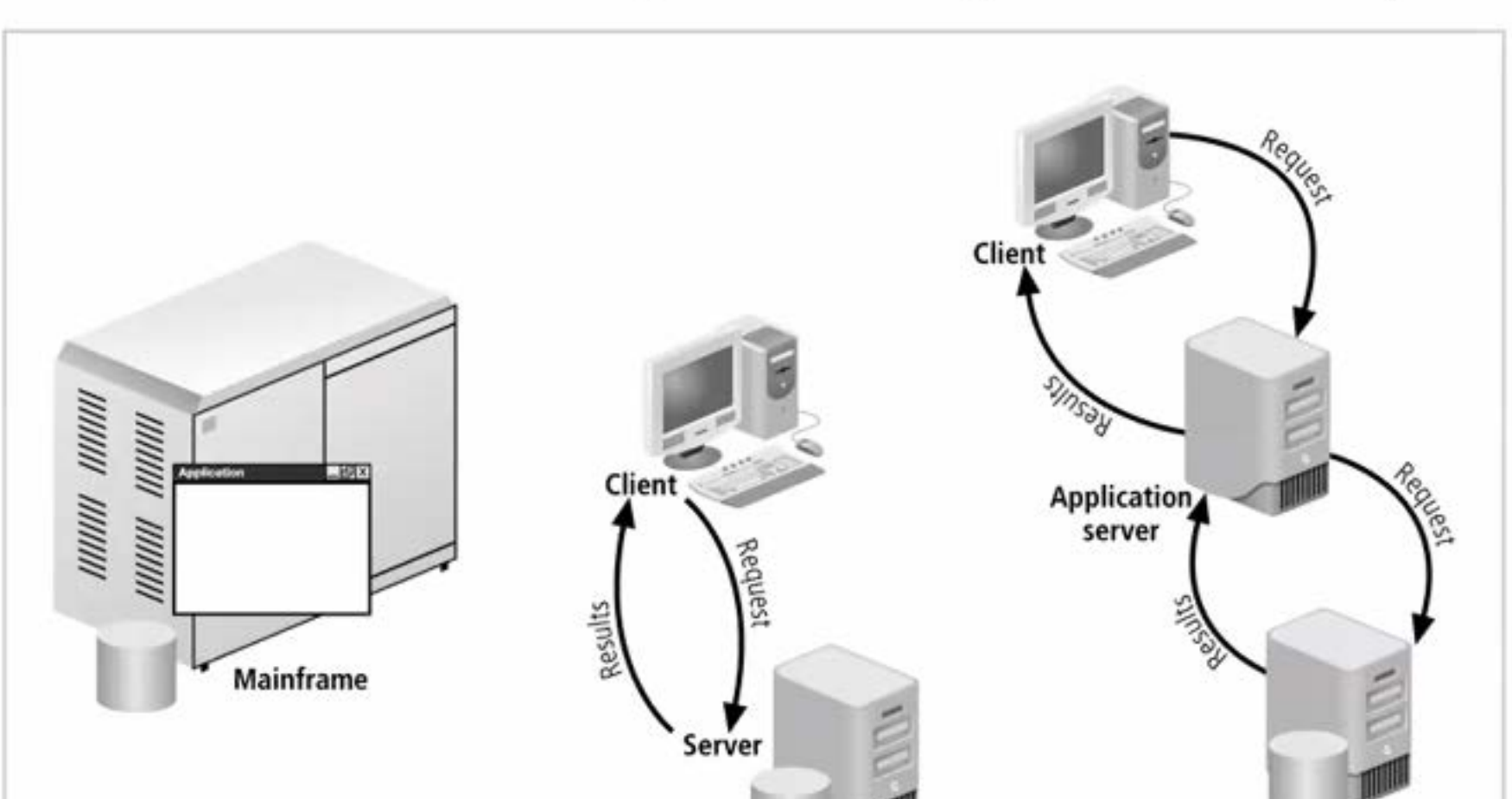

FIGURE 1-3 Examples of different client/server tier design

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)

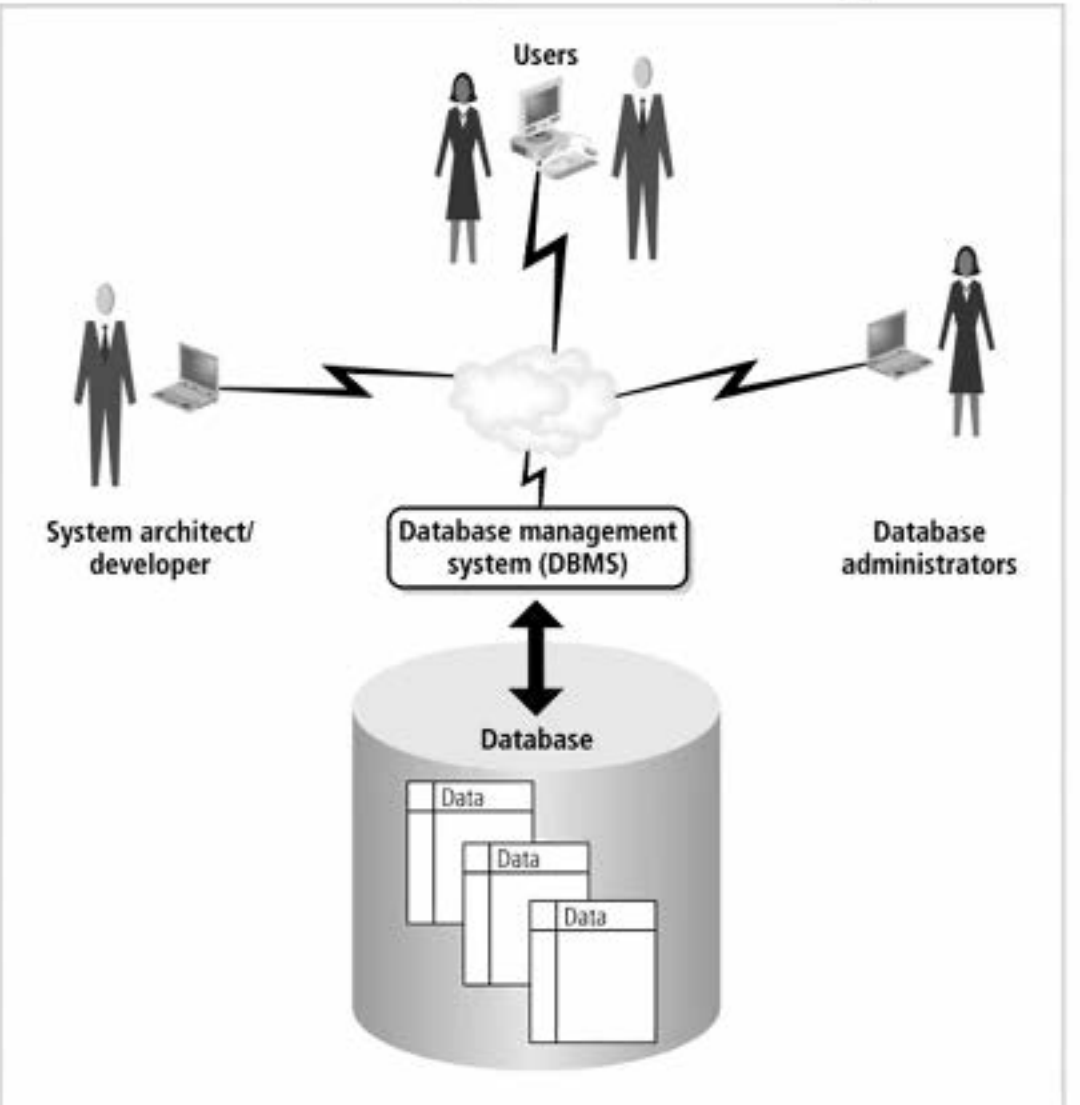

FIGURE 1-4 Database and DBMS environment

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
  - Based on C.I.A. triangle:
    - confidentiality, integrity, availability
- Cannot achieve 100% security while leaving systems operational
- Security policies must be balanced according to the C.I.A. triangle

SQL Injection Attacks

- Many web servers have backing databases
  - Much of their information stored in database
- Web pages are built (in part) based on queries to database
  - Possibly using some client input . . .

SQL Injection Mechanics

- Server plans to build a SQL query
- Needs some data from client to build it
  - E.g., client's user name
- Server asks client for data
- Client, instead, provides a SQL fragment
- Server inserts it into planned query
  - Leading to a "somewhat different" query

An Example

```
"select * from mysql.user
   where username = ' " . $uid . " ' and
   password=password(' ". $pwd " ');"
```

- Intent is that user fills in his ID and password
- What if he fills in something else?

  ```
  'or 1=1; -- '
  ```

What Happens Then?

- $uid has the string substituted, yielding

```
"select * from mysql.user
   where username = ' ' or 1=1; -- ' ' and
   password=password(' ". $pwd " ');"
```

- This evaluates to true
  - Since 1 does indeed equal 1
  - And -- comments out rest of line
- If script uses truth of statement to determine valid login, attacker has logged in

Basis of SQL Injection Problem

- Unvalidated input
- Server expected plain data
- Got back SQL commands
- Didn't recognize the difference and went ahead
- Resulting in arbitrary SQL query being sent to its database
  - With its privileges

Solution Approaches

- Carefully examine all input
  - To filter out injected SQL
- Use database access controls
  - Of limited value
- Randomization of SQL keywords
  - Making injected SQL meaningless

Information Security (continued)

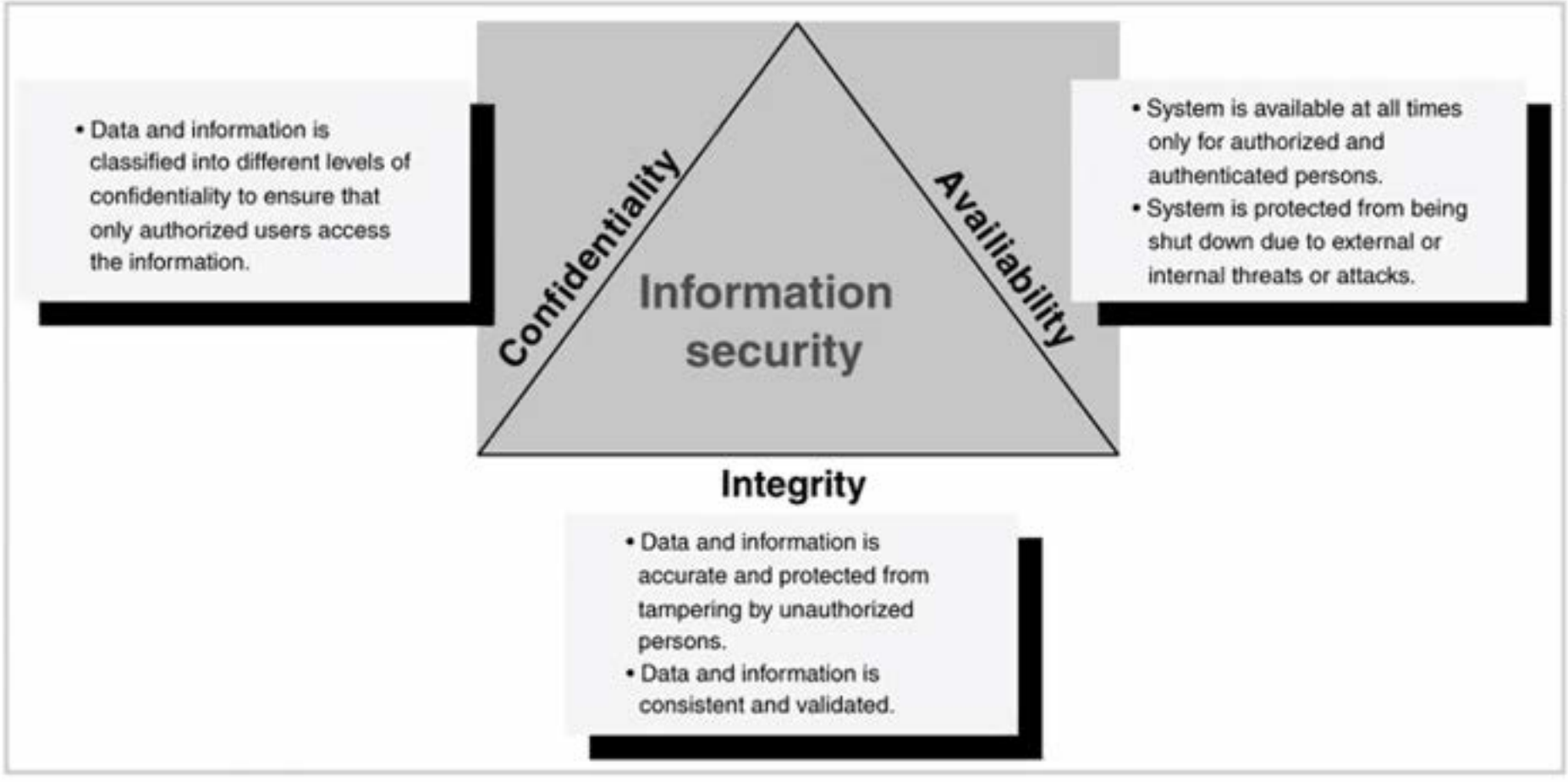

FIGURE 1-5 Information security C.I.A triangle

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)

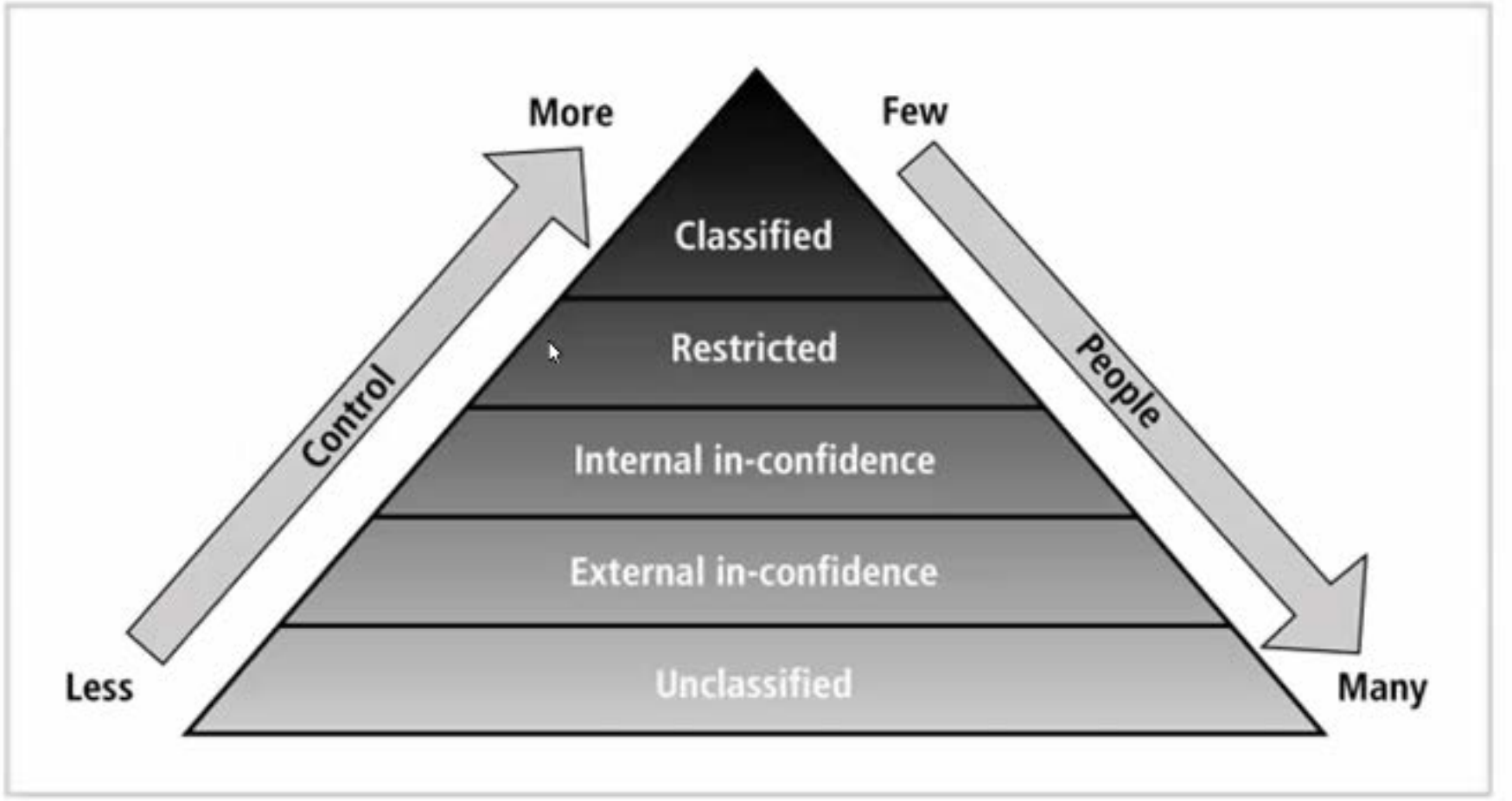

FIGURE 1-6 Confidentiality classification