DATABASE SECURITY CHECKLIST

S/N	Database Security Checklist	Yes/No	Remarks
Authentication			
1	Implement strong authentication mechanisms		
2	Enforce password policies (complexity, expiration, etc.).		
3	Use multi-factor authentication (MFA) for additional security.		
Authorization and Access Control			
1	Define and enforce access control policies.		
2	Assign roles and permissions based on the principle of least privilege.		
3	Regularly review and update user access levels		
4	How many users have been given system administrator privileges? Do these users require the privilege to execute their job function?		
5	Can database resources be accessed without using database management systems (DBMS) commands and structured query language (SQL) statements?		
6	Are security levels for all users and their roles identified within the database, and are access rights for all users and/or groups of users justified		
7	Is system administrator authority granted to the job scheduler		
8	Are actual passwords embedded into database utility jobs and scripts		
9	How is a trigger created, and when does it fire		
10	Are copies of production data altered or masked to protect sensitive data		
Logical Schema			
1	Do all entities in the entity-relation diagram exist as tables or views?		
2	Are all relations represented through foreign keys?		
3	Are nulls for foreign keys allowed only when they follow the cardinality expressed in the entity relation model?		
4	Are constraints specified clearly?		
Physical Schema			

1	Has allocation of initial and extension space (storage) for tables, logs, indexes and temporary areas been executed based on the requirements?		
2	Are indexes by primary key or keys of frequent access present?		
3	If the database is not normalized, is justification accepted?		
Access time reports			
1	Are indexes used to minimize access time?		
2	Have indexes been constructed correctly?		
3	Are any open searches not based on indexes justified?		
Encryption			
1	Encrypt data at rest using database-level encryption.		
2	Encrypt data in transit using SSL/TLS.		
3	Manage and protect encryption keys securely.		
Database Encryption Key Management			
1	Establish a secure key management system.		
2	Periodically rotate encryption keys.		
3	Monitor and audit key access and usage.		
Data Masking and Redaction			
1	Apply data masking or redaction for sensitive information.		
2	Ensure that only authorized users can access the complete dataset.		
Vulnerability Management			
1	Regularly scan for vulnerabilities in the database.		
2	Develop and implement a patch management process.		
3	Address and remediate identified vulnerabilities promptly		
Database Activity Monitoring:			
1	Implement real-time monitoring of database activities.		
2	Set up alerts for unusual or suspicious behavior.		
3	Respond promptly to alerts and investigate incidents.		
Audit Logging			

1	Enable and configure detailed audit logging.		
2	Regularly review audit logs for suspicious activities.		
3	Ensure logs are stored securely and retained for compliance.		
Backup and Recovery			
1	Establish regular backup schedules.		
2	Store backups securely, and test restoration processes.		
3	Implement a disaster recovery plan.		
Database Patch Management			
1	Regularly update and patch the database management system.		
2	Follow a testing process before applying patches in a production environment.		
User Training and Awareness			
1	Provide security training to database administrators and users.		
2	Promote awareness of security, best practices and potential risks.		
3	Conduct periodic security training sessions.		
Compliance Requirements			
1	Ensure compliance with relevant industry regulations (e.g. ISO 27001, GDPR, HIPAA, PCI DSS).		
2	Periodically review and update security measures to meet evolving compliance standards.		