Understanding default permissions

If your security policies require more granular access control, you can grant or deny SQL compliance manager permissions on each audited SQL Server instance and archive database. These permissions determine whether a user can view audited events and the corresponding SQL statements by default.

You can set default permissions when you register a SQL Server instance to audit. When you set default permissions, SQL compliance manager grants read privileges to the guest account on the selected Repository databases. This setting allows a SQL Server login to view audit data collected from that registered SQL Server instance only.

You can also specify the appropriate permissions on each archive database that contains audit data. You can grant or deny access per database. When you set default permissions, SQL compliance manager grants read privileges to the guest account on the selected archive database only.

As you assign permissions, keep in mind that permissions granted to a login are applied along side any default permissions you set at the server or database level.