Question: 1

Which of the following can be accomplished by altering a table to use column access control?

A. Restrict the access to specific rows for all or some users
B. Hide column definitions from the DB2 catalog table SYSIBM.SYSCOLUMNS
C. Pre-materialize a view with the changed values provided by the column mask
D. Modify the values returned for table columns based on column masking definitions

Answer: D

Question: 2

Which of the following is an advantage of role-based security?

A. If you DROP a role that owns objects, those objects will also be dropped
B. Within a trusted connection. DB2 allows multiple roles to be associated with any given thread at any point in time
C. Roles are used to provide a more flexible technique than security group definitions or userids in assigning and controlling authorization
D. If a role creates an object, a user requires no additional privileges to access the object if the access uses that role as the object owner in the SQL statement

Answer: A

Question: 3

For best DB2 lock avoidance, which of the following BIND/REBIND options should be included in the REBIND command execution?

A. ACQUIRE(USE)ISOLATION(CS)
B. ACQUIRE(USE)ISOLATION(RR)
C. CURRENTDATA(NO)ISOLATION(CS)
D. CURRENTDATA(YES) ISOLATION(CS)

Answer: C

Explanation:
https://www.ibm.com/support/knowledgecenter/SSEPEK_12.0.0/perf/src/tpc/db2z_chooseisolation option.html

Question: 4

Which authority prevents unintended access to user data but allows installation or migration of a DB2 subsystem?

A. SYSADM
B. SYSCTRL
C. Installation SYSADM
D. Installation SYSOPR

Answer: D

Explanation:
https://www.ibm.com/support/knowledgecenter/SSEPEK_12.0.0/inst/src/tpc/db2z_requiredauth4installation.html
You are not required to use the SYSADM or installation SYSADM authority to install or migrate a Db2 subsystem. Instead, you can use the installation SYSOPR authority to perform all installation or migration tasks while preventing unintended access to user data.

Question: 5

Which of the following is TRUE about the SYSCTRL authority?

A. It is designed to allow access to all data directly in DB2
B. It is designed not to be a part of the administrative authorizations
C. It is designed so group privileges cannot be granted to SYSCTRL
D. It is designed to be an administrator in a system with sensitive data

Answer: D

Explanation:
https://www.ibm.com/support/knowledgecenter/SSEPEK_10.0.0/seca/src/tpc/db2z_sysctrlauthority.html
The SYSCTRL authority is designed for administering a system that contains sensitive data. With the SYSCTRL authority, you have nearly complete control of the DB2® subsystem. However, you cannot access user data directly unless you are explicitly granted the privileges to do so.