Chapter 16

Database Administration and Security

CENGAGE

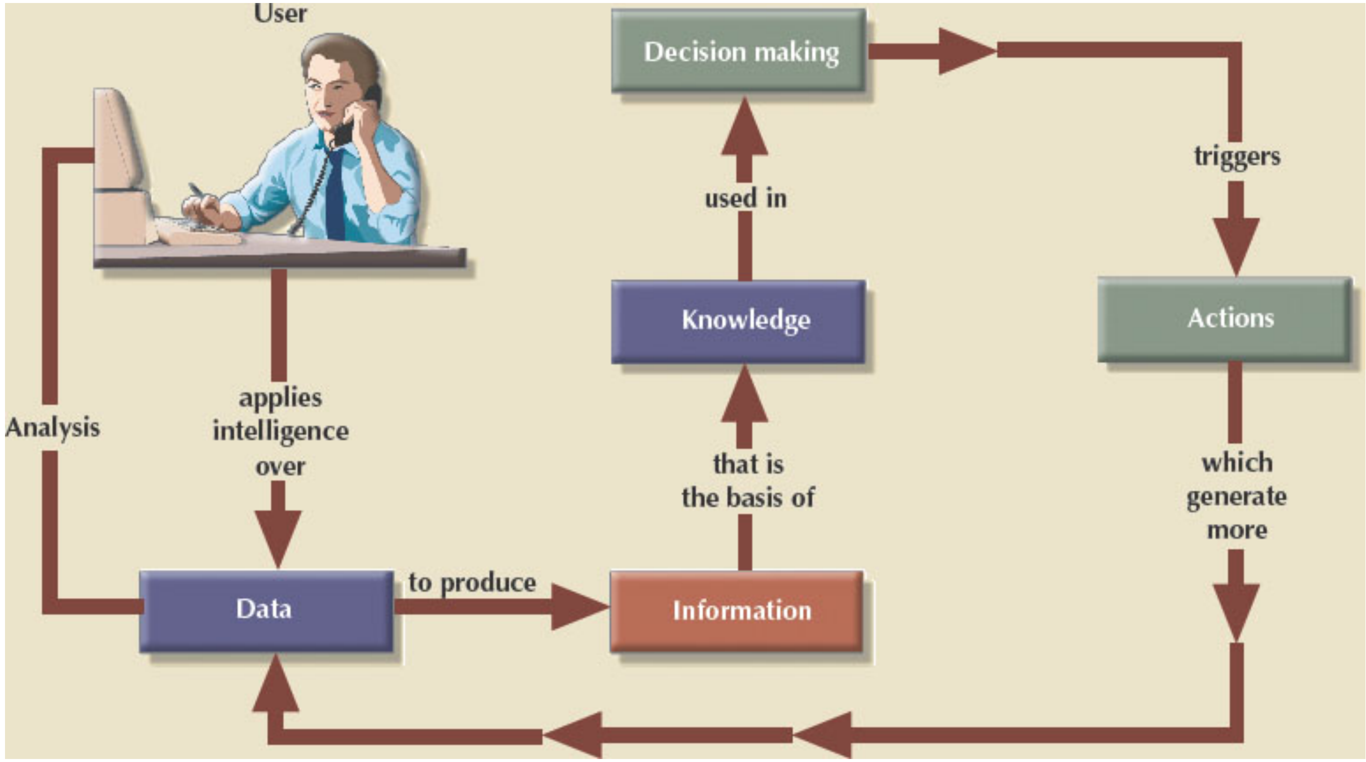
Learning Objectives (1 of 2)

- In this chapter, you will learn:
  - That data are a valuable business asset requiring careful management
  - How a database plays a critical role in an organization
  - That the introduction of a DBMS has important technological, managerial, and cultural consequences for an organization
  - About the database administrator’s managerial and technical roles

Learning Objectives (2 of 2)

- In this chapter, you will learn:
  - About data security, database security, and the information security framework
  - About several database administration tools and strategies
  - How cloud-based data services impact the DBA's role
  - How various technical tasks of database administration are performed with Oracle

Figure 16.1 - The Data-Information-Decision Making Cycle



Data

- Dirty data
  - Data that suffer from inaccuracies and inconsistencies
- Data quality
  - Ensuring accuracy, validity, and timeliness of data
- Data profiling software
  - Determine data patterns and compare them against standards defined by the organization
- Master data management (MDM) software
  - Helps prevent dirty data by coordinating across multiple systems

Need for and Role of a Database in an Organization (1 of 2)

- At the top management level
  - Enable strategic decision making and planning
  - Identify growth opportunities
  - Define and enforce organizational policies
  - Reduce costs and boost productivity
  - Provide feedback

Need for and Role of a Database in an Organization (2 of 2)

- At the middle management level
  - Deliver the data required for tactical planning
  - Monitor the use of resources
  - Evaluate performance
  - Enforce security and privacy of data in the database
- At the operational management level
  - Represent and support company operations
  - Produce query results within specified performance levels
  - Enhance the company’s short-term operations

Introduction of a Database: Special Considerations

- Technological aspect
  - Selecting, installing, configuring, and monitoring the DBMS to ensure that it operates efficiently
- Managerial aspect
  - Careful planning to create an appropriate organizational structure
- Cultural aspect
  - Listening to people's concerns about the system and explaining its uses and benefits

Evolution of the Database Administration Function

- Information systems (IS) department
  - Provides end users with data management support and solutions for information needs
- Database administrator
  - Responsible for control of the centralized and shared database
- Systems administrator
  - General coordinator of all DB As
- Data administrator (DA) or information resource manager (IRM)
  - Has a higher degree of responsibility and authority than the DBA

Figure 16.2 - The IS Department's Internal Organization

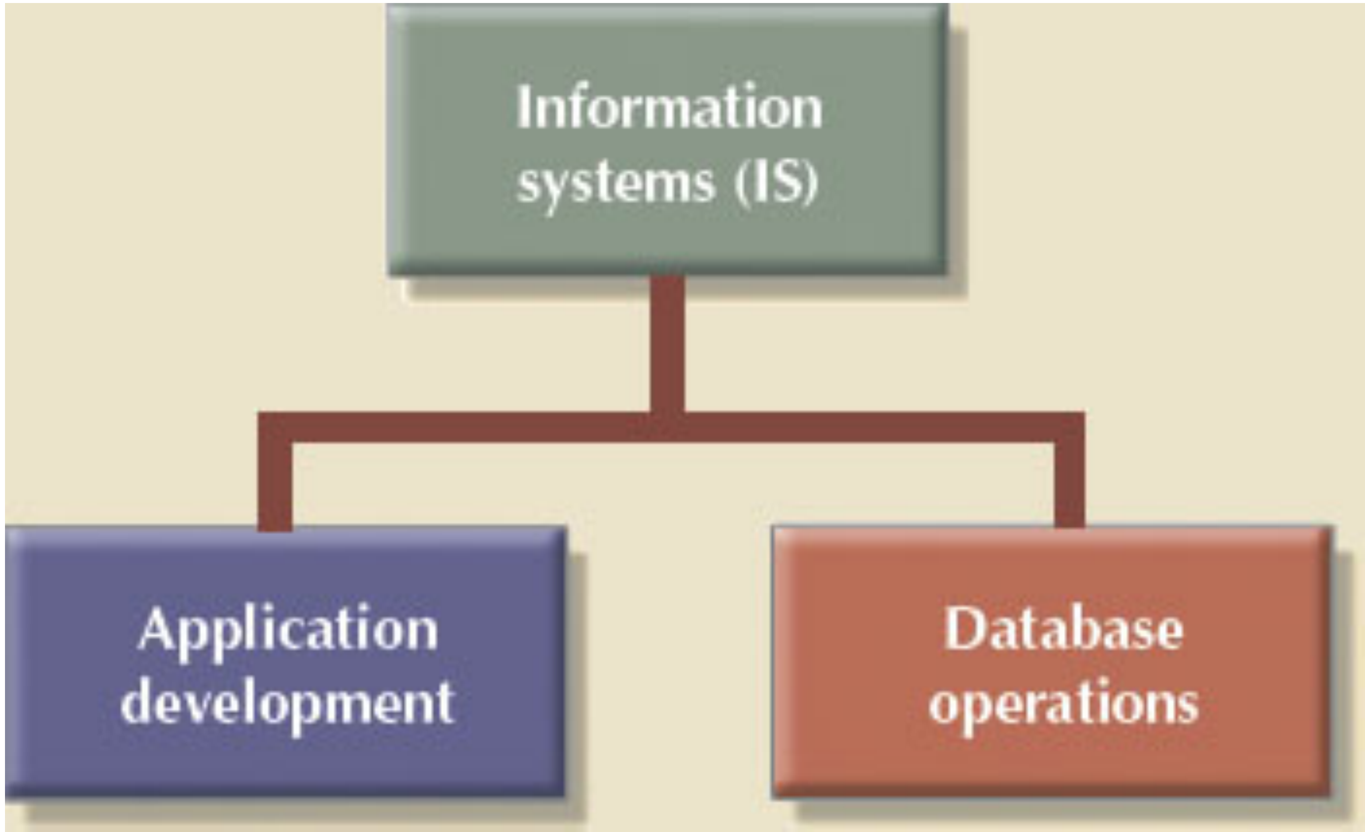


Figure 16.3 - The Placement of the DBA Function

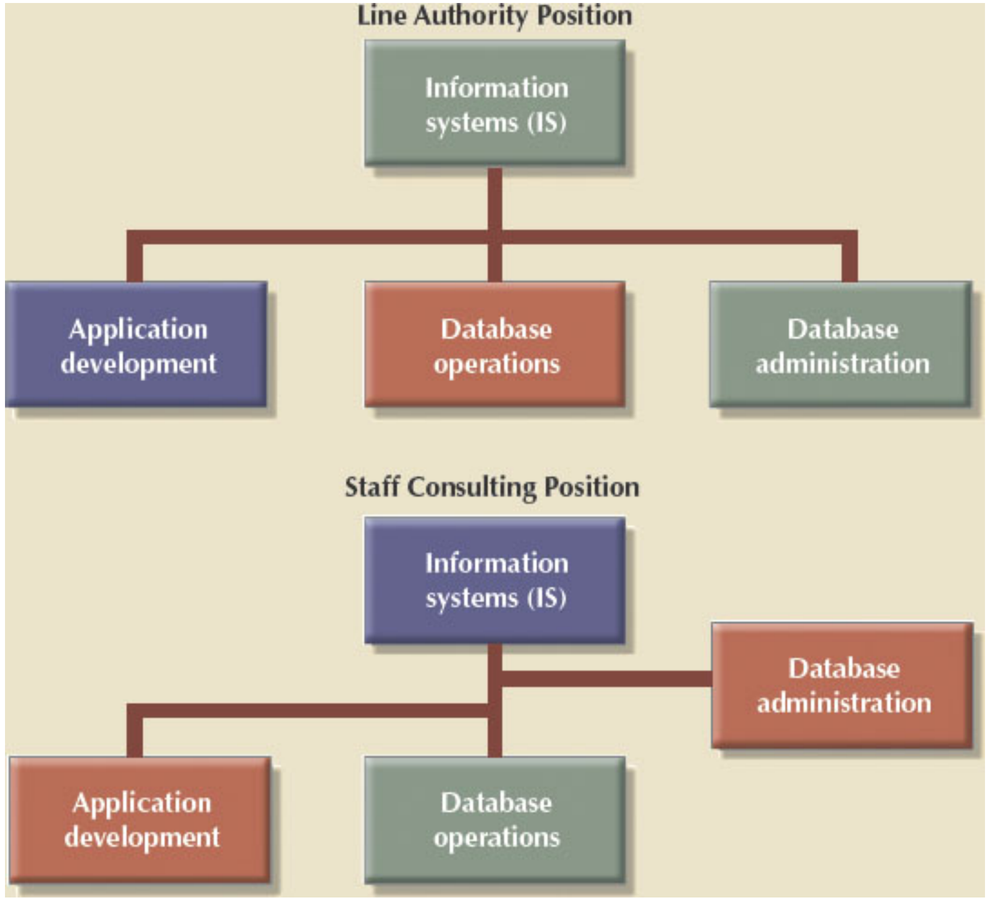


Figure 16.4 – A DBA Functional Organization

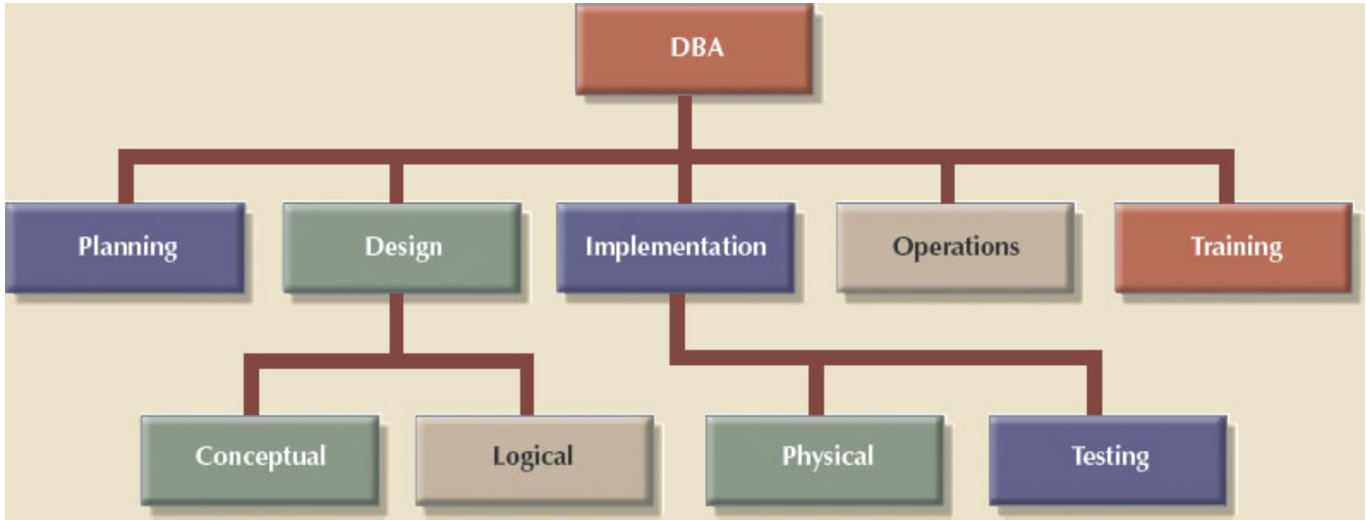


Table 16.1 - Contrasting DA and DBA Activities and Characteristics

DATA ADMINISTRATOR (DA)	DATABASE ADMINISTRATOR (DBA)
Performs strategic planning	Controls and supervises
Sets long-term goals	Executes plans to reach goals
Sets policies and standards	Enforces policies and procedures Enforces programming standards
Job is broad in scope	Job is narrow in scope
Focuses on the long term	Focuses on the short term (daily operations)
Has a managerial orientation	Has a technical orientation
Is DBMS-independent	Is DBMS-specific

Table 16.2 - Desired DBA Skills

MANAGERIAL	TECHNICAL
Broad business understanding	Broad data-processing background and up-to-date knowledge of database technologies
Coordination skills	Understanding of Systems Development Life Cycle
Analytical skills	Structured methodologies • Data flow diagrams • Structure charts • Programming languages
Conflict resolution skills	Knowledge of Database Life Cycle
Communication skills (oral and written)	Database modeling and design skills • Conceptual • Logical • Physical
Negotiation skills	Operational skills: Database implementation, data dictionary management, security, and so on

Experience: 10 years in a large DP department

DBA’s Managerial Role (1 of 4)

- Provide end-user support
- Enforce policies, procedures, and standards for correct data creation, usage, and distribution within the database
- Manage data security, privacy, and integrity
- Manage data backup and recovery
  - Fully recover data in case of data loss
  - **Database security officer (DSO)**: Ensures database security and integrity

DBA’s Managerial Role (2 of 4)

- **Disaster management**: Planning, organizing, and testing of database contingency plans and recovery procedures
- Backup and recovery measures must include at least periodic data and application backups:
  - **Full backup** or **database dump**: Produces a complete copy of the entire database
  - **Incremental backup**: Produces a backup of all data since the last backup date
  - **Concurrent backup**: Takes place while the user is working on the database

DBA’s Managerial Role (3 of 4)

- Backup and recovery measures must include at least:
    - Proper backup identification
    - Convenient and safe backup storage
    - Physical protection of both hardware and software
    - Personal access control to the software of a database installation
    - Insurance coverage for the data in the database

DBA's Managerial Role (4 of 4)

- Additional points:
  - Data recovery and contingency plans must be tested, evaluated and practiced frequently
  - Backup and recovery plan not likely to cover all information system components
- Ensure data is distributed to the right people at the right time and in the right format

DBA's Technical Role

- Evaluate, select, and install DBMS and related utilities
- Design and implement databases and applications
- Test and evaluate databases and applications
- Operate the DBMS, utilities, and applications
- Train and support users
- Maintain the DBMS, utilities, and applications

Security Goals

- **Confidentiality**: Protecting data against unauthorized access
- **Compliance**: Activities that meet data privacy and security reporting guidelines
- **Integrity**: Keeping data consistent and free of errors or anomalies
- **Availability**: Accessibility of data whenever required by authorized users and for authorized purposes

Security Policies

- Collection of standards, policies, and procedures created to guarantee security
  - Ensures auditing and compliance
- Security audit process
  - Identifies security vulnerabilities
  - Identifies measures to protect the system

Security Vulnerabilities

- Weakness in a system component that could allow unauthorized access or cause service disruptions
- Categories: Technical, managerial, cultural, and procedural
- **Security threat**: Imminent security violation
- **Security breach**: Occurs when a security threat is exploited and could lead to a database whose integrity is preserved or corrupted

Table 16.4 - Sample Security Vulnerabilities and Related Protective Measures (1 of 3)

SYSTEM COMPONENT	SECURITY VULNERABILITY	SECURITY MEASURES
People	• The user sets a blank password. • The password is short or includes a birth date. • The user leaves the office door open all the time. • The user leaves payroll information on the screen for long periods of time.	• Enforce complex password policies. • Use multilevel authentication. • Use security screens and screen savers. • Educate users about sensitive data. • Install security cameras. • Use automatic door locks.
Workstation and servers	• The user copies data to a flash drive. • The workstation is used by multiple users. • A power failure crashes the computer. • Unauthorized personnel can use the computer. • Sensitive data is stored on a laptop computer. • Data is lost due to a stolen hard disk or laptop. • A natural disaster occurs.	• Use group policies to restrict the use of flash drives. • Assign user access rights to workstations. • Install uninterrupted power supplies (UPSs). • Add security locks to computers. • Implement a kill switch for stolen laptops. • Create and test data backup and recovery plans. • Protect the system against natural • disasters—use co-location strategies.

Table 16.4 - Sample Security Vulnerabilities and Related Protective Measures (2 of 3)

SYSTEM COMPONENT	SECURITY VULNERABILITY	SECURITY MEASURES
Operating system	• Buffer overflow attacks • Virus attacks • Root kits and worm attacks • Denial-of-service attacks • Trojan horses • Spyware applications • Password crackers	• Apply OS security patches and updates. • Apply application server patches. • Install antivirus and antispyware software. • Enforce audit trails on the computers. • Perform periodic system backups. • Install only authorized applications. • Use group policies to prevent unauthorized installations.
Applications	• Application bugs—buffer overflow • SQL injection, session hijacking, etc. • Application vulnerabilities—cross-site scripting, nonvalidated inputs • Email attacks—spamming, phishing, etc. • Social engineering emails	• Test application programs extensively. • Build safeguards into code. • Do extensive vulnerability testing in applications. • Install spam filters and antivirus software for email systems. • Use secure coding techniques (see www.owasp.org). • Educate users about social engineering attacks.

Table 16.4 - Sample Security Vulnerabilities and Related Protective Measures (3 of 3)

SYSTEM COMPONENT	SECURITY VULNERABILITY	SECURITY MEASURES
Network	• IP spoofing • Packet sniffers • Hacker attacks • Clear passwords on network	• Install firewalls. • Use virtual private networks (VPNs). • Use intrusion detection systems (IDSs). • Use network access control (NAC). • Use network activity monitoring.
Data	• Data shares are open to all users. • Data can be accessed remotely. • Data can be deleted from a shared resource.	• Implement file system security. • Implement share access security. • Use access permission. • Encrypt data at the file system or database level.

Database Security

- DBMS features and related measures that comply with the security requirements
- **Authorization management**: Procedures to protect database security and integrity
  - User access management
  - View definition
  - DBMS access control
  - DBMS usage monitoring
    - **Audit log**: Automatically records description of database operations performed by all users

Database Administration Tools

- Database monitoring
- Database load testing
- Database performance tuning
- SQL code optimization
- Database bottleneck identification and remediation
- Database modeling and design
- Database data extraction, transformation, and loading

Data Dictionary (1 of 2)

- Two main types:
  - Integrated - Included with the DBMS
  - Standalone - Third-party systems
- **Active data dictionary**: Automatically updated by the DBMS with every database access
- **Passive data dictionary**: Requires running a batch process
- Main function - Store description of all objects that interact with the database

Data Dictionary (2 of 2)

- Key element of information resource management
  - Can be described as the **information resource dictionary**
- Metadata is the basis for monitoring database use and for assigning access rights to users
- DBA uses data dictionary to support data analysis and design

Computer-Aided Systems Engineering (CASE) Tools

- Automated framework for the Systems Development Life Cycle (SDLC)
- Use structured methodologies and powerful graphical interfaces
- Classified according to extent of support provided:
  - **Front-end CASE tools**: Provide support for the planning, analysis, and design phases
  - **Back-end CASE tools**: Provide support for the coding and implementation phases

Components of a CASE Tool

- Graphics
- Screen painters and report generators
- Integrated repository
- Analysis segment
- Program documentation generator

Developing a Data Administration Strategy

- **Information engineering (IE)**: Translates strategic goals into data and applications
- **Information systems architecture (ISA)**: Helps plan, develop, and control future information systems
- Critical success factors:
  - Management commitment and defined standards
  - Thorough analysis of the company situation
  - End-user involvement
  - Training and a small pilot project

DBA's Role in the Cloud

- Significant impact on role of DBAs
- Tasks split between internal DBA and cloud service provider
- Cloud service partner company provides:
  - DBMS installation and updates
  - Server/network management
  - Backup and recovery operations

Oracle Database Administration Tools

- Ensure the RDBMS starts automatically
- Create tablespaces and datafiles
  - **Tablespace**: Logical storage space
  - **Datafile**: Physically stores the database’s data
- Manage users and establish security
  - **User**: Allows a given person to log on to the database
  - **Role**: Authorizes a user to connect to the database and use its system resources
  - **Profile**: Controls how much of the database resource a given user can access

Types of Tablespace

- SYSTEM
  - Stores the data dictionary data
- USERS
  - Stores the table data created by the end users
- TEMP
  - Stores the temporary tables and indexes created during the execution of SQL statements
- UNDOTBS1
  - Stores database transaction recovery information

Customize Database Initialization Parameters

- Fine-tuning a database is an important task that usually requires modification of parameters
- Initialization parameters reserve resources used by the database at run time
- After modifying parameters database restart may be required