Answer 2

If a user creates a new relation r1 with a foreign key referencing another relation r2. The user needs at least **SELECT** privileges on the relation r2.

If an admin has not allowed the **SELECT** privilege to any user, the administrator does not want anyone to read that data. If the administrator has created a table r1, where some confidential data is stored. For general users to reference a foreign key referencing from r1, they need the read privileges for r2. If the administrator wants a user to be able to reference a foreign key, the administrator has to give **SELECT** privileges to that user.

If this type of access is allowed for all users without any authorization, any user can read any attribute from any table. Clearly, we don't want this approach as we want to give administrators more control over who can access which table.

Answer 3

Integrity constraints define what type of values can exist in attributes of a table. It includes constraints about the type of data that can be inserted into the table, specific constraints on the values, constraints about uniqueness in a column, whether null values are allowed or not, constraints about the default values of a column. They might define special checks on individual values in cells.
While on the other hand authorization constraints are related to which type of queries are allowed for which users. They include who can read which tables, can update which type of tables, can reference attributes from other tables, can read views, can update views, can grant access to other users, can revoke access to other users, can grant access to others to grant access, etc. These are more related to users interacting with the database.

Answer 4

Part 1

There is a total of 6 actions in the given procedure.
Assuming that before step 1, user D does not have any privilege.
After step 1, user D does **not have** SELECT ON T privilege.
After step 2, user D does **not have** SELECT ON T privilege.
After step 3, user D does do have SELECT ON T privilege.
After step 4, user D does do have SELECT ON T privilege.
After step 5, user D does do have SELECT ON T privilege.
After step 3, user D does **not have** SELECT ON T privilege.

User D gets access to after step 3 by user C. After step 6, user A revokes SELECT ON T privilege C which is being cascaded to all the users which user C has granted privilege. And hence, user D loses the privilege.

Part 2

User C has first received the privilege from user A. After step 5, access is revoked from user B and which is not propagated to other users. Because user B has received the privilege from user A which is not revoked anywhere, so user C will continue having access to SELECT ON T access.