

Common Enterprise Control Weaknesses

DBMS Environment

The following is a summation of the most common internal control weaknesses that exist within various DBMS (e.g., DB2, MS SQL Server, Oracle, Lotus Notes):

Issue	Description
User Access	<ul style="list-style-type: none">• Users with inappropriate privileged access to the database and operating system installation and source files.• Developers with inappropriate privileged access to the production environment, including acting as database administrators (DBAs) in the production environment.
Passwords	<ul style="list-style-type: none">• Usernames and passwords which had been embedded into scripts to support backup procedures.• Default accounts and passwords enabled on the database.• Minimum password length set to one digit.• Passwords identical to user names.
Unauthorized Users	<ul style="list-style-type: none">• Terminated users remaining in the system.
Account Lockout	<ul style="list-style-type: none">• User account lockouts are not enabled.
Privileged Access	<ul style="list-style-type: none">• Tools in use may allow privileged access to databases outside of the application.

NT Operating System Environment

The following is a summation of the most common internal control weaknesses affecting operating system security on the NT platform:

Issue	Description
Guest Passwords	User passwords being broken using freely available password programs.
Guest Accounts	The guest accounts not disabled and the default passwords not changed.
Shutting Down the System	Unauthorized users having the privilege to shut down the servers.
Legal Notice	No legal notice displayed at the logon screen level.
Account Lockout	Accounts may not be set to lock out in the event of multiple (five) incorrect password attempts.
Account Reset	Accounts may be automatically reset after a minimal amount of time (e.g., 20 minutes).
Password Age	No maximum password age set (e.g., 30 days) and the minimum password age may be set to 0 days.
Password History	The password history may not be set (e.g., remember the last 15 passwords).
Password Never	The option may not be disabled; therefore, expired users may not be asked to change their passwords at regular intervals.
Password Complexity	Default system passwords may not be changed, and the system may allow blank passwords.

Source: ISACA's Information Systems Control Journal, Volume 3, 2003