To protect the DBMS against service degradation there are certain minimum recommended security safeguards. For example:

• Change default system passwords.
• Change default installation paths.
• Apply the latest patches.
• Secure installation folders with proper access rights.
• Make sure only required services are running.
• Set up auditing logs.
• Set up session logging.
• Require session encryption.

Protecting the data in the database is a function of authorization management. Authorization management defines procedures to protect and guarantee database security and integrity. Those procedures include, but are not limited to, user access management, view definition, DBMS access control, and DBMS usage monitoring.

• **User access management**: This function is designed to limit access to the database and likely includes at least the following procedures:

• **Define each user to the database**: This is achieved at the operating system level and at the DBMS level. At the operating system level, the DBA can request the creation of a logon user ID that allows the end user to log on to the computer system. At the DBMS level, the DBA can either create a different user ID or employ the same user ID to authorize the end user to access the DBMS.

• **Assign passwords to each user:** This, too, can be done at both operating system and DBMS levels. The database passwords can be assigned with predetermined expiration dates. The use of expiration dates enables the DBA to screen end users periodically and to remind users to change their passwords periodically, thus making unauthorized access less probable.

• **Define user groups**: Classifying users into user groups according to common access needs facilitates the DBA's job of controlling and managing the access privileges of individual users. Also, the DBA can use database roles and resource limits to minimize the impact of rogue users in the system.

• **Assign access privileges**: The DBA assigns access privileges or access rights to specific users to access specified databases. An access privilege describes the type of authorized access. For example, access rights may be limited to read-only, or the authorized access might include READ, WRITE, and DELETE privileges. Access privileges in relational databases are assigned through SQL GRANT and REVOKE commands.

• **Control physical Access**: Physical security can prevent unauthorized users from directly accessing the DBMS installation and facilities. Some common physical security practices found in large database installations include secured entrances, password-protected workstations, electronic personnel badges, closed-circuit video, voice recognition, and biometric technology.

• **View definition**: The DBA must define data views to protect and control the scope of the data that are accessible to an authorized user. The DBMS must provide the tools that allow the definition of views that are composed of one or more tables and the assignment of access rightsto a user or a group of users. The SQL command CREATE VIEW is used in relational databases to define views.