3 Security Requirements

Below MS SQL Server security requirements are compiled using “Center for Internet Security Benchmark for MS SQL Server 2005”. The requirements are derived from CIS Level 1 settings which are generally considered safe to apply to most systems. The use of Level 1 settings is estimated not to have negative impact on performance or functionality.

Requirements are either mandatory (M) or recommended (R) as stated in column three in the following table.

#	Config Item	M/R	Action	Description
1.	**Operating System and Network Specific Configuration**			
2.	Physical security	M	Place the SQL Server in an area where it will be physically secure.	Place the server where only authorized personnel can obtain access.
3.	SQL Servers accessed via Internet	M	If the SQL Server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.	Limit the database contents of this SQL Server to information meant for public dissemination only.
4.	SQL Servers accessed via Internet	M	A firewall must be put between the SQL server and the Internet. Block TCP port 1433 and UDP port 1434 on the perimeter firewall. If named instances are listening on additional ports, these must be blocked too. In a multi-tier environment, consider to use multiple firewalls to create more secure screened subnets.	Consider separating Web logic and business logic onto separate computers.
5.	IPSEC	R	It is recommended to use IPSEC policy filters to block connections to ports other than the configured SQL Server ports.	IPSEC offers authentication, integrity, confidentiality, and anti-replay services. SSL can provide these services for all database connections; however, IPSEC can allow these services to be configured on selected computers and ports.
6.	Encryption	R	It is recommended to implement SSL. Use the fully-qualified DNS name of the server in the certificate to help prevent masquerading.	
7.	Test and development servers	R	Maintain test and development servers on a separate network segment from the production servers.	Test patches carefully before applying them to production systems.

#	Config Item	M/R	Action	Description
8.	Dedicated Server	R	It is recommended to install SQL Server on a computer that does not provide additional services, e.g., Web or Mail Services.	Vulnerabilities in other application services could lead to a compromise of the SQL Server.
9.	Install OS according to Windows baseline	M	Configure Windows OS according to Microsoft Best Practise and SCA Security Baseline – Windows Servers	
10.	Disk subsystem	R	Use RAID for critical data files	Raid Level 10 is recommended. Use the level of RAID which will provide the best reliability and performance for your environment.
11.	Separate partitions	M	Create separate partitions for OS/SQL program files, SQL data files, and SQL transaction logs.	Separate partitions provide greater protections via host and file permissions at the volume level as well as allowing greater control over data storage usage and monitoring of the database.
12.	Services	M	Disable the following services on a SQL Server machine if they are not absolutely necessary	The disabling of services has to be balanced with application requirements, since certain applications require the use of certain services to function correctly.
			Alerter	
			Clipbook Server	
			Computer Browser	
			DHCP Client	
			Distributed File System	
			Distributed Transaction Coordinator	
			Fax Service	
			Internet Connection Sharing	
			IPSec policy agent	Unless IPSec policies will be used
			License Logging	
			Logical Disk Manager Administrative Service	
			Messenger	
			NetMeeting Remote Desktop Sharing	
			Network DDE	
			Network DDE DSDM	
			Print Spooler	
			Remote Access Connection Manager	
			Remote Registry	Unless network management software requiring remote registry access will be used
			Removable Storage	
			RunAs Service	
			Smart Card	

#	Config Item	M/R	Action	Description
			Smart Card Helper	
			Task Scheduler	Unless batch jobs scheduled with the SQL Server Agent or scheduled tasks will be used
			Telephony	
			Telnet	
			Windows Installer	
13.	MSSQL Server Service Account	M	Use a low-privileged Local or Domain account for the MSSQLServer service.	The services account should only be a domain account if the SQL Server requires remote communications with other domain systems such as those used for backup over the network. Otherwise, a local user account should be used. See items 15 – 19 for additional information on the service account.
14.	SQLServerAgent Service Account	M	Use a low-privileged domain account for SQLServerAgent if replication, DTS, or other inter-server connection is required.	Replication and other inter-server communications require the SQLServerAgent service account to be a domain account.
15.	Local users group membership	M	Assign the local service account as a member of only the Users group	The “Users” group is a local machine group.
16.	Domain users group membership	M	Make a domain service account a member of only the Domain Users group	
17.	SQL Server service account rights	M	Grant the SQL Server service account(s) the following rights:	These rights are assigned by default.
			Log on as a service	
			Act as part of the operating system	
			Log on as a batch job	
			Replace a process-level token	
			Bypass traverse checking	
			Adjust memory quotas for a process	
			Permission to start SQL Server Active Directory Helper	
			Permission to start SQL Writer	
18.	SQL Server Agent service account rights	M	Grant the SQL Server Agent service account(s) the following rights:	These rights are assigned by default.
			Log on as a service	
			Act as part of the operating system	Only on Windows 2000
			Log on as a batch job	

#	Config Item	M/R	Action	Description
			Replace a process-level token	
			Bypass traverse checking	
			Adjust memory quotas for a process	
			Permission to start SQL Server Active Directory Helper	
			Permission to start SQL Writer	
19.	Integration Service account rights	M	Grant the Integration Service account(s) the following rights:	
			Log on as a service	
			Permission to write to the application event log	
			Bypass traverse checking	
			Create global objects	
			Impersonate a client after authentication	
20.	SQL Server services account rights	M	Deny the service account the "Log on locally" right.	The service accounts do not have a need to log on to the console. This will prevent a brute force attack on the service account.
21.	SQL Server services account rights	M	If a service account is a domain account, configure the account to have the Windows permission "Log on Locally" to the database server only.	This, combined with the recommendation in item 17, 18, 19, will prevent an attempt to logon to any domain computer using the services account.
22.	SQLServer Proxy accounts	M	Create dedicated user accounts specifically for proxies, and only use these proxy user accounts for running job steps.	A SQL Server Agent proxy defines the security context for a job step. A proxy provides SQL Server Agent with access to the security credentials for a Microsoft Windows user. Each proxy can be associated with one or more subsystems. A job step that uses the proxy can access the specified subsystems by using the security context of the Windows user. Before SQL Server Agent runs a job step that uses a proxy, SQL Server Agent impersonates the credentials defined in the proxy, and then runs the job step by using that security context.
23.	SQLServer Proxy accounts	M	Only grant the necessary permissions to proxy user accounts. Grant only those permissions actually required to run the job steps that are assigned to a given proxy account.	

#	Config Item	M/R	Action	Description
24.	SQLServer Proxy accounts	M	Do not run the SQL Server Agent service under a Microsoft Windows account that is a member of the Windows Administrators group.	
	SQL Server Installation and Patches			
25.	Patches and hotfixes	M	Ensure the Current SQL Server service pack and hotfixes are installed.	Check Microsoft's website for the latest service pack/hotfix for SQL Server 2005. Automatic updates are appropriate for non-production databases only. In multiple instance environments, updates must be applied to each SQL Server instance.
26.	SQL Server Ports	R	Change SQL Server default ports from 1433 and 1434.	Using a non-default port helps protect the database from attacks directed to the default port.
27.	Naming conventions	M	In naming SQL Server instances, limit the instance name to less than 16 characters with no reference to a version number or other sensitive information.	Version or other sensitive information in the server name makes it easier for an attacker to develop an attack strategy against the server.
28.	Authentication mode	M	Select Windows authentication mode.	Windows provides a more robust authentication mechanism than SQL Server authentication. If SQL Server authentication is required, configure SQL Server account password and lockout properties with local or domain-based group policies.
29.	Rename sa account	R	The "sa" account should be renamed to something that is not easily identifiable as the "sa" account. ALTER LOGIN sa WITH NAME = <new name>	It is more difficult to script attacks against the "sa" account if the username is not known.
30.	Strong password	M	Use a strong password for the "sa" login account.	A strong password for the "sa" login account is required regardless of which mode is chosen and regardless of whether the "sa" account is disabled.
31.	Sample databases	M	Do not install the sample databases. Delete all sample databases if they already exist.	None of the sample database are installed by default
32.	Initialization parameter	M	C2 Audit Mode– Set to 1 if no custom defined audit trace is enabled	Specifies whether automatic auditing of security events is enabled.

#	Config Item	M/R	Action	Description
33.	Initialization parameter	M	Remote Access– Set to 0 unless replication is being used or the requirement is justified	Allows logons from remote servers.
34.	Recommended periodic administrative procedures	R	Run the Microsoft Baseline Security Analyzer weekly and follow the security recommendations as closely as possible to secure the operating system.	
35.	Recommended periodic administrative procedures	R	Run the SQL Best Practices Analyzer regularly and note any changes to the environment.	
	SQL Server Settings			
36.	SQL Server Configuration Manager	M	Disable the “Named Pipes” network protocol.	If Named Pipes is required, change the name to something other than \\.\pipe\sql\query. Named Pipes protocol is disabled by default for MSSQLSERVER and SQLEXPRESS and enabled for SQL Native Client.
37.	SQL Server Properties	R	The following settings are recommended:	
	Auto Restart SQL Server		Set the SQL Server service start mode to “Automatic□	This is found in the SQL Server Configuration Manager.
	Auto Restart SQL Server Agent		If the SQL Server Agent is required, set the “SQL Server Agent□ start mode to “Automatic□.	This is found in the SQL Server Configuration Manager.
	Distributed Transaction Coordinator		Set the “Distributed Transaction Coordinator□ service start mode to “Disabled□ if this service is not required.	This is found in the SQL Server Configuration Manager.
	Cross database-ownership chaining		Disable the cross_db_ownership_chaining option.	Use sp_dboption to check for databases for which cross-database ownership chaining is enabled. This is found in the General page of SQL Server Properties window. This is disabled by default.
	Advanced Server Settings		Do not enable direct modifications to the system catalogs.	This access level is disabled by default in SQL Server 2005 and cannot be enabled. You must use the documented API’s to access them.
	Backup/Restore from tape timeout		Set the Backup/Restore from tape timeout period to “Try for 5 minutes”	This option is found in the Database Settings page of SQL Server Properties window.

#	Config Item	M/R	Action	Description
	Media Retention		Set the default backup media retention to the minimum number of days needed to retain a full backup of the database. Ideally, this should be as high as your resources permit.	This option is found in the Database Settings page of SQL Server Properties window.
38.	Data Directory	M	The default data directory should be a dedicated data partition	
39.	Data Log Directory	M	The default log directory should be a dedicated partition separate from all programs and data	
40.	Replication	R	Do not enable replication.	Section “Replication” covers security recommendations if replication is required.
41.	Other SQL Server Configuration Options	R	Save a maximum of 14 SQL error logs.	Truncate logs on a regular schedule, weekly, bi-weekly etc. to prevent oversize logs. This option is found under Management-> SQL Server Logs ->Configure Note: The number of retained agent’s error logs cannot be customized as it is hard coded at nine.
42.	Database Mail	M	Disable Database Mail where messaging is not required.	This option is found in the Advanced page of the SQL Server Properties window.
43.	Trace Messages	R	Error Log/Include execution trace messages = off	This is a defence in depth measure to reduce the threat of a disk exhaustion based denial of service. General Page on SQL Server Agent properties.
44.	User-defined stored procedures	R	Ensure that all user-defined stored procedures are stored in encrypted format.	
45.	User-defined extended stored procedures	R	Avoid using user-defined extended stored procedures. If extended functionality is required, use Common Language Runtime (CLR) assemblies instead.	This feature will be removed in a future version of SQL Server
46.	Extended stored procedures	M	Disable access to the following extended stored procedures:	The disabling of access to stored procedures has to be balanced with application requirements, since certain applications require the use of external stored procedures to either export or import data. In the case where stored procedures need to be left on the server, document this information and note as an exception.
			xp_available media	

#	Config Item	M/R	Action	Description
			xp_cmdshell	Disabled by default
			xp_dirtree	
			xp_dsninfo	
			xp_enumdsn	
			xp_enumerrorlogs	
			xp_enumgroups	
			xp_eventlog	
			xp_fixeddrives	
			xp_getfiledetails	
			xp_getnetname	
			xp_logevent	
			xp_loginconfig	
			xp_msver	
			xp_readerrorlog	
			xp_servicecontrol	
			xp_sprintf	
			xp_sscanf	
			xp_subdirs	
47.	SQLmail extended stored procedures	M	Disable access to the following SQLMail extended stored procedures:	SQLMail is replaced by Database mail in MSS2005. It remains for backwards compatibility. Both mail tools are disabled by default.
			xp_deletemail	Disabled by default
			xp_findnextmsg	Disabled by default
			xp_get_mapi_default_profile	Disabled by default
			xp_get_mapi_profiles	Disabled by default
			xp_readmail	Disabled by default
			xp_sendmail	Disabled by default
			xp_startmail	Disabled by default
			xp_stopmail	Disabled by default
48.	WebTask extended stored procedures	M	Disable access to the following WebTask extended stored procedures. Delete the xpweb70.dll file that implements the following Web Task extended stored procedures:	WebTask is disabled by default.
			xp_cleanupwebtask	Disabled by default.
			xp_convertwebtask	Disabled by default.
			xp_dropwebtask	Disabled by default.
			xp_enumcodepages	Disabled by default.
			xp_makewebtask	Disabled by default.
			xp_readwebtask	Disabled by default.
			xp_runwebtask	Disabled by default.
49.	OLE Automation stored procedures	M	Disable access to the following OLE Automation stored procedures:	Disabled by default.
			sp_OACreate	Disabled by default
			sp_OADestroy	Disabled by default

#	Config Item	M/R	Action	Description
			sp_OAGetErrorInfo	Disabled by default
			sp_OAGetProperty	Disabled by default
			sp_OAMethod	Disabled by default
			sp_OASetProperty	Disabled by default
			sp_OAStop	Disabled by default
50.	Registry access extended stored procedures	M	Disable access to the following Registry access extended stored procedures:	
			xp_regaddmultistring	
			xp_regdeletekey	
			xp_regdeletevalue	
			xp_regenumvalues	
			xp_regremovemultistring	
			xp_regwrite	
51.	Advanced Setting	M	SQL Server Event forwarding/Forward events to a different server = off	SQL Server Agent properties page.
	Access Controls			
52.	SQL Server install directory permissions	M	Modify the permissions to the [Drive]:\Program Files\Microsoft SQL Server directory.	Assign the SQL Server service account Full Control. Remove the Users group's permission.
53.	SQL Server database instance directory permissions	M	Delete or secure old setup files. Protect files in the <system drive>:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\Install, e.g., sqlstp.log, sqlsp.log and setup.iss. ".X" represents the installations of various SQL Server installs due to the fact that multiple instances of SQL Server or SQL Express can be installed.	If the current system was upgraded from SQL Server version 2000, check setup.iss in the %Windir% folder and the sqlstp.log in the Windows Temp folder for passwords. Microsoft distributes a free utility called Killpwd, which will locate and remove passwords found in these setup files from your system. This tool does not work with a native SQL 2005 installation. Microsoft is scheduled to release an updated tool, but no release date has been given at this time.
54.	Assigning System Administrators role	M	When assigning database administrators to the System Administrators role, map their Windows accounts to SQL logins, then assign them to the role.	Assign only authorized DBAs to the SQL Server System Administrators role.
55.	SQL Logins	M	Ensure that all SQL Logins have strong passwords according to SCA Password Policy.	Verify that the passwords are not blank and cannot be easily compromised.
56.	OS Guests access	M	Deny database login for the Guests OS group.	Assuming your Guests group was not renamed as part of your OS lockdown: EXEC sp_denylogin 'Computer_Name\Guests'

#	Config Item	M/R	Action	Description
57.	Fixed Server Roles	M	Only use the fixed server roles sysadmin, serveradmin, setupadmin etc, to support DBA activity.	Avoid assigning these roles to application database user accounts, application administrator accounts, application developer accounts or application roles.
58.	SQL Server Database Users and Roles	M	Remove the guest user from all databases except master and tempdb.	
59.	Statement Permissions	M	Grant DDL statement permissions to only the database and schema owner, not individual users.	DBO has all statement permissions for the database by default
60.	Database Owners Permissions	M	Ensure dbo owns all user-created database schemas	Having dbo own all user-created database schemas prevents issues raised when users need to be deleted
61.	Low-privileged users	M	Do not grant object permissions to PUBLIC or GUEST.	Do not grant the REFERENCES object permission to an application user, application administrator, or application role.
62.	Stored Procedure Permissions	M	Grant execute permissions on stored procedures to database roles (not users).	
63.	Using the GRANT option	M	Do not assign the GRANT option of object permission to a user or role.	
64.	SQL Server Agent subsystem privileges	R	Restrict proxy access to required/approved subsystems	Allowing access to CmdExec and ActiveX subsystems allows direct OS access and should be avoided unless business justifications for doing so exist.
65.	User-defined Database Roles	R	Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.	Only if there is a need for user-defined database roles.
66.	Database Roles	M	Avoid nesting database roles.	
67.	Users and Roles	M	Ensure that the members of the roles (users/groups/other roles) in the target database actually exist.	

#	Config Item	M/R	Action	Description
68.	Application Roles	R	Use application roles to limit access to data to users of specific applications. Use encryption to protect the role name and password in the connection string. Use “EXECUTE AS WITH NO REVERT” or “WITH COOKIE” to allow individuals to access the application without knowing the password.	This provides a permission based rather than password based mechanism to sandbox access.
69.	Use of Predefined Roles	M	Avoid assigning predefined roles to PUBLIC or GUEST.	
70.	Linked or Remote Servers	R	Use linked servers rather than remote servers where required. Disable linked servers otherwise	Remote servers are available for backward compatibility purposes only. Applications that must execute stored procedures against remote instances of SQL Server should use linked servers instead.
71.	Linked or Remote Servers	M	Configure linked or remote servers to use Windows authentication where required. Disable linked servers otherwise.	When linking SQL Server databases, the user’s current identity will be used to authenticate the connection.
72.	Linked Server logins	M	Allow linked server access only to those logins that need it. Disable linked servers otherwise.	
	Backup and Disaster Recovery			
73.	Backups – General	M	Use Full database backups combined with differential or transaction log backups to restore the database to a specific point in time.	Database backups should be made to another server or disk that is not physically attached to the same server as the database. This will reduce the risk of total loss in case of disk failure.
74.	System databases	M	It is important to include the system databases in your backup plan i.e. the master, msdb and model databases.	The tempdb database contains no permanent data and does not require backups.

#	Config Item	M/R	Action	Description
75.	Backing up Master database	R	Backup the master database when any of the following events occur: • A database is created or deleted • Login accounts are created, deleted or modified • Server-wide or database settings are modified	
76.	Backing up MSDB database	R	Backup the msdb database when any of the following events occur: • Alerts, jobs, schedules or operators are created, deleted or modified • Backups and restores are performed	
77.	Backup Media	R	Password protect the backup media.	Assign a password to backups to reduce the probability of an incorrect data restore. Note: This password is not intended to prevent unauthorized access to backup data. See http://msdn.microsoft.com/en-us/library/ms186865(SQL.90).aspx for additional details.
78.	Access to Backup Files	M	Restrict access to the backup files to System Administrators.	
79.	Access to Backup Files	M	Restrict restore permissions to DBAs and db_owners.	
	Replication			
80.	SQL Server Agent service account	M	Configure replication agents to use a Windows account rather than a SQL Server Agent account. Grant only the required permissions to each agent.	Use Windows Authentication for all replication agent connections.

#	Config Item	M/R	Action	Description
81.	Replication administration roles	M	Avoid modifying replication administration permissions assigned to the roles by default. Only assign authorized application administrators and DBAs these roles.	The permissions needed to support and administer replication are assigned to sysadmin, db_owner and replmonitor by default.
82.	Snapshot share folder	M	Store the snapshot folder, which houses a snapshot of the replicated changes, on an explicit share and not an administrative share.	
83.	Publication Access List	M	The domain accounts used by the SQL Server Agent service and the Replication proxy account must be entered in the Publication Access List so that all replication agents will be able to participate in the replication process.	
84.	Secure Communications	M	Use secure connections, such as VPN or proxy servers, for all replication over the Internet.	
85.	Database connections	M	Configure the database connections for replication agents to use Windows authenticated logons.	
86.	Filtering	R	Employ replication filters to protect the data.	
87.	Distribution databases	R	All distribution databases and snapshot files must be located in protected and audited locations.	
	Auditing Policy and Procedures			
88.	Auditing – General	M	Prepare a schedule for reviewing audit information regularly according to SCA Common Logging Standard.	
89.	SQL Server Properties – Security Tab	M	Through the SQL Server Management Studio, enable auditing for SQL Server.	At a minimum, enable failed login attempts. Auditing of failed login attempts only is enabled by default.
90.	SQL Server Logs	M	SQL Server audit data must be protected from loss. The SQL Server and SQL Server Agent logs must be backed up before they are overwritten.	Adjust the number of logs to prevent data loss. The default is six.

#	Config Item	M/R	Action	Description
91.	SQL Profiler	M	Use SQL Profiler to generate and manage audit trails.	Ensure sufficient resources to support Profiler activity
92.	Profiler Events	M	Capture the following events using SQL Profiler	A third-party auditing tool may be used in lieu of SQL Profiler.
			Audit Add DB User Event	Occurs when a database user login has been added or removed.
			Audit Add Login to Server Role	Addition or removal of login accounts to/from server roles.
			Audit Add Member to DB Role	Addition and deletion of logins from a database role.
			Audit Add Role Event	Occurs when a database role is added or removed.
			Audit Addlogin Event	Occurs when a login has been added or removed.
			Audit App Role Change Password	Whenever passwords are changed for an application role.
			Audit Backup/Restore	Occurs whenever a backup or restore command is issued.
			Audit Broker Conversation	Reports audit messages related to Service Broker dialog security.
			Audit Broker Login	Reports audit messages related to Service Broker transport security.
			Audit Change Audit	Occurs whenever an audit trace modification is made.
			Audit Change Database Owner	Occurs when you use the ALTER AUTHORIZATION statement to change the owner of a database, and the permissions required to do that are checked.
			Audit DBCC	Occurs whenever a DBCC command is issued
			Audit Database Management	Occurs when a database is created, altered, or dropped.
			Audit Database Object Access	Occurs when database objects, such as schemas, are accessed.
			Audit Database Object GDR	Occurs when a GRANT, REVOKE, or DENY has been issued for database objects, such as assemblies and schemas.
			Audit Database Object Management	Occurs when a CREATE, ALTER, or DROP statement is executed on database objects, such as schemas.
			Audit Database Object Take Ownership	Occurs when a change of owner for objects within database scope occurs.
			Audit Database Operation	Occurs when operations in a database, such as checkpoint or subscribe query notification, occur.
			Audit Database Principal Impersonation	Occurs when an impersonation occurs within the database scope, such as EXECUTE AS <*user*> or SETUSER.

#	Config Item	M/R	Action	Description
			Audit Database Principal Management	Occurs when principals, such as users, are created, altered, or dropped from a database.
			Audit Database Scope GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a statement permission by any user in Microsoft SQL Server for database-only actions such as granting permissions on a database.
			Audit Login Change Password	Occurs whenever a user changes their Microsoft SQL Server login password.
			Audit Login Change Property	Occurs when you use the sp_defaultdb stored procedure, the sp_defaultlanguage stored procedure, or the ALTER LOGIN statement to modify a property of a login.
			Audit Login	Occurs when a user has successfully logged in to SQL Server.
			Audit Login Failed	Indicates that a user tried to log in to Microsoft SQL Server and failed.
			Audit Login GDR Event	Occurs when a Microsoft Windows login right was added or removed.
			Audit Logout	Indicates that a user has logged out of (logged off) Microsoft SQL Server.
			Audit Object Derived Permission Event	Occurs when a CREATE, ALTER, or DROP was issued for an object.
			Audit Schema Object Access	Occurs when an object permission (such as SELECT) is used.
			Audit Schema Object GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a schema object permission by any user in Microsoft SQL Server.
			Audit Schema Object Management	Occurs when server objects are created, altered, or dropped.
			Audit Schema Object Take Ownership	Occurs when the permissions to change the owner of schema object (such as a table, procedure, or function) is checked. This happens when the ALTER AUTHORIZATION statement is used to assign an owner to an object.
			Audit Server Alter Trace	Occurs for all statements that check for the ALTER TRACE permission. Statements that check for ALTER TRACE include those used to create or configure a trace, or to set a filter on a trace.
			Audit Server Object GDR	Occurs whenever a GRANT, REVOKE, or DENY is issued for a server object permission by any user in Microsoft SQL Server.
			Audit Server Object Management	Occurs in the case of CREATE, ALTER, or DROP for server objects.

#	Config Item	M/R	Action	Description
			Audit Server Object Take Ownership	Occurs when the owner is changed for objects in server scope.
			Audit Server Operation	Occurs when Security Audit operations such as altering settings, resources, external access, or authorization are used.
			Audit Server Principal Impersonation	Occurs when there is an impersonation within server scope, such as EXECUTE AS <*login*>.
			Audit Server Principal Management	Occurs when server principals are created, altered, or dropped.
			Audit Server Scope GDR	Occurs when a GRANT, REVOKE, or DENY is issued for permissions in the server scope, such as creating a login.
			Audit Server Starts and Stops	Occurs when the Microsoft SQL Server service state is modified.
			Audit Statement Permission Event	Occurs when a statement permission has been used.

4 Surface Area Configuration Tool

The SQL Server Surface Area Configuration tool is a tool that can be used to protect the SQL Server installation by:

- Disable unnecessary services
- Disable unused network protocols
- Disable unused features of SQL Server components

The following section highlights key issues that must be considered while configuring an SQL Server through the Surface Area Configuration Tool.

#	Config Item	Action	Description
1.	Ad Hoc Remote Queries	Disable Ad Hoc Remote Queries where not required	Disabled by default.
2.	CLR Integration	Disable CLR Integration where not required	Disabled by default.
3.	DAC	Disable the Dedicated Administrator Connection where not required	Disabled by default.
4.	Database Mail	Disable Database Mail where messaging is not required	Disabled by default.
5.	Native XML Web Services	Do not configure XML Web Services endpoints where not required	Disabled by default.
6.	OLE Automation	Disable OLE Automation where not required	Disabled by default.
7.	Service Broker	Do not configure Service Broker endpoints where not required	Disabled by default.
8.	SQL Mail	Do not enable SQL Mail where not required or where Database Mail could be used instead.	Disabled by default.
9.	Web Assistant	Disable Web Assistant where not required	Disabled by default.
10.	xp_cmdshell	Disable the xp_cmdshell stored procedure where not required	Disabled by default.
11.	Ad Hoc Data Mining	Disable ad hoc data mining queries where not required	
12.	Anonymous Connections	Disable anonymous connections to the Analysis Services where not required	
13.	Linked Objects	”Enable links To other instances” should be disabled where not required.	

#	Config Item	Action	Description
14.	Linked Objects	”Enable links From other instances” should be disabled where not required.	
15.	User-Defined Functions	Disable loading of user-defined COM functions where not required	
16.	Scheduled Events and Report Delivery	Disable scheduled events and report delivery where not required	
17.	Web Service and HTTP Access	Disable Web Service and HTTP access where not required	
18.	Windows Integrated Security	Enable Windows integrated security for report data source connections	

5 SQL Server Application Development Best Practises

The following section gives recommendations and best practises when developing applications using MS SQL Server. These recommendations should be considered in all application development to minimise the risk for known attacks against applications using SQL databases.

#		Action	Description
1.	Ownership Chaining	Use ownership chaining within a single database to simplify permissions management.	Avoid using cross database ownership chaining.
2.	Role Assignments	Assign permissions to roles rather than users. The principle of "Least Privilege" applies, thus users should not be given access to roles they do not need for their job function.	Ensure that roles, rather than users own objects to avoid application changes when a user is dropped.
3.	Encrypted connections	Enable encrypted connections between the user and the server.	Consider allowing only encrypted connections. When allowing SQL Server authentication, encrypt either the network layer with IPSec or the session with SSL
4.	Error Handling	Do not propagate errors back to the user.	Log errors or transmit them to the system administrator.
5.	User Input	Prevent SQL injection by validating all user input before transmitting it to the server.	Only permit minimally privileged accounts to send user input to the server. Minimize the risk of SQL injection attack by using parameterized commands and stored procedures.
6.	Developer awareness	Increase awareness of issues such as cross-site scripting, buffer overflows, SQL injection and dangerous APIs.	
7.	Developer awareness	Identify categories of threats that apply to your application, such as denial of service, escalation of privileges, spoofing, data tampering, information disclosure and repudiation.	
8.	Security reviews	Add security reviews to all stages of the application development lifecycle (from design to testing).	
9.	Distributing SQLEXPRESS	If you distribute SQLEXPRESS, install SQLEXPRESS using Windows security mode as the default.	Never install a blank sa password. Use the Microsoft Installer to install SQLEXPRESS.

#		Action	Description
10.	Net-Libraries	If SQLEXPRESS will operate as a local data store, disable any unnecessary client protocols.	Remote access is disabled by default.
11.	Customer awareness	Let your customers know that your product includes SQLEXPRESS so that they can be prepared to install or accept SQLEXPRESS -specific software updates.	
12.	SQL Server Agent	Change the SQL Server Agent Startup Type to “Disabled”.	SQLEXPRESS installs SQL Server Agent by default and the Service startup type is “Manual”.