COLLEGE OF
COMPUTER STUDIES

QUEZON CITY
UNIVERSITY

WEEK 11-12
DATABASE ADMINISTRATION

IM101 - ADVANCED DATABASE SYSTEM

v2020

LEARNING OUTCOMES:

At the end of the session, the students should be able to:

1. Understand the roles of Data and Database Administration
2. Discuss the Database Environments' human architecture
3. Identify the different types of Data and Database Security

Ineffective Data Administration

1. Multiple data definitions
2. Missing data elements
3. Inappropriate data sources and timing
4. Inadequate familiarity
5. Poor response time and excessive downtime
6. Damage, sabotage, and stolen data
7. Unauthorized access

Traditional Administration

- **Data Administration**
  - A high-level function that is responsible for the overall management of data resources in an organization, including maintaining corporate wide data definitions and standards
- **Database Administration**
  - a technical role responsible for logical and physical database design and addressing technical problems, such as
    - Security compliance
    - Performance of database
    - Backup and recovery
    - Availability of database

Traditional Administration

- **Characteristics of Data Administration**
  - Policies, Procedures and Standards
    - Data Policies
    - Data Procedures
    - Data Standards
  - Planning
  - Data Conflict (ownership) Resolution
  - Managing the Information Repository
  - Internal Marketing

Traditional Administration

- **Traditional Database Administration**
  - **Database Management technical role**
    - Security compliance
    - Performance of databases
    - Backup and recovery
    - Availability of database
  - **Database Administration implements administrator standards and procedure including**
    - Implementation of programming specifications
    - Applications requirements
    - Policies
    - procedures

Traditional Administration

- **Core Roles of Database Administration**
  - Analyzing and designing database
  - Selecting DBMS and software tools
  - Installing/upgrading DBMS
  - Tuning database performance
  - Improving query processing performance
  - Managing data security, privacy, and integrity
  - Data backup and recovery

Traditional Administration

- **Trends in Database Administration**
  - Increased used of procedural logic
    - Features such as triggers, stored processes, and persistent stored modules
  - Proliferation of e-Business Applicants
    - Major priorities are High data availability, convergence of legacy data, analysis of user behavior and internet performance engineering
  - Increase Use of Smartphones
    - Most DBMS vendors offer small-footprint versions of their products, typically in support of specific applications

Life Cycle Phase

1. Planning
2. Analysis
3. Design
4. Implementation
5. Maintenance

Life Cycle Phase

Planning

This involves identifying the need for a new database, defining its purpose, and establishing the scope of the project.

Life Cycle Phase

Analysis

During this stage, the requirements of the database are gathered from stakeholders, and the existing system is analyzed to identify its strengths and weaknesses.

Life Cycle Phase

Design

In this stage, the structure and organization of the database are designed based on the requirements gathered during the analysis phase. This includes creating an **entity-relationship diagram**, defining **tables** and their **relationships**, and establishing data integrity constraints.

Life Cycle Phase

Implementation

This stage involves the actual creation of the database based on the design specifications. It includes **creating tables**, setting up **relationships**, and implementing data **validation rules**.

Life Cycle Phase

Maintenance

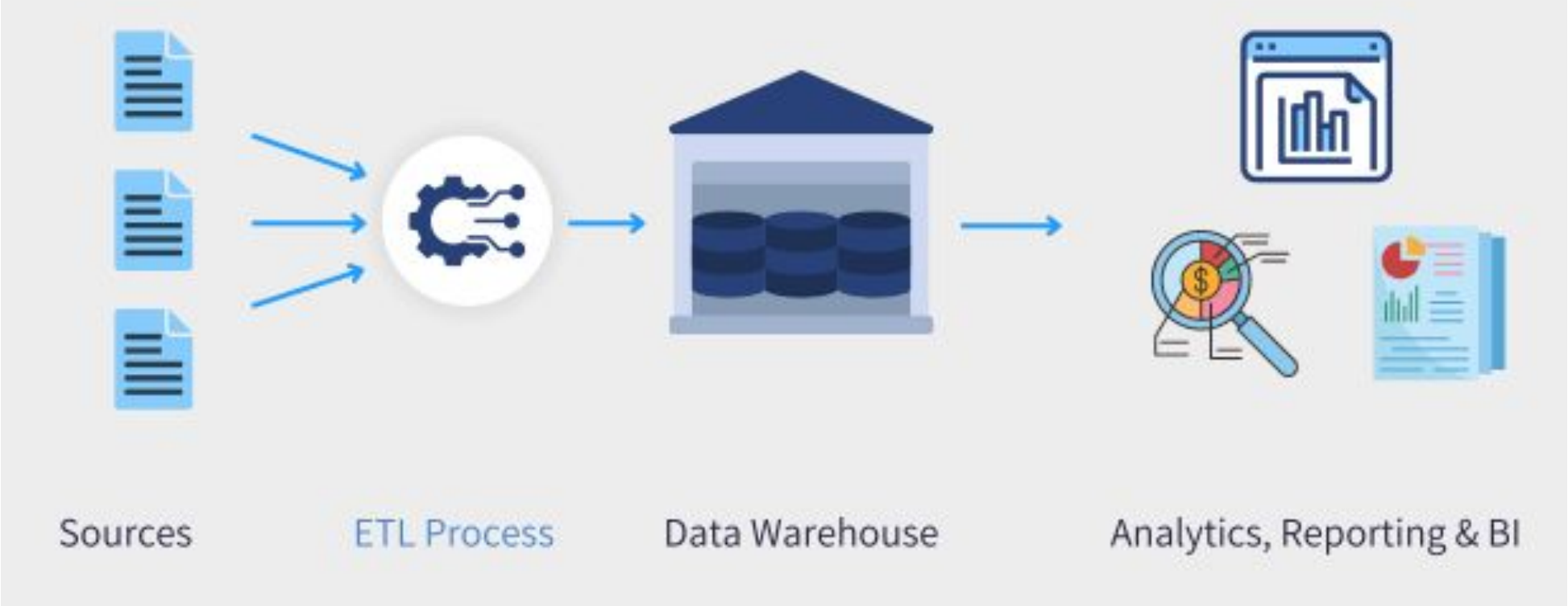
After deployment, the database requires ongoing maintenance to ensure its performance, security, and integrity.

Additionally, as the needs of the organization change, the database may need to evolve to accommodate new requirements.

Traditional Administration

- **Data Warehouse Administration**
  - New role, coming with growth in data warehouse
  - Similar to DA/DBA roles
  - Emphasis on integration and coordination of metadata/data across many data sources
  - Specific roles:
    - Support decision support applications
    - Manage data warehouse growth
    - Establish service level agreements regarding data warehouse and data marts

Data Warehouse Diagram



Extract, transform, and load (**ETL**) is the process of combining data from multiple sources into a large, central repository called a data warehouse.

The Open Source Movement and Database Roles

- **Summary of Evolving Data Administration Roles**
  - Selecting technologies
  - Communicating with users about data needs
  - Making performance and capacity decisions
  - Budgeting and planning data warehouse requirements

The Open Source Movement and Database Roles

- An alternative to proprietary packages such as Oracle, Microsoft SQL Server, or Microsoft Access
- MySQL is an Example of an open-source DBMS
- Less expensive than proprietary packages
- Source code available, for modification
- Absence of complete documentation
- Ambiguous licensing concerns
- Not as feature-rich as proprietary DBMS
- Vendors may not have certification programs

Open Source DBMS

SQL Database

1. MySQL
2. MariaDB
3. Firebird - Mozilla Public License
4. MonetDB - Mozilla Public License

NoSQL

5. MongoDB

The Open Source Movement and Database Roles

- **Types of Considerations when Selecting DBMS**
  - Features/Functionality
    - Does the DBMS provide the capabilities you need?
  - Support
    - How broad is the use of DBMS?
    - Does the DBMS come with ancillary resources and documentation?
  - Ease of Use
    - It depends on the availability of tools
  - Stability
    - How much and how badly does the DBMS fail over time?

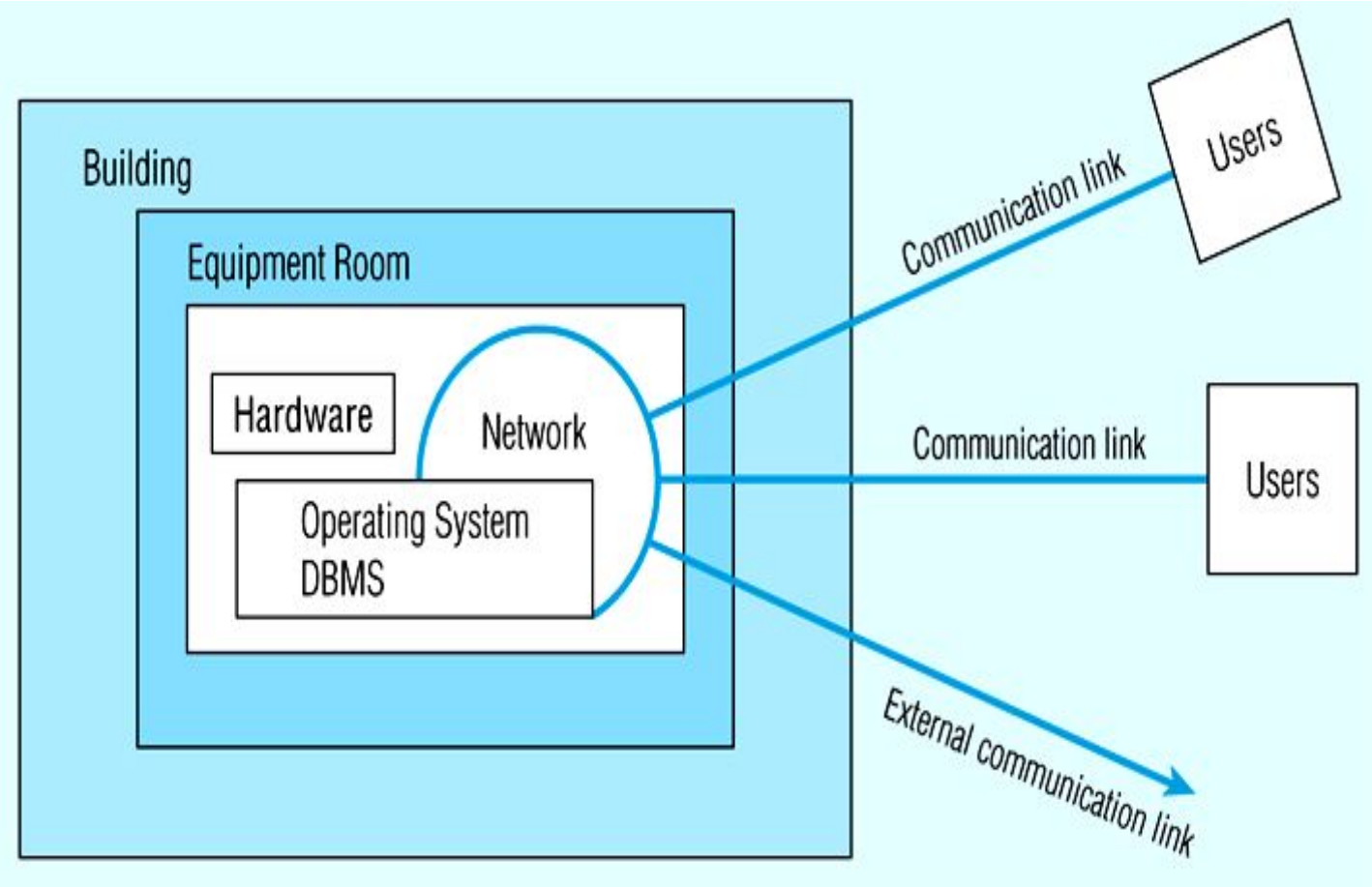
The Open Source Movement and Database Roles

- **Types of Considerations when Selecting DBMS**
  - Speed
    - Pace how fast is the response time to queries and transactions with proper database tuning?
  - Training
    - How simple is learning how to use the DBMS to developers and users?
  - Licensing
    - What are the terms and conditions of the open source license and commercial licenses

Information System Security

- **Three Security Goals**
  - Confidentiality
    - Ensuring that data is protected against unauthorized access,
  - Integrity
    - Refers with keeping data consistent and free of errors or anomalies
  - Availability
    - Refers to the accessibility of data whenever required by authorized users and for authorized purposes

Information System Security



Information System Security

- **Security Policy**
  - A collection of standards, policies, and procedures created to guarantee the security of a system and ensure auditing and compliance.
  - The security audit process starts by identifying security vulnerabilities in the organization's information system infrastructure and identifying measures to protect the system and data against those vulnerabilities.

Information System Security

- **Security Vulnerability**
  - A collection of standards, policies, and procedures created to guarantee the security of a system and ensure auditing and compliance.
  - The security audit process starts by identifying security vulnerabilities in the organization's information system infrastructure and identifying measures to protect the system and data against those vulnerabilities.

Information System Security

- **Security Vulnerability**
  - Technical
    - Example would be a flaw in the operating system or web browser
  - Managerial
    - Example an organization might not educate users about critical security issues
  - Cultural
    - Users might hide passwords under their keyboards or forget to shared confidential reports
  - Procedural
    - Company procedures might not require complex password or the checking of users IDs

Information System Security

- **Security Breach**
  - An event in which a security threat is exploited to endanger the integrity, confidentiality, or availability of the system
    - Preserved
      - Action is required to avoid the recurrence of similar security problems, but data recovery may not be necessary
    - Corrupted
      - Action is required to avoid the recurrence of similar security problems and the database must be recovered to a consistent state

Information System Security

- **Database Security**
  - Change default system password
  - Change default installation paths
  - Apply the latest patches
  - Secure installation folders with proper access rights
  - Make sure that only required services are running
  - Set up auditing logs
  - Set up session logging
  - Require session encryption

Managing Data Security

- **Threats of Data Security**
  - Accidental Losses, Including Human Error, Software, and Hardware-Caused Breaches
    - Steps that can be taken to resolve the danger of accidental loss
      1. User authorization
      2. Standard software installation procedures
      3. Hardware maintenance schedule

Managing Data Security

- **Threats of Data Security**
  - Theft and Fraud
    - Physical protection should also provide for
      - Employees
      - Offices
      - Other places
  - The creation of a firewall to prevent unauthorized access

Managing Data Security

- **Threats of Data Security Cont…**
  - Loss of Privacy or Confidentiality
    - Privacy Loss is usually taken to mean loss of protection of personal data
    - Confidentiality Loss is usually taken to mean loss of protection of critical organizational data
  - Loss of Data Integrity
    - Data is compromised, then data is null or corrupted
  - Loss of Availability
    - Threat category involves the introduction of viruses designed to corrupt data or software, or make the device unusable

Managing Data Security

- **Establishing Client/Server Security**
  - Physical security, logical security and change control security must be established across all client / server environment components, including servers, client workstations, network and associated components, and users.
    - Server Security
      - Database management systems, such as Oracle and SQL Server, offer significant functionality to database managers
    - Network Security
      - data encryption is obviously an essential aspect of network security such that attackers cannot read a data packet that is being transmitted

Database Software Data Security Features

- **The most important Data Management software protection features follow:**
  - Views or Subschemas
    - A view is generated by querying one or more of the base tables at the time of the request, generating a dynamic result table for the user.

```
CREATE VIEW MATERIALS_V AS
  SELECT Product_T.ProductID, ProductName, Footage,
       FootageOnHand
  FROM Product_T, RawMaterial_T, Uses_T
  WHERE Product_T.ProductID = Uses_T.ProductID
  AND RawMaterial_T.MaterialID = Uses_T.MaterialID;
```

Database Software Data Security Features

SELECT * FROM MATERIALS_V;

ProductID	ProductName	Footage	FootageOnHand
1	End Table	4	1
2	Coffee Table	6	11
3	Computer Desk	15	11
4	Entertainment Center	20	84
5	Writer's Desk	13	68
6	8-Drawer Desk	16	66
7	Dining Table	16	11
8	Computer Desk	15	9

8 rows selected.

Database Software Data Security Features

- **The most important Data Management software protection features follow:**
  - Views or Subschemas
    - A view is generated by querying one or more of the base tables at the time of the request, generating a dynamic result table for the user.
  - Integrity Controls/Domains
  - Authorization Rules
  - User-defined Procedures
  - Encryption
  - Authentication Schemes
    - Password
    - Strong Authentication
  - Backup

Database Software Data Security Features

```
CREATE DOMAIN PriceChange AS DECIMAL
  CHECK (VALUE BETWEEN .001 and .15);
```

```
PriceIncrease PriceChange NOT NULL,
```

```
CREATE ASSERTION TerritoryAssignment
  CHECK (NOT EXISTS
    (SELECT * FROM Salesperson_T SP WHERE SP.TerritoryID IN
      (SELECT SSP.TerritoryID FROM Salesperson_T SSP WHERE
        SSP.SalespersonID < > SP.SalespersonID)));
```

Subject	Object	Action	Constraint
Sales Dept.	Customer record	Insert	Credit limit LE $5000
Order trans.	Customer record	Read	None
Terminal 12	Customer record	Modify	Balance due only
Acctg. Dept.	Order record	Delete	None
Ann Walker	Order record	Insert	Order aml LT $2000
Program AR4	Order record	Modify	None

	Customer records	Order records
Read	Y	Y
Insert	Y	Y
Modify	Y	N
Delete	N	N

	Salespersons (password BATMAN)	Order entry (password JOKER)	Accounting (password TRACY)
Read	Y	Y	Y
Insert	N	Y	N
Modify	N	Y	Y
Delete	N	N	Y

Database Software Data Security Features

Privilege	Capability
SELECT	Query the object.
INSERT	Insert records into the table/view. Can be given for specific columns.
UPDATE	Update records in table/view. Can be given for specific columns.
DELETE	Delete records from table/view.
ALTER	Alter the table.
INDEX	Create indexes on the table.
REFERENCES	Create foreign keys that reference the table.
EXECUTE	Execute the procedure, package, or function.

Database Software Data Security Features

- **Application Security Issues in Three-Tier Client/Server Environment**
  - Companies can gather information about those that access their web sites
    - If they carry out e-commerce activities, selling products over the Web
    - If the company sells customer information without the knowledge of customers
    - If an organization wishes to make only static HTML pages available
    - If some of the HTML files loaded on the Web server are sensitive

Database Software Data Security Features

- **Additional methods of Web security includes ways to restrict access to Web servers**
  - Restrict the number of users on the Web server as much as possible
  - Restrict access to the Web server, keeping a minimum number of ports open.
  - Remove any unneeded programs that load automatically when setting up the server.

Database Software Data Security Features

- **Additional methods of Web security includes ways to restrict access to Web servers**
  - Privacy
    - Legislation on data privacy generally gives individuals the right to know what data was collected about them and to correct any errors in those data
    - Individuals must safeguard their rights to privacy and be aware of the privacy implications of the tools they use.
    - W3C created a standard the Privacy Preference Platform

Platform for Privacy Preferences Project

is an emerging industry standard that enables web sites to express their privacy practices in a standardized format that can be automatically retrieved and interpreted by user agents.

Database Software Data Security Features

- **Additional methods of Web security includes ways to restrict access to Web servers**
  - P3P addresses the following aspects of online privacy:
    - Who is collecting the data?
    - What information is being collected, and for what purpose?
    - What information will be shared with others, and who are those others?
    - Can users make changes in the way their data will be used by the collector?
    - How are disputes resolved?
    - What policies are followed for retaining data?
    - Where can the site's detailed policies be found, in readable form?

VAPT

- **Vulnerability Assessment & Penetration Testing**
- It is a security testing to identify security vulnerabilities in an application, network, endpoint, and cloud.
- Both the Vulnerability Assessment and Penetration Testing have unique strengths and are often collectively done to achieve complete analysis.

Reference:
https://www.inspirisys.com/vulnerability-assessment-penetration-testing#:~:text=VAPT%20stands%20for%20Vulnerability%20Assessment,done%20to%20achieve%20complete%20analysis.

Database Backup and Recovery

- **Basic Recovery Facilities**
  - Backup facilities
  - Journalizing facilities
  - Checkpoint facility
  - Recovery facility

Database Backup and Recovery

- **Recovery and Restart Procedures**
  - Disk Mirroring
  - Restore/Rerun
  - Maintaining Transaction Integrity
    - Atomic
    - Consistent
    - Isolated
    - Durable
  - Backward Recovery
  - Forward Recovery

Database Backup and Recovery

- **Types of Database Failure**
  - Aborted Transactions
  - Incorrect Data
  - System Failure
  - Database Destruction

Database Backup and Recovery

- **Disaster Recovery**
  - Components of Recovery Plan
    - Develop a comprehensive, documented strategy
    - Find a multidisciplinary team
    - Build an offsite location datacenter for backup
    - Submit backup copies of databases

Authorization Management

- **Authorization Management Procedures**
  - User access management
    - Define each user to the database
    - Assign password to each user
    - Define user group
    - Assign access privileges
    - Control physical access
  - View Definition
  - DBMS access control
  - DBMS usage monitoring

Thank you!