Default Access Security Checks in Policy Templates

⚠ Click on the Policy Template name to order the table according to Security Checks marked as default.

Access Security Checks	CIS for SQL Server 2000	CIS for SQL Server 2005	CIS for SQL Server 2008	CIS for SQL Server 2008 R2	CIS for SQL Server 2012	CIS for SQL Server 2014	CIS for SQL Server 2016	CIS for SQL Server 2017	CIS for SQL Server 2019	DISA-NIST STIG for SQL Server 2012	DISA-NIST STIG for SQL Server 2014	
Always Encrypted												
Appropriate cryptographic modules have been used to encrypt data.										X		
Assembly host policy				X	X	X	X	X	X			
Backup Encryption (Native)												
Backup Encryption (Non-Native)												
Certificate private keys were never exported												
Contained database authentication type					X	X	X	X	X			
DAC Remote Access		X	X	X	X	X	X	X	X			

Dangerous Extended Stored Procedures (XSPs)	X	X	X								
Database Master Key encrypted by Service Master Key										X	X
Database Master Keys Encrypted by Password										X	
Database roles and members											
Dynamic Data Masking											
Encryption Methods											
Files On Drives Not Using NTFS	X	X	X								
Fixed Roles Assigned To public Or guest	X	X	X								
Guest User Enabled	X	X	X	X	X	X	X	X	X		
Linked server is running as a member of sysadmin group											

NTFS Folder Level Encryption											
Operating System Version											
Public role permissions											
Remote Access	X	X	X	X	X	X	X	X	X		
Required Administrative Accounts Do Not Exist											
Row-Level Security											
Server roles and members											
Signed Objects											
SQL Job permissions											
SQL Jobs and Agent											
SQL Server Browser Running											
SQL Server database level encryption										X	

Startup Stored Procedures	X	X	X	X	X	X	X	X	X	X	
Startup Stored Procedures Enabled	X	X	X	X	X	X	X	X	X	X	
Startup Stored Procedures permissions											
Stored Procedures Encrypted	X	X	X								
Symmetric key				X	X	X	X	X	X		
Symmetric Keys Not Encrypted with a Certificate										X	X
Sysadmins Own Trustworthy Databases										X	X
Transparent Data Encryption											
Unacceptable Database Ownership										X	X
User Defined Extended Stored Procedures (XSPs)	X	X	X								