Computer Hardware
Operating Systems (OS) & System Software
Applications
Distributed Systems vs. Legacy Systems
Production Environment vs. Development and Testing Environments
General Control and Application Reviews
Computer Hardware

- Definition: All physical mediums to record, retrieve, store, process, input, output, and transmit digital and analog signals/information.
  - CPU
  - Hard drive
  - Memory
  - Mother Board
  - Video Card/Sound Card/Camera
  - Network Interface Card
  - CD ROM/USB/PS2 Connector
  - Mobile Devices
OS Built-in Controls: authentication and authorization, scheduler, traffic controller, planner, and security to resources of a computer system and/or its network (wired or wireless).

- Microsoft Windows
- UNIX/Linux
- Novell Netware,
- AS/400 & Mainframe

Some OS work with third party security software:
- Mainframe – TOP Secret, ACF2, RACF
System Software

* System Software: software used by System users (such as Database Administrator (DBA) System Administrator (SA) to support the running of OS

* Database Management Systems, SQL, Network Client, OnLine Transaction Processors (OLTP), etc.

* System Utilities such as FTP, Telnet, SNA and Shell Scripts
Databases

- Types of Databases
  - Flat-file
  - Hierarchical Database
  - Network Database
  - Relational Database
- Benefits of database versus traditional file organization
- Audit Concerns in a Database Environment
Databases Pros. And Cons.

Benefits

* Data independence (e.g. n-tier application)
* Reduction of data redundancy (via Normalization)
* Maximize data consistency (primary key/foreign key)
* Reducing maintenance cost through data sharing
* Security Feature
* Enforce Data integrity
Databases Pros. And Cons.

**Drawbacks**

* Steep Learning Curve
* Complex Tech Support
Database Terminology (continued)

**Database Management System (DBMS)**

- Access and control functions;
- A variety of management and security features
- Older versions are hierarchical, in that there is a specific and somewhat rigid "parent and child" relationship among data elements
- Newer versions are relational, allowing dynamic reformatting of the tables that drive data access, so that they are more flexible and adaptable to changing needs
Database management systems have features to help ensure the integrity and security of data stored in the DBMS tables. These include:

- Rules
- Triggers
- A Stored Procedure
- Security
Database Administration (DBA)

A function involved in the coordination and control of data related activities, the DBA can be one or more people, depending on how large the environment is.
Database Terminology (continued)

Data Dictionary/ Directory System (DD/DS) : Software that manages a repository of information about data and the database environment, allowing applications to share data elements and each application to have its own view of that data.

In Relational Databases, Data is organized into tables, columns and rows. A table is equivalent to a file, as it represents a collection of records. A row is a horizontal set of data fields or components. A column is a vertical set of data fields or components (think of a spreadsheet's rows and columns for a comparison).
Rules define format and range of data that can be stored. For example, a rule can stipulate that a "loan interest" field cannot hold a negative number, or that allowable rates will be within a range of 6-12%.
**Triggers** can activate a DBMS stored procedure when a field, record or table is inserted, updated or deleted. For example, a trigger can cause an email to be sent to the security administrator when a record in the USER ID table is added or deleted.
A stored procedure is a program written in the native language of the DBMS. Stored procedures behave like any other program, although native DBMS has additional verbs for database actions unique to the DBMS environment. Examples include SORT, LOCK, UNLOCK and COMMIT.
Because relational databases are highly customizable, users can present data in any way they wish.

One of the most important concepts of the database is known as a view. Although the data is stored in tables, which may never change attributes, users can customize or delete a view easily without affecting the data.

Views manipulate the data to present the important pieces that users would like to see, while removing the unnecessary data that is not used. This is similar to copying and pasting the important parts of documents into one file.
DBMS Security Features

- **Security** features - the DBMS provides ability to allow or deny a user or group access to a database, table, record or field. Some systems can also allow or deny a user or group administration ability. Additional security features including data encryption and scrambling.

- **DBMS Access Controls**: users, programs, transactions, etc.

- **Audit Trails**
Types of Databases

A database management system (DBMS) manages data by providing organization, access, control and security functions. There are four classes of database structures. They are listed in the order of their evolutionary appearance:

- Flat File
- Hierarchical
- Networked
- Relational
Flat-File: A flat-file stores records without any relationships what so ever. Records can be stored in any arbitrary sequence, or in the order they were created. There can be one or more indices to optimize searching for records.
Hierarchical Database

A hierarchical database stores records in a hierarchical order such as last name, customer number, or part number. Every record contains the record data and pointers to the child records. Some hierarchical databases also store pointers to the parent records. Records are placed into the database in the order they appear in the physical word.
Hierarchical Database

* All searches begin at the top of the database. Following pointers down (or up) take you from record-to-record in their sorted order

* If a new record needs to be inserted into the structure, the position of the record on the disk does not change; only the pointers need to be updated

* A hierarchical database can have only one top (or root) record
A network database is similar in construction to a hierarchical database except there can be more than one root record.
A relational database is a collection of data items organized as a set of formally described tables from which data can be accessed easily. A relational database is created using the relational model. The software used in a relational database is called a relational database management system (RDBMS).

Relational term

- relation, base relvar
- derived relvar
- tuple
- attribute

SQL equivalent

- table
- view, query result, result set
- row
- column
Examples of relational databases include:

* DB2
* Informix
* Lotus Approach
* MS Access
* Oracle
* SQL Server
* Sybase
Audit Concerns in a Database Environment

- The database can become the single point of failure.
- When the database is unavailable, all applications relying on the database will not work.
- Many applications might be authorized to update the same data fields.
- How do applications become authorized?
- What is the synchronization schedule for the databases replicates?
- Applications working against the database may not have the same security and integrity controls.
- Distributed copies of the database may not have the same security settings.
Chapter 9 – Auditing Databases

* Database vulnerabilities and threats:
  - Easily guessed passwords
  - Missing Patches
  - Misconfigurations
  - Excessive Privileges
  - Web application attacks (SQL-injection)
  - Insider mistakes
  - Weak or non-existent audit controls
  - Social engineering
Chapter 9 – Auditing Databases

* **Oracle Defaults example**
  * - User Account: system / Password: manager
  * - User Account: sys / Password: change_on_install
  * - User Account: dbsnmp / Password: dbsnmp

* **Microsoft SQL Server & Sybase Defaults**
  * - User Account: SA / Password: null

* **Safeguards against password crackers:**
  * - Not all databases have Account Lockout
  * - Database Login activity is seldom monitored
  * - Scripts and Tools for exploiting weak passwords are widely available
Chapter 9 – Auditing Databases

* Missing Patches:
  * Privilege Escalation
    * – Become a DBA or equivalent privileged user
  * Denial of Service Attacks
    * – Result in the **database crashing or failing to respond** to connect requests or SQL Queries.
  * Buffer Overflow Attacks: memory safety issue
    * – Result in an **unauthorized user** causing the application to perform an action the application was not intended to perform.
    * – **Can allow arbitrary commands to be executed** no matter how strongly you’ve set passwords and other authentication features.
Chapter 9 – Auditing Databases

- **Misconfigurations Can Make Databases Vulnerable**
  - **Oracle**
    - External Procedure Service
    - Default HTTP Applications
    - Privilege to Execute UTL_FILE
  - **Microsoft SQL Server**
    - Standard SQL Server Authentication Allowed
    - Permissions granted on xp_cmdshell
  - **Sybase**
    - Permission granted on xp_cmdshell
  - **IBM DB2**
    - CREATE_NOT_FENCED privilege granted (allows logins to create SPs)
  - **MySQL**
    - Permissions on User Table (mysql.user)
Chapter 9 – Auditing Databases

Database Security Lifecycle – Management Aspects

- Inventory
- Classification: e.g. confidential, internal user, public, etc.
- Access
- Prioritize
- Remediation
- Monitoring
Chapter 9 – Auditing Databases

* Secure Configuration/Hardening Standards
* Patching Process
* Implement the Principal of Least Privilege
* Defense in Depth / Multiple Levels of Security
* Vulnerability Scan
* Remediation Action Plan
* Active monitoring
* Encryption of data-in-motion / data-at-rest
Chapter 9 – Auditing Databases

- Strong Password policy
- Patch Management
- Database Server Security
- Disable non used functions
- Use selective encryption:
  - At network level: use SSL, database proprietary protocols.
  - At file level for backups, laptops, etc.
- Object and system permissions
- Restriction on new database installations
- DBA Privileges!!!
- DBMS configurations and settings – best practices & hardening standards
- Audit trail aggregation and monitoring – e.g. SIEM
Chapter 9 – Auditing Databases

- Database Related Policies & Procedures:
  - DB Version, patch level
  - Build & Hardening Standard
  - OS Security Requirements

- Database Directory and Registry Key Access

- Database Authentication and Authorization
  - Provisioning and de-provisioning process
  - Password Requirements
  - Default Usernames and Passwords
  - Service Accounts
  - Remove “Public” Permission
  - Access to Database objects (tables, views, triggers, store procedures, etc.)
Chapter 9 – Auditing Databases

- Encryption (Data-in-Use, At-Rest, In-Motion)
  - Network Encryption
  - Back up Encryption
- Monitoring
  - Logging and Audit trail
  - Reviewing Practice
- Capacity Planning and Performance Monitoring
- Database Backup, Restore and Recovery