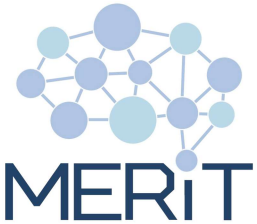
Co-funded by
the European Union

MERIT

Database Security

UNIT 1 . Introduction to Database Security

Database Security

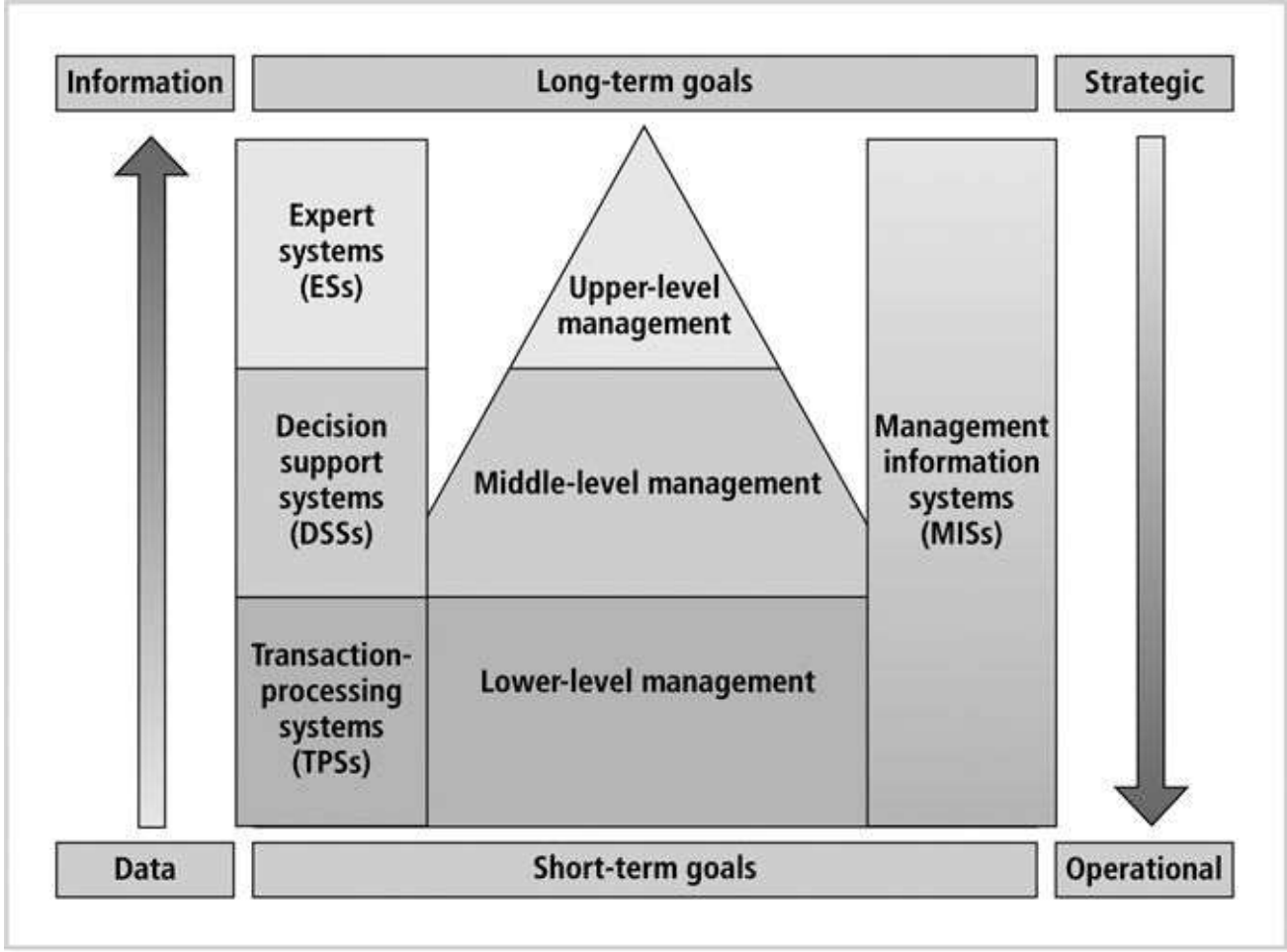


- Database security: degree to which data is fully protected from tampering or unauthorized acts
- Comprises information system and information security concepts

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

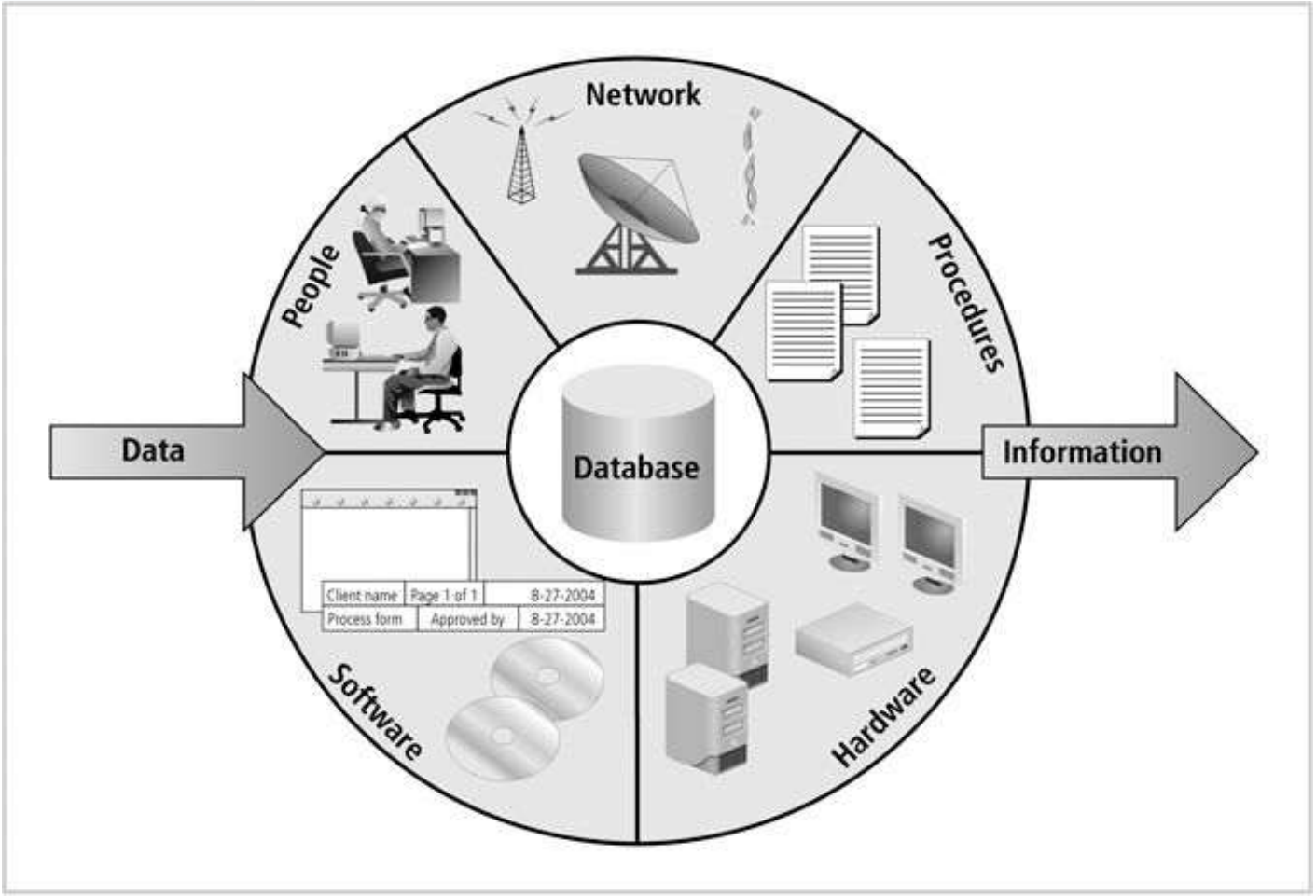
Information Systems (continued)



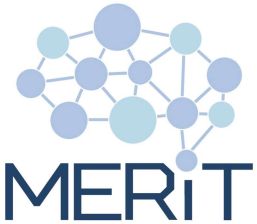
Information Systems (continued)

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

Information Systems (continued)

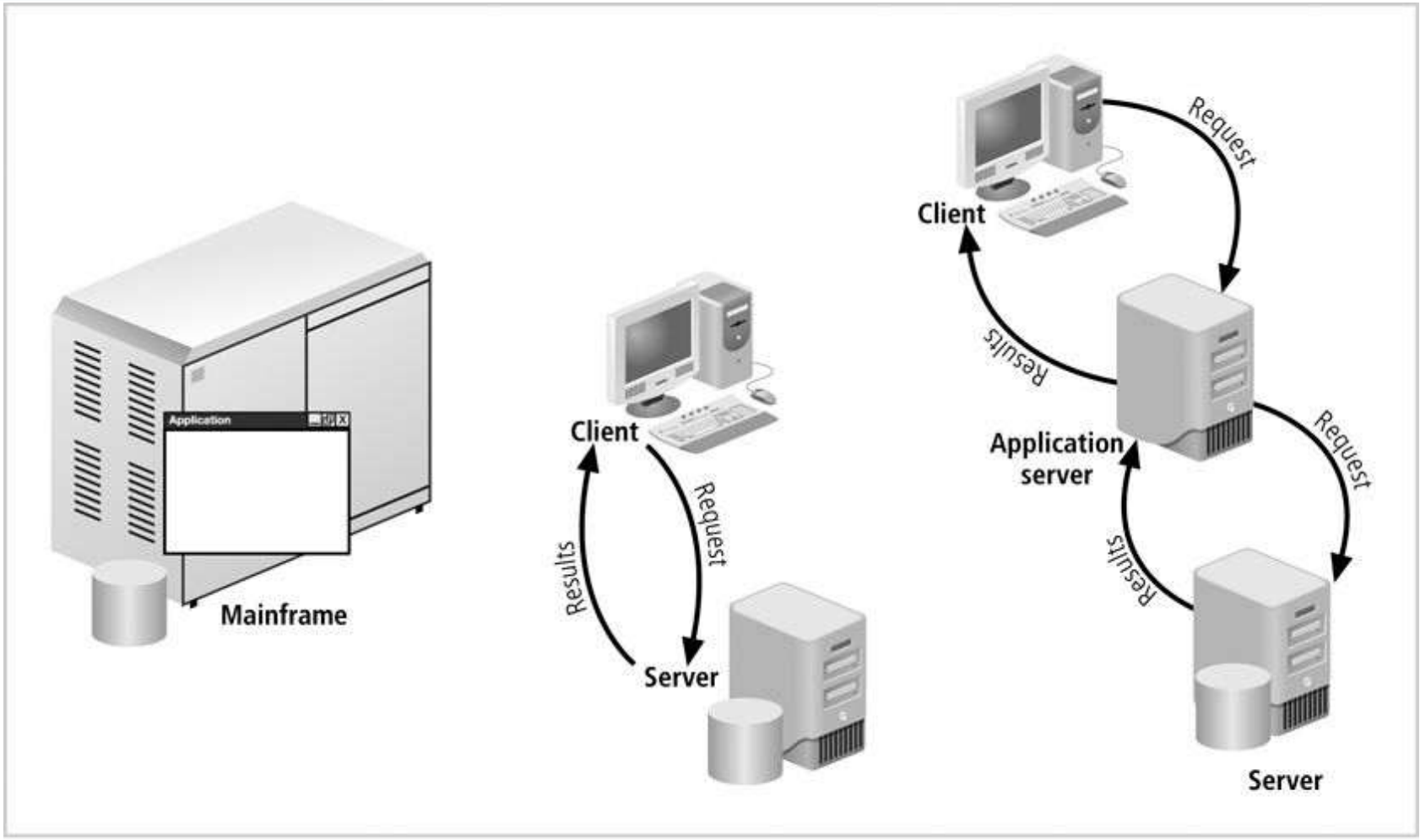


Information Systems (continued)

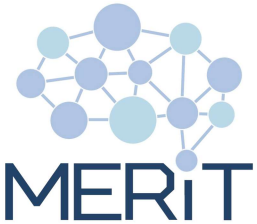


- Client/server architecture:
  - ✔ Based on the business model
  - ✔ Can be implemented as one-tier; two-tier; n-tier
  - ✔ Composed of three layers
- Tier: physical or logical platform
- Database management system (DBMS): collection of programs that manage database

Information Systems (continued)



Database Management

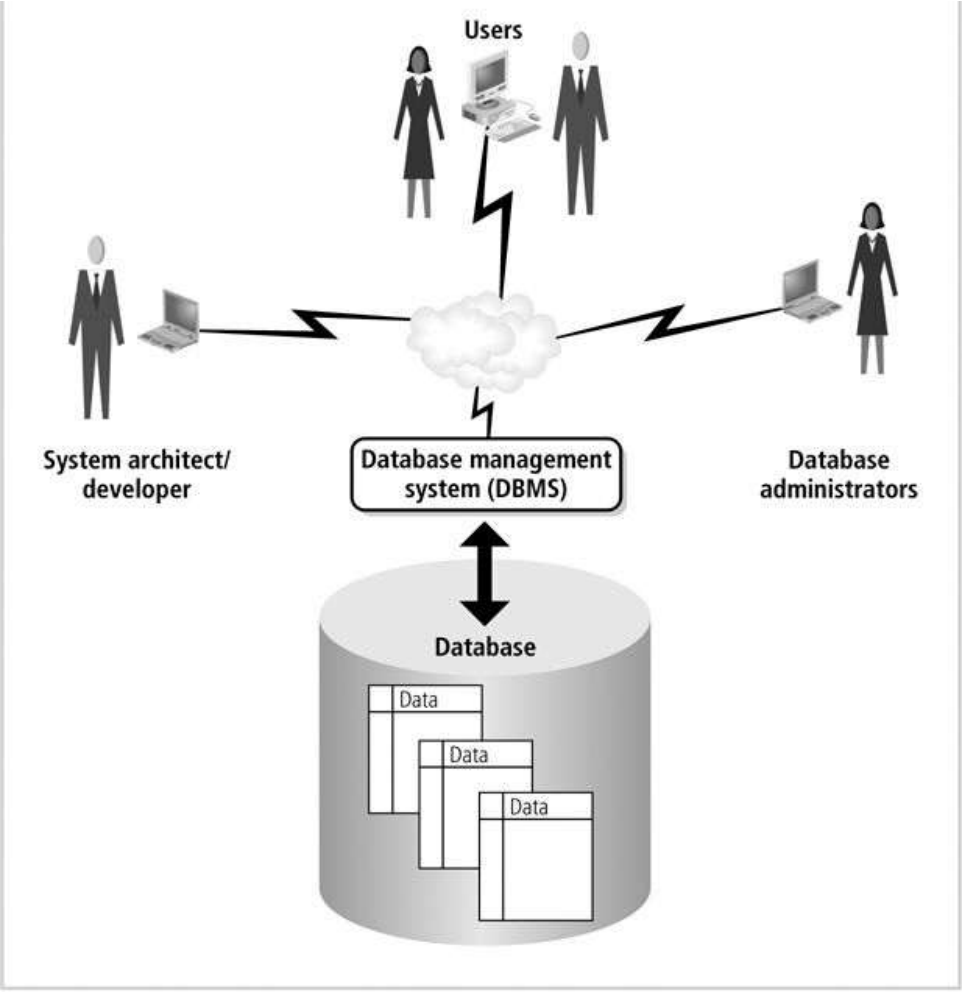


- Essential to success of information system
- DBMS functionalities:
  - ✔ Organize data
  - ✔ Store and retrieve data efficiently
  - ✔ Manipulate data (update and delete)
  - ✔ Enforce referential integrity and consistency
  - ✔ Enforce and implement data security policies and procedures
  - ✔ Back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

Database Management (continued)

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

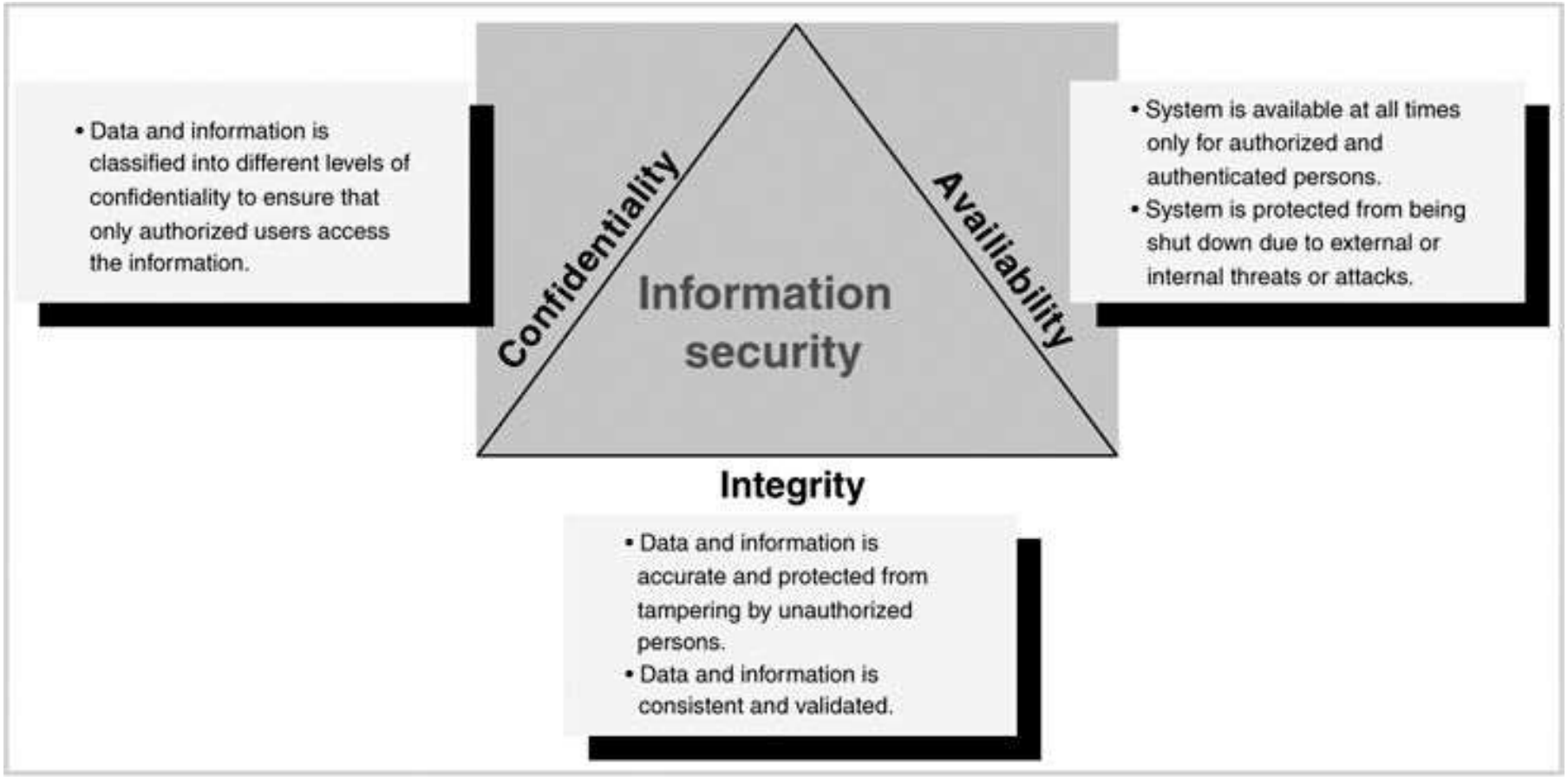
Database Management (continued)



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

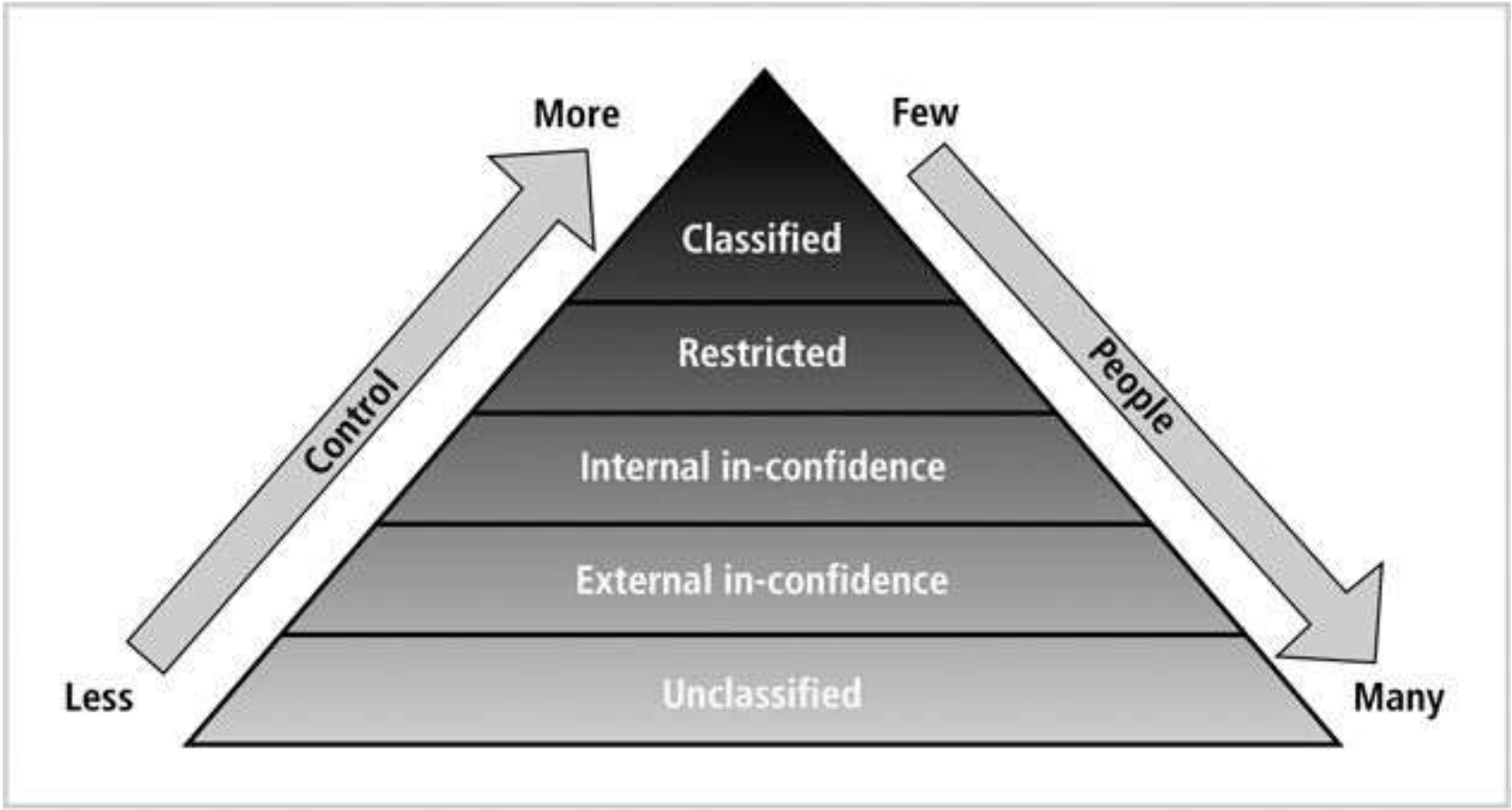
Information Security (continued)



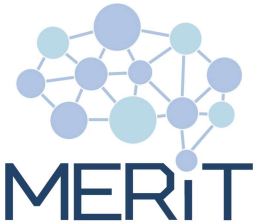
Confidentiality

- 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)



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

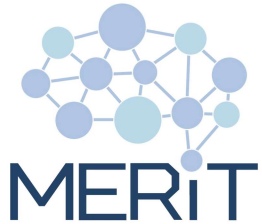
Integrity (continued)

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.)
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)

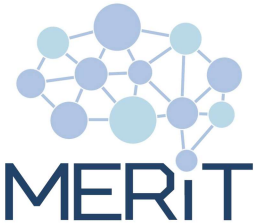
Type of Data Degradation	Description	Reasons for Data Losing Integrity
Data read inconsistency	Indicates that a user does not always read the last committed data, and data changes that are made by the user are visible to others before changes are committed.	▪ DBMS does not support or has weak implementation 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)

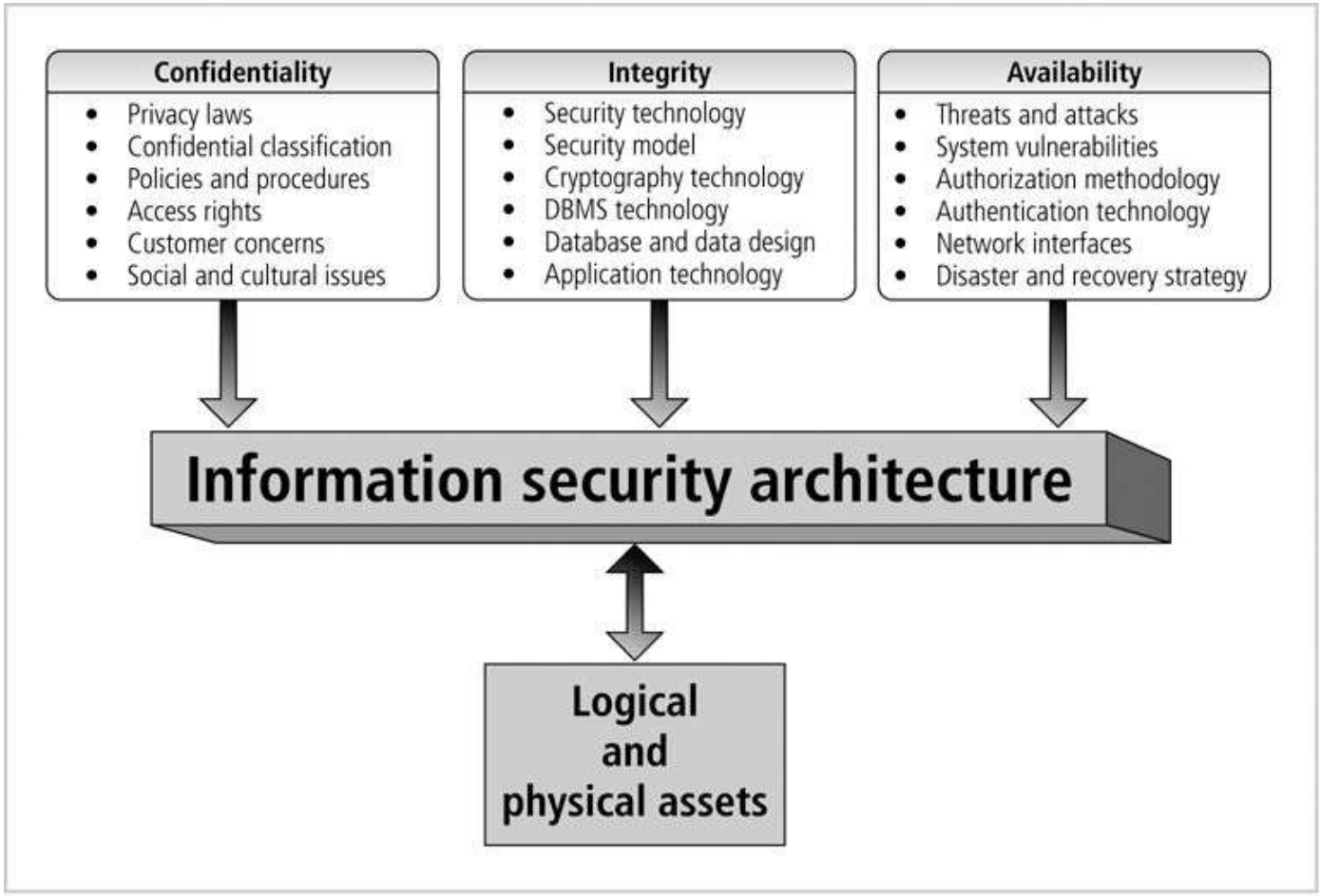


- Reasons for a system to become unavailable:
  - ✔ External attacks and lack of system protection
  - ✔ System failure with no disaster recovery strategy
  - ✔ Overly stringent and obscure security policies
  - ✔ Bad implementation of authentication processes

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

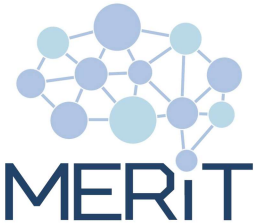
Information Security Architecture (continued)



Information Security Architecture (continued)

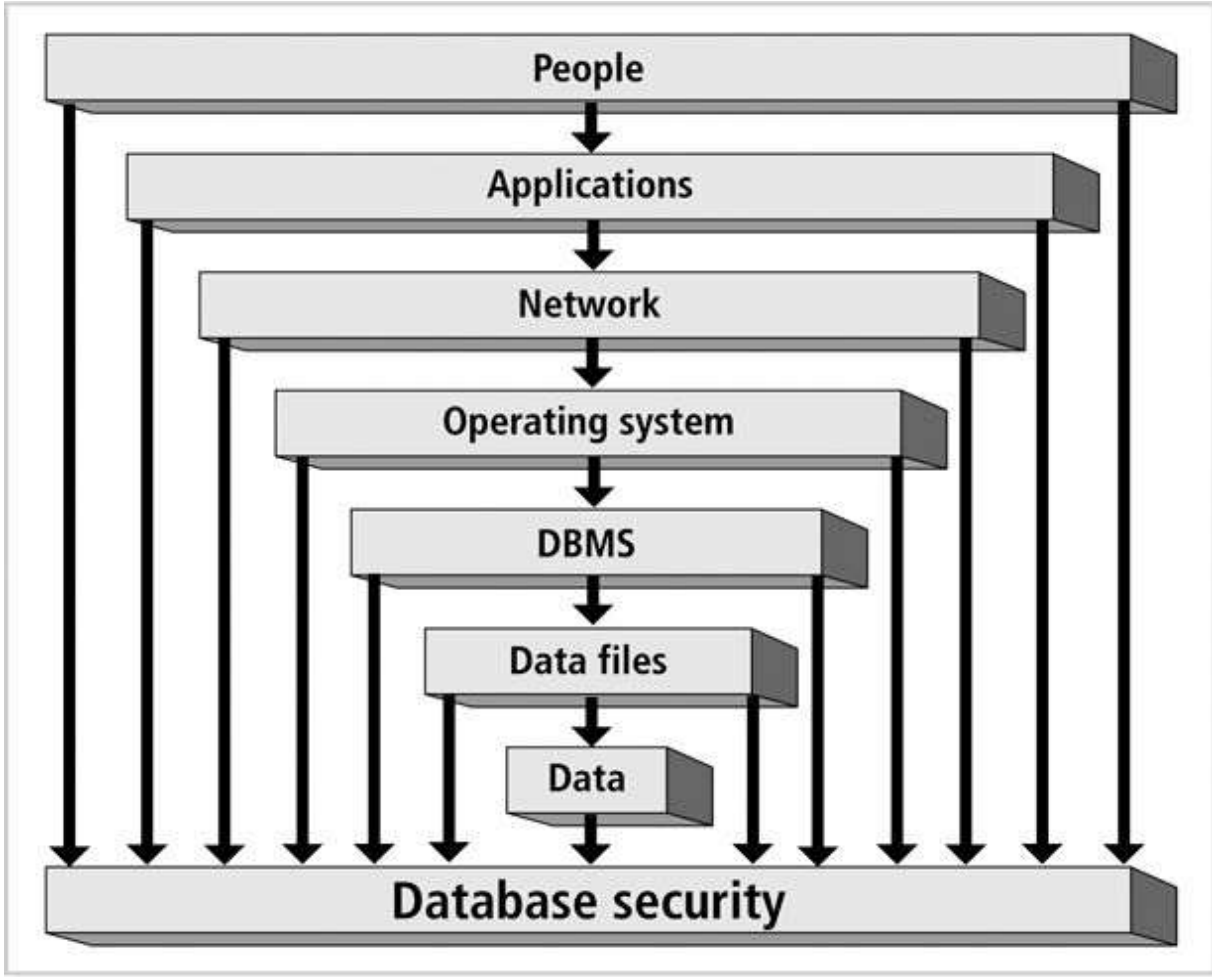
- Components include:
  - ✔ Policies and procedures
  - ✔ Security personnel and administrators
  - ✔ Detection equipments
  - ✔ Security programs
  - ✔ Monitoring equipment
  - ✔ Monitoring applications
  - ✔ Auditing procedures and tools

Database Security

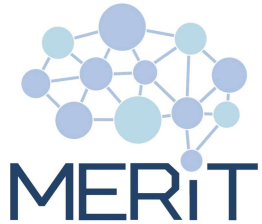


- Enforce security at all database levels
- Security access point: place where database security must be protected and applied
- Data requires highest level of protection; data access point must be small

Database Security (continued)

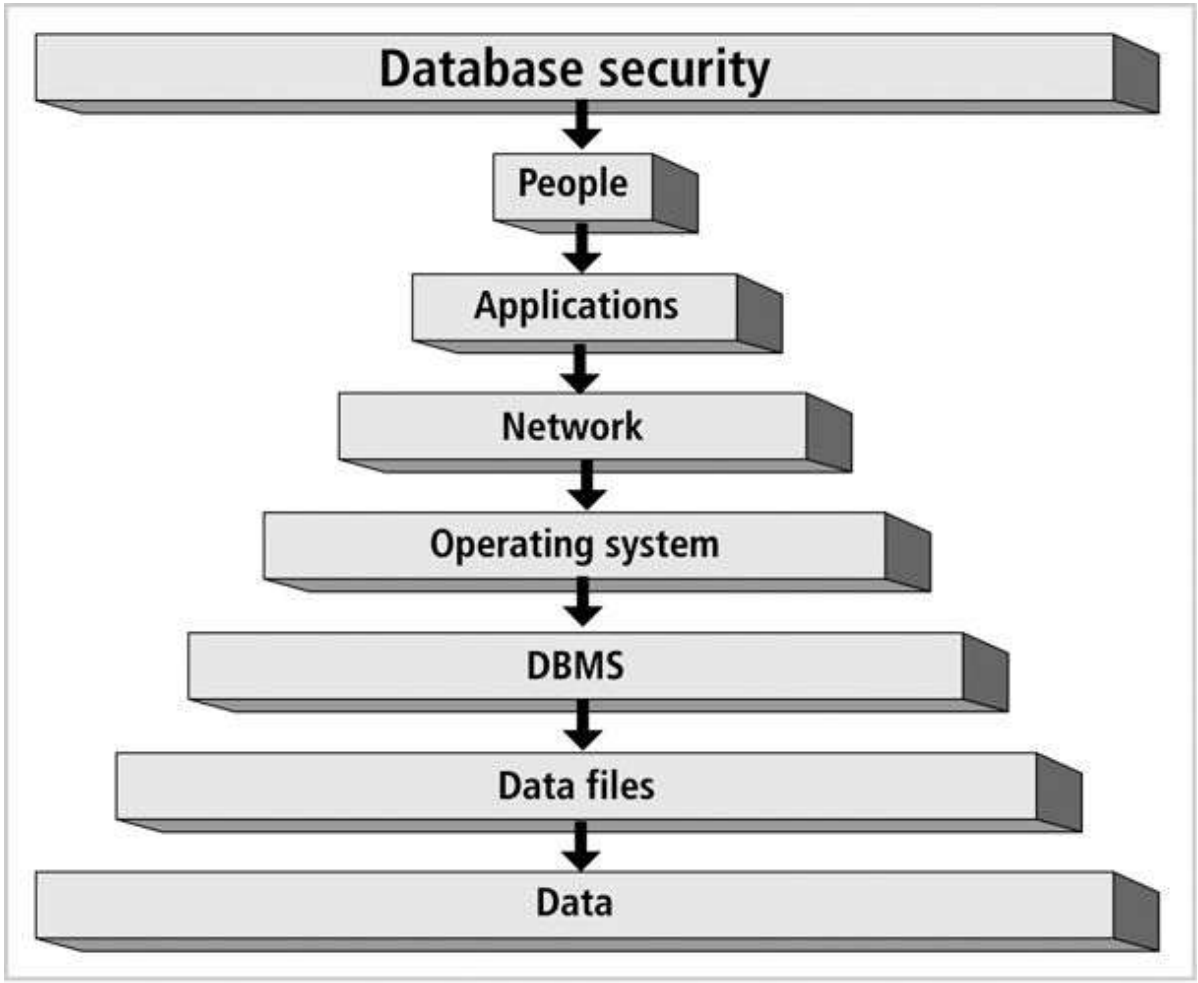


Database Security (continued)



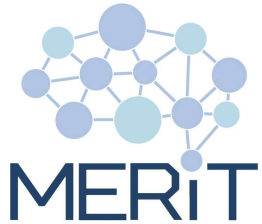
- Reducing access point size reduces security risks
- Security gaps: points at which security is missing
- Vulnerabilities: kinks in the system that can become threats
- Threat: security risk that can become a system breach

Database Security (continued)



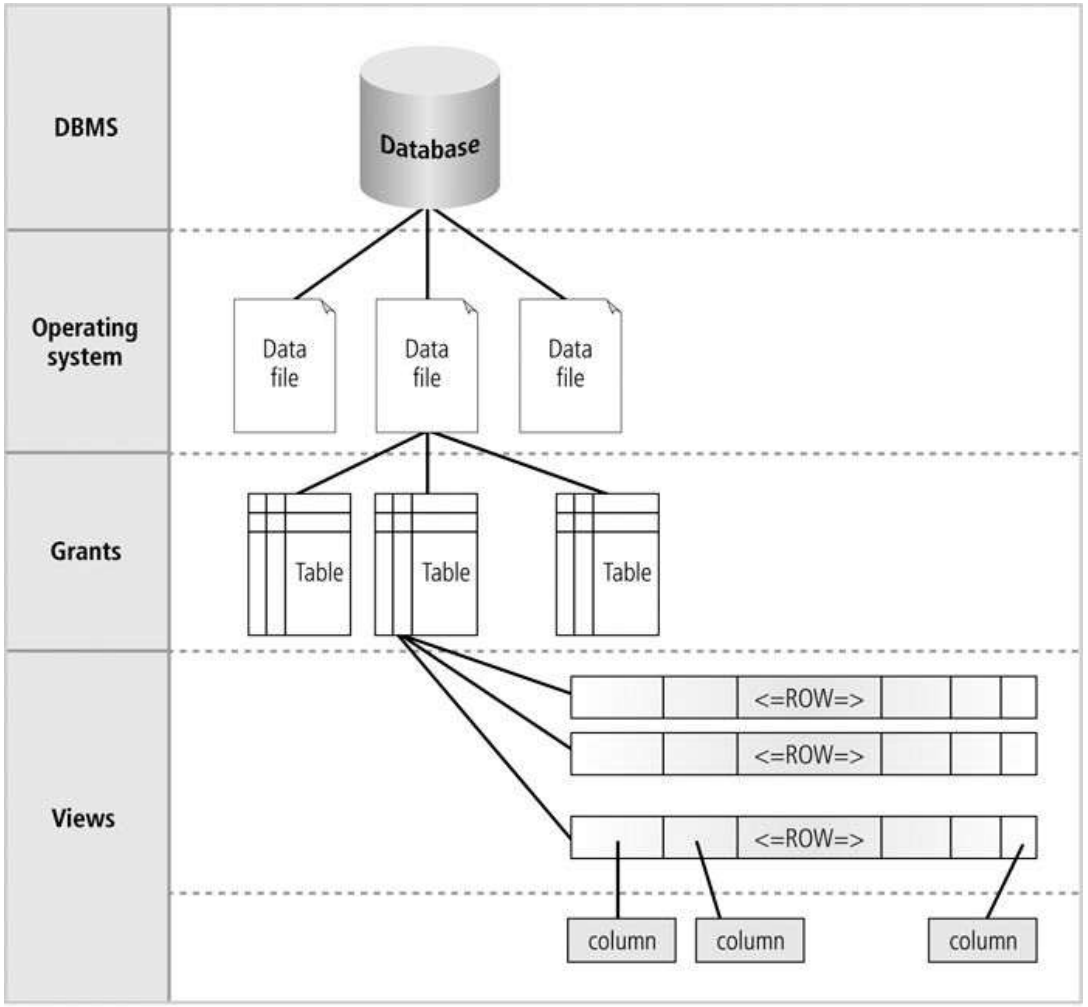
Database Security (continued)

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)

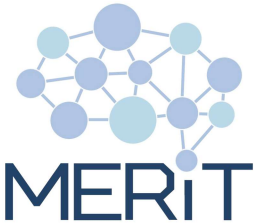
Database Security Levels (continued)



Threats to Database Security

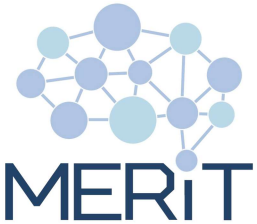
1. Granted excessive privileges and permissions, and privilege and permission abuse on database
2. Unauthorized privilege exploitation by hackers
3. SQL injection by hackers
4. Weak audit
5. Weak authentication
6. Database rootkits
7. Exposure of backup data

Database Security Protection



- ☐ Impose database security **policies** and regulations.
- ☐ Database security **practices.**
  - ✔ Access control.
  - ✔ Auditing.
  - ✔ Authentication.
  - ✔ Encryption.
  - ✔ Integrity controls.
- ☐ Application design security.
- ☐ Replication/synchronization and backups.
- ☐ Intrusion detection for Database rootkits, malicious code injection.

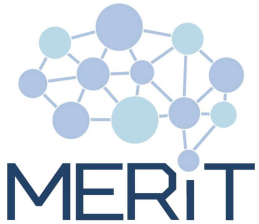
Security Regulations in Database Security: GDPR, HIPAA, ISO/IEC 27001



GDPR and Database Security

- **Scope:** Applies to databases storing personal data of EU residents
- **Key Requirements:**
  - Encrypt or pseudonymize personal data in databases
  - Implement access controls and audit logs
  - Minimize data collected and retained
- **For Databases:**
  - Ensure data subject rights (e.g., deletion, rectification) are enforceable via DB management tools
  - Design databases with privacy by design and by default
- **Impact of Non-compliance:** Fines up to €20M or 4% of global annual revenue

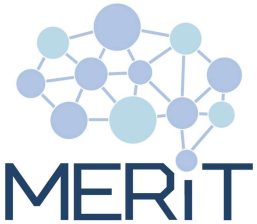
Security Regulations in Database Security: GDPR, HIPAA, ISO/IEC 27001



HIPAA and Database Security

- **Scope:** U.S. healthcare databases storing *Protected Health Information (PHI)*
- **Key Database Measures:**
  - Encryption at rest and in transit
  - Role-based access control (RBAC) to PHI fields
  - Activity monitoring and audit logging
- **Required Safeguards:**
  - **Administrative:** Policies for DB user access and incident response
  - **Physical:** Secure DB server environments
  - **Technical:** Access control, integrity checks, and backup encryption
- **Compliance Risk:** Fines up to $1.5M/year per violation

Security Regulations in Database Security: GDPR, HIPAA, ISO/IEC 27001



ISO/IEC 27001 and Database Security

- **Focus:** Securing information assets, including databases
- **Key ISMS Controls (Annex A relevant to DBs):**
  - A.8.2: Information classification
  - A.9.1: User access management
  - A.12.4: Logging and monitoring database activity
  - A.10.1: Cryptographic controls
- **Implementation in DB Systems:**
  - Periodic risk assessments on database threats
  - Backup, restore, and disaster recovery planning
  - Secure database configurations and updates
- **Benefit:** Demonstrates global best practices and improves trust

Review questions:

- What is Database security?
- What are the common security threats to database systems?
- How to protect database?