SQL Server Security Checklist

Area	Security Measure	Description
Authentication	Use Windows Authentication	Prefer Windows Authentication over SQL Server Authentication for better security through integrated login management.
	Disable SQL Server 'sa' account	Disable or rename the default 'sa' account to prevent common brute force attacks.
	Enforce Strong Password Policy	Ensure strong passwords for SQL Server logins with complexity requirements and regular expiration.
Authorization	Follow Principle of Least Privilege	Grant users the minimum required permissions to perform their tasks to reduce risk of unauthorized access.
	Use Role-Based Access Control (RBAC)	Assign permissions using database roles instead of granting permissions directly to users.
	Regularly Review User Permissions	Periodically audit user permissions using `` `sp_helprolemember` `` or `` `sys.database_principals` `` to ensure they are appropriate.
Network Security	Enable Firewall Rules	Restrict SQL Server access by allowing only trusted IP addresses through firewall rules.
	Use Encrypted Connections (TLS)	Force encryption for all connections to SQL Server to protect data in transit.
	Disable SQL Server Browser Service	Turn off the SQL Server Browser service unless absolutely necessary to reduce exposure to network scans.
Auditing and Logging	Enable SQL Server Auditing	Enable SQL Server Audit or Extended Events to log and monitor activities, such as failed login attempts and schema changes.
	Enable Login Auditing	Enable SQL Server login auditing to detect unauthorized login attempts (`` `FAILED_LOGIN_GROUP` ``).
	Monitor Error Logs and Event Logs	Regularly review SQL Server error logs, Windows event logs, and audit logs for suspicious activities.

Data Encryption	Enable Transparent Data Encryption (TDE)	Encrypt sensitive data at rest using TDE to protect the database files and backup files.
	Use Always Encrypted	Use Always Encrypted for column-level encryption to protect highly sensitive data even from DBAs.
	Encrypt Backups	Use backup encryption to secure backup files from being stolen or compromised.
User Management	Remove Unnecessary Logins	Remove unused or unnecessary SQL Server logins to reduce the attack surface.
	Disable Unused Accounts	Disable rather than delete unused accounts, especially if you may need to restore access for auditing or investigations.
	Monitor SQL Server Login Activity	Regularly check for inactive or dormant logins and remove them if not needed.
Patching and Updates	Keep SQL Server Up-to-Date	Apply the latest SQL Server patches and cumulative updates to protect against known vulnerabilities.
	Patch Underlying OS and Hardware	Ensure the operating system and hardware are regularly patched with security updates.
Service Accounts	Use Separate Service Accounts	Run SQL Server services (Engine, Agent, etc.) under minimally privileged, separate accounts for each service.
	Restrict SQL Server Service Account Permissions	Do not grant excessive permissions to SQL Server service accounts (e.g., avoid granting local admin or sysadmin permissions).
	Use Managed Service Accounts (MSA/gMSA)	Use Managed Service Accounts (MSA/gMSA) to manage service accounts with automatic password management.
SQL Server Configuration	Disable Unused Features	Disable features like `` `xp_cmdshell` ``, `` `OLE Automation` ``, `` `SQL Mail` ``, or other unused features that may pose security risks.
	Restrict Access to Extended Stored Procedures	Limit access to dangerous extended stored procedures, such as `` `xp_cmdshell` ``, to avoid misuse.
	Disable Cross-Database Ownership Chaining	Prevent users with permissions in one database from gaining unauthorized access to objects in another.

Backup Security	Secure Backup Files	Store backups in a secure location with restricted access, and encrypt backup files.
	Use Backup Compression and Encryption	Compress and encrypt backups to reduce risk of data leaks.
Physical Security	Restrict Physical Access to SQL Server	Ensure that the physical server hosting SQL Server is located in a secure environment with restricted access.
Monitoring and Alerts	Set Up Alerts for Critical Security Events	Create alerts for events like failed logins, permission changes, or database object changes.
	Monitor SQL Server for Suspicious Activity	Use monitoring tools like Extended Events or third-party security solutions to detect and respond to abnormal behavior.
Compliance	Adhere to Industry Compliance Standards	Ensure SQL Server meets applicable industry standards such as GDPR, HIPAA, PCI DSS, etc., and implement controls accordingly.
	Perform Regular Security Audits	Conduct security audits regularly to ensure the SQL Server environment is in compliance with internal and external policies.

This checklist helps ensure your SQL Server instances are secure by addressing various aspects such as authentication, authorization, encryption, logging, and patching.