ARDHI UNIVERSITY

SCHOOL OF EARTH SCIENCE, REAL ESTATE, BUSINESS AND INFORMATICS (SERBI)

DEPARTMENT OF COMPUTER SYSTEM AND MATHEMATICS (CSM)

BACHELOR OF SCIENCE IN INFORMATION SYSTEM MANAGEMENT (B.Sc. ISM)

SEMESTER II, THIRD YEAR 2023/2024

IS353 INFORMATION SYSTEMS AUDIT AND CONTROL

INSTRUCTOR NAME: Dr. EMMANUEL FREDY MWAKASEGE

TASK: GROUP 04 ASSIGNMENT 01

GROUP PARTICIPANTS

SN	NAME	REGISTRATION NUMBER
1	JOHN Z PETRO	27829/T.2021
2	ANITHA S MUGASHA	26933/T.2021
3	PEVSON R KAHWA	26999/T.2021
4	THOMAS N JOSEPH	27017/T.2021
5	ROSE E MWANJALILA	27005/T.2021
6	LUCIA E NGALYA	26983/T.2021

QUESTION: With respect to organization controls over information and processes, discuss "Database controls" in details. Provide clear examples to support your explanations.

In modern organizations, databases play a critical role in storing, managing, and retrieving vast amounts of information. Database controls are the unsung heroes of information system security, silently safeguarding the lifeblood of many organizations. These controls ensure the Confidentiality, Integrity, and Availability (CIA triad) of information stored within databases, minimizing risks and maximizing trust. Let's delve into the key aspects of database controls along with detailed examples:

1. Access Controls

Access controls are foundational in regulating who can access the database and what actions they can perform. Imagine a high-security building. Access controls for databases function similarly. Their primary purpose is to restrict access to the database itself and specific data elements based on a user's role and responsibilities. This includes:

i. **User Authentication:** The first line of defense is verifying a user's identity before granting entry. Multi-factor authentication (MFA) adds an extra layer of security by requiring a second verification factor, like a code from a smartphone app, alongside a traditional password. Single sign-on (SSO) streamlines the process by allowing users to access multiple databases with a single login, reducing the risk of password fatigue and forgotten credentials.

   Example: A healthcare organization requires doctors to use their unique username and password, along with a fingerprint scan, to access patient records in the electronic health record (EHR) system.

ii. **User Authorization:** Not everyone needs access to everything. User authorization assigns specific permissions to users based on their job functions. For instance, a customer service representative might only require read access to view customer contact information for troubleshooting purposes. In contrast, a finance manager might have read-write access to update customer account details

   Example: A finance department employee has read-only access to financial data, while the finance manager has permission to modify and approve financial transactions.

iii. **Role-based Access Control (RBAC):** This approach simplifies permission management by defining user roles with predefined access levels. Instead of managing individual user privileges for each data element, users are assigned roles that inherit specific permissions. This ensures consistency and reduces the risk of accidental permission oversights

   Example: In an educational institution, teachers have access to student grades and attendance records, while administrative staff can manage student enrollment and scheduling.

2. Data Security Controls

Data security controls are the bodyguards of the database, safeguarding information from unauthorized access, modification, or deletion. In today's digital age, where cyber threats are ever-present, these controls are vital for building trust and protecting sensitive data.

i. **Data Encryption**: Encryption scrambles data using a secret key, making it unreadable to anyone who doesn't possess the key. This is particularly important for highly sensitive data like credit card numbers or social security numbers. Data can be encrypted at rest (when stored in the database) and in transit (when being transferred between systems). Imagine a locked briefcase for your data even if someone intercepts it, they can't access the contents without the key. This involves:

   a) **Encrypting Data-at-Rest**: Utilizing encryption algorithms to protect data stored on disk or in backups from unauthorized access.

   Example: A financial institution encrypts customer account numbers and personal information stored in its database to prevent unauthorized access in the event of a data breach.

   b) **Encrypting Data-in-Transit**: Encrypting data as it travels between the database server and client applications to prevent eavesdropping and tampering.

   Example: Using SSL/TLS encryption to secure data transmitted between a web application and the database server during online banking transactions.

ii. **Database Activity Monitoring**: Constant vigilance is key. Database activity monitoring keeps a watchful eye on all database access attempts, including successful logins and failed attempts. This allows security personnel to detect suspicious activity, such as repeated failed logins or attempts to access unauthorized data. Think of security cameras for your database they record activity, providing an audit trail for potential investigations.

3. Audit Trails

Audit trails provide a detailed record of database activities, helping organizations monitor and investigate security incidents. This includes:

i. **Logging database activities**: Capturing and logging all user actions, including logins, queries, modifications, and access attempts.

   Example: An e-commerce platform logs every user interaction with the database, including product searches, purchases, and account updates, to track customer behavior and detect any suspicious activities.

ii. **Forensic Analysis**: Analyzing audit trail data to identify security breaches, unauthorized access, or data manipulation.

Example: After detecting a data breach, a cybersecurity team reviews database audit logs to determine the extent of the intrusion and identify the compromised accounts.

4. **Data Integrity Controls**

Data integrity controls ensure the accuracy, consistency, and reliability of data stored in the database. This involves:

i. **Referential Integrity Constraints**: Enforcing relationships between tables to maintain data consistency and prevent orphaned or invalid records.

Example: A customer cannot be deleted from the database if they have associated orders, ensuring that the database maintains referential integrity.

ii. **Data Validation Rules**: Implementing rules and constraints to validate data input and prevent the entry of incorrect or invalid data. Data validation acts as a gatekeeper at the point of entry. It enforces rules to ensure data entered conforms to specific formats and ranges.

Example 1: A database for a vehicle registration system validates license plate numbers to ensure they meet the specified format and do not contain special characters.

Example 2: Date Field: Might only accept entries in a YYYY-MM-DD format, preventing nonsensical entries like "blue Tuesday."

Example 3: Age Field: Might restrict values to a valid range, say, between 18 and 120.

5. Disaster Recovery Planning

Disaster recovery planning ensures that organizations can recover from database failures or data loss events with minimal disruption. This includes:

i. **Backup and Restore Procedures**: Establishing regular backup schedules and procedures to create copies of the database that can be restored in case of data loss or corruption.

Example: An online retailer performs daily backups of its product catalog and customer database, stored both on-site and off-site, to protect against data loss due to hardware failures or cyberattacks.

ii. **Failover and Redundancy**: Implementing failover systems and redundant hardware to maintain database availability in the event of hardware failures or network outages.

Example: A financial institution uses a mirrored database server located in a different geographic region to ensure uninterrupted access to customer accounts and transactions.

iii. **Testing and Maintenance**: Regularly testing disaster recovery plans and conducting maintenance activities to ensure they remain effective and up-to-date.

Example: A healthcare provider conducts quarterly drills to simulate database failures and practice the execution of its disaster recovery plan, identifying areas for improvement and optimization.