Step	Name	Client Assistance Request
1	**Test Access to Database Files - SQL Server 2008** LA-1: General system security settings are appropriate	Provide operating system security permissions for the following SQL Server database system files: - Binaries and utilities Provide the organization's baseline security standards for the operating system (e.g. Windows or UNIX) of the selected server.
2	**Test Default Accounts & Passwords - SQL Server 2008** LA-1: General system security settings are appropriate	Provide a report of all system users in the current database, showing whether default accounts have been updated / deleted. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: select * from sys.syslogins
3	**Test Host Based Authentication - SQL Server 2008** LA-1: General system security settings are appropriate	Provide the system settings for Server Authentication. This is typically obtained by executing the following: STEP 1: <Right-click> appropriate server instance. STEP 2: Click [properties]. STEP 3: Click [Security] tab.
4	**Test Account Lockout - SQL Server 2008** LA-2: Password settings are appropriate	There are two possible Windows authentication modes used to enforce password lockout: . Windows Authentication Mode . SQL Server and Windows Authentication Mode If Windows Authentication mode is in use, provide a report showing that Windows Authentication is being used. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [START] – [PROGRAMS] – [MICROSOFT SQL SERVER], then click on [SQL SERVER MANAGEMENT STUDIO] to launch the SQL Server Management tool. STEP 2: In the left-hand pane, expand the server group, right-click on the server and select Properties. STEP 3: On the Security Tab, under Authentication, the options are 'Windows Authentication Mode' or 'SQL Server and Windows Authentication Mode'. Take a screenshot of this screen. If Windows Authentication is in use, provide a report of the password policy, outlining complexity requirements and minimum password length. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [Start]-[Programs] - [Administrative Tools] - [Local Security Policy]. STEP 2: Click on [Account Policies] - [Account Lockout Policy]. Take a screenshot of this screen.

		If SQL Server and Windows Authentication mode is in use and SQL Server 2008 is being run on Windows Server 2003, also provide a report of SQL logins which have Windows Password policy applied. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: select * from sys.sql_logins
5	**Test Idle Session Timeout - SQL Server 2008** LA-2: Password settings are appropriate	Provide a screenshot of the idle timeout setting by performing the following: STEP 1 : Open SQL Server Management Studio. Ensure that you open a connection to Analysis Server (not Database Engine). In the Object Explorer pane, right-click the server to which you have connected. Click the Properties menu item. Ensure the General page is selected, as it will be by default. Click the Show Advanced (All) Properties check box. STEP 2 : Locate the IdleConnectionTimeout setting and take a screenshot.
6	**Test Logging of Unsuccessful Login Attempts - SQL Server 2008** LA-2: Password settings are appropriate	Provide a screenshot of the auditing of failed login attempts using SQL Server Management Studio: STEP 1: <Right-click> appropriate server instance. STEP 2: Click [Properties]. STEP 3: Click [Security] tab and take a screenshot. Provide details around the following: - the frequency with which failed login attempts are reviewed, - the procedures for addressing failed login attempts of a suspicious and recurring nature and - if failed-login attempt reports are filed or safeguarded in some other manner. Provide a file of failed login attempt reports.
7	**Test Password Composition - SQL Server 2008** LA-2: Password settings are appropriate	There are two possible Windows authentication modes used to enforce password complexity and a minimum password length: . Windows Authentication Mode . Mixed Mode If Windows Authentication mode is in use, provide a report showing that Windows Authentication is being used. This is typically obtained by taking a screenshot of the following:

		STEP 1: Click on [START] – [PROGRAMS] – [MICROSOFT SQL SERVER], then click on [SQL SERVER MANAGEMENT STUDIO] to launch the SQL Server Management tool. STEP 2: In the left-hand pane, expand the server group, right-click on the server and select Properties. STEP 3: On the Security Tab, under Authentication, the options are 'Windows Authentication Mode' or 'SQL Server and Windows Authentication Mode'. Take a screenshot of this screen. If Windows Authentication is in use, provide a report of the password policy, outlining complexity requirements and minimum password length. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [Start] - [Programs] - [Administrative Tools] - [Local Security Policy]. STEP 2: Click on [Account Policies] - [Password policy]. Take a screenshot of this screen. If SQL Server and Windows Authentication mode is in use and SQL Server 2008 is being run on Windows Server 2003, also provide a report of SQL logins which have Windows Password policy applied. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: select * from sys.sql_logins
8	**Test Password Expiration - SQL Server 2008** LA-2: Password settings are appropriate	There are two possible Windows authentication modes to enforce password expiration: . Windows Authentication Mode . Mixed Mode If Windows Authentication mode is in use, provide a report showing that Windows Authentication is being used. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [START] – [PROGRAMS] – [MICROSOFT SQL SERVER], then click on [SQL SERVER MANAGEMENT STUDIO] to launch the SQL Server Management tool. STEP 2: In the left-hand pane, expand the server group, right-click on the server and select Properties. STEP 3: On the Security Tab, under Authentication, the options are 'Windows Authentication Mode' or 'SQL Server and Windows Authentication Mode'. Take a screenshot of this screen. If Windows Authentication is in use, provide a report of the password history. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [Start]-[Programs] - [Administrative Tools] - [Local Security Policy]. STEP 2: Click on [Account Policies] - [Password policy]. Take a screenshot of this screen. If SQL Server and Windows Authentication mode is in use and SQL Server 2008 is being run on Windows Server 2003, also provide a report of SQL logins which have Windows Password policy applied. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility:

		select * from sys.sql_logins
9	**Test Password History - SQL Server 2008** LA-2: Password settings are appropriate	There are two possible Windows authentication modes used to enforce password history: . Windows Authentication Mode . Mixed Mode If Windows Authentication mode is in use, provide a report showing that Windows Authentication is being used. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [START] – [PROGRAMS] – [MICROSOFT SQL SERVER], then click on [SQL SERVER MANAGEMENT STUDIO] to launch the SQL Server Management tool. STEP 2: In the left-hand pane, expand the server group, right-click on the server and select Properties. STEP 3: On the Security Tab, under Authentication, the options are 'Windows Authentication Mode' or 'SQL Server and Windows Authentication Mode'. Take a screenshot of this screen. If Windows Authentication is in use, provide a report of the password history. This is typically obtained by taking a screenshot of the following: STEP 1: Click on [Start]-[Programs] - [Administrative Tools] - [Local Security Policy]. STEP 2: Click on [Account Policies] - [Password policy]. Take a screenshot of this screen. If SQL Server and Windows Authentication mode is in use and SQL Server 2008 is being run on Windows Server 2003, also provide a report of SQL logins which have Windows Password policy applied. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: select * from sys.sql_logins
10	**Test Access to Privileged IT Functions - SQL Server 2008** LA-3: Access to privileged IT functions is limited to appropriate individuals	Provide a report of the roles assigned to all developers with access to the production database and their permissions, using the stored procedures sp_helpuser and the sp_helprotect. This is typically obtained by executing the following: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: sp_helprolemember 'db_securityadmin' sp_helprolemember 'db_owner' sp_helprolemember 'db_accessadmin' sp_helpsrvrolemember 'sysadmin' sp_helpsrvrolemember 'serveradmin' sp_helpsrvrolemember 'securityadmin'
11	**Test Access to Data Modification Utilities - SQL Server 2008** LA-4: Access to system resources	Please Provide: STEP 1) Using Windows Explorer Please provide Screen Shots for the Following - Right Click on Directory --> [Properties]-->[Security Tab]-->[Advanced]: - \Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn - \Program Files\Microsoft SQL Server\80\Tools\Binn - \Program Files\Microsoft SQL Server\80\Com

	and utilities is limited to appropriate individuals	
12	**Test Access to Production Data - SQL Server 2008** LA-4: Access to system resources and utilities is limited to appropriate individuals	If specific application roles are used to limit the access permissions of end-users, provide a report on the permissions assigned to the roles. This is typically obtained by executing the following commands: STEP 1: From the [START] menu open SQL Server Management Studio and click on [New Query] and select the [Results to File] icon or from the command line (click on [START] - [RUN] - type CMD in the 'Open:' text box) type sqlcmd -o 'filename' to launch the SQL Query utility outputting the results to the filename entered. STEP 2: Run the following query from within the SQL Query window or sqlcmd utility: EXEC sp_helprotect 'application rolename' The above query returns permissions for each application role.