

**SOLUTION OVERVIEW** Microsoft SQL Server database security guidelines are defined by the following tools and organizations: Center for Internet Security (CIS), Microsoft Best Practices Analyzer (MSBPA) and the Database Security Technical Implementation Guide (STIG). They all provide guidance for ensuring that access to your SQL Server is auditable, secure and consistent. These guidelines offer recommendations to comply with Federal regulations like the Sarbanes-Oxley Act of 2002, specifically Section 404, PCI and COBIT to name a few. These regulations mandate that IT define the right business disciplines and best practices for SQL Server access in order to prevent internal and external intrusions and for enhancing SQL Server confidentiality, data integrity and availability.

In order to define the right baselines, track the changes and report those findings to auditors, you must be able answer the following questions:

1. Who has access to my SQL Server data?
2. What has changed with SQL Server permissions, logins & access?
3. How do I define a secure baseline and maintain it across my SQL Server enterprise?
4. How can I implement repeatable processes to help maintain my standards?
5. What is the best way for me to comply with Federal regulations with regards to my SQL Server databases?

### **How Does SQLsecure Address These Requirements?**

Idera SQLsecure is a security analysis solution that identifies SQL Server security violations and ensures security policies are enforced. You can find out who has access to what and identify each user's effective rights across all SQL Server objects. Furthermore, you can also alert on violations of your corporate policies, and secure your environment (internally and externally) from the most common methods of intrusion.

A key course of action to comply with Federal regulations is developing, maintaining and enforcing internal controls and procedures for your IT environment. SQLsecure is a necessary tool for establishing the right controls to meet those regulations.

SQLsecure helps IT organizations address the requirements of Sarbanes Oxley and COBIT (Control Objectives for Information and related Technologies) where they apply to Microsoft SQL Server. SQLsecure helps you to define your SQL Server baselines by providing three Idera defined templates (**Level-1 Basic, Level-2 Balanced, Level-3 Strong**) which provide "realistic" guidelines for establishing the right security checks for your environment. In addition, it can also extract your permissions, settings from any point in time, and identify any changes or vulnerabilities that may exist. This gives you the power to proactively address these exceptions before reports are delivered to your auditors.

Listed below is a chart that details Sarbanes Oxley section 404 and the COBIT regulation and shows how SQLsecure and SQLcompliance manager address those regulations.

Sarbanes-Oxley	Summary	Idera - SQL secure
- Section 404	A statement of management’s responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and management’s assessment, as of the end of the company’s most recent fiscal year of the effectiveness of the company’s internal control structure and procedures for financial reporting, Section 404 requires the company’s auditor to attest to , and report on management’s assessment of the effectiveness of the company’s internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board. (Source: Securities and Exchange Commission.)	Extracts existing login, access information and provides a score card report identifying potential problems. Provides saved snapshots that report on what the SQL Server access settings are at a particular point in time. Delivers an assessment feature that identifies changes in permissions, logins, configuration, access, surface area and data integrity and also provides reports for the auditors.
- COBIT Objective DS 5.1	<b>Management of IT Security</b> Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements.	Helps IT to define the right levels of protection against database intrusion and ensures that the right security checks are in place. An assessment can be run at any time to provide a detailed view of SQL server settings to ensure that the system setup is in compliance with the standards determined by the IT department or external regulations.
- COBIT Objective DS 5.3	<b>Identity Management</b> “All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.”	All users of SQL Server (internal, external and temporary) can be uniquely identifiable with SQL secure. Should their access/permissions change, an assessment can be run to identify those changes. All assessments are stored in a secure repository for future assessments and reporting. Once changes are approved and implemented, SQLSecure can confirm those changes. Users can be easily identified and their access rights can be enforced.
- COBIT Objective DS 5.4	<b>User Account Management</b> “Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.”	Provides a means to confirm that employees who are granted/revoked access rights are confirmed and documented. Employees who are no longer with the organizations are easily identified. All access rights for all users are identified ,documented and stored in the SQLsecure repository. The user can run reports on a periodic basis to confirm the permissions of all accounts and related privileges.
- COBIT Objective DS 5.5	<b>Security Testing, Surveillance and Monitoring</b> “Ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.”	Helps you to define the right security settings to your SQL server with our Idera defined security checks. It also provides you with snapshot and assessment features to identify any abnormalities. In addition, our SQLcompliance manager solution can detect any changes in data and objects in real-time. Abnormalities like failed logins for any selected database can be detected.
- COBIT Objective DS 5.7	<b>Protection of Security Technology</b> “Ensure that important security-related technology is made resistant to tampering and security documentation is not disclosed unnecessarily, i.e., it keeps a low profile. However, do not make security of systems reliant on secrecy of security specifications.”	Access to the repository is controlled by strict “segregation-of-duties” to administer user access. Secure also helps to expose any security holes that may exist on your server.