



# SECURITY and COMPLIANCE SOLUTIONS for SARBANES OXLEY and COBIT®

## 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 **Sarbanes-Oxley**, specifically **Section 404**, and (**Control Objectives for Information and Related Technology**) **COBIT®** framework. These regulations mandate that IT define the right business disciplines and good 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 SQL secure address these requirements?

Idera SQL secure 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. SQL secure is a necessary tool for establishing the right controls to meet those regulations.

SQL secure helps IT organizations address the requirements of Sarbanes Oxley and COBIT® where they apply to Microsoft SQL Server. SQL secure 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 permission settings from any point in time, and identify any changes or vulnerabilities that may exist. This gives you the power to proactively address those exceptions before reports are delivered to your auditors.

### **Confidential and Proprietary**

Idera, SQLsecure, SQL compliance manager are trademarks of BBS Technologies Inc. All other product and company names herein may be trademarks of their respective owners.



## How does SQL compliance manager address these requirements?

SQL compliance manager is a comprehensive SQL Server auditing solution that uses policy-based algorithms to track changes to your SQL Server objects and data. SQL compliance manager answers the questions pertaining to "who" did "what", "when", "where" and "how" to your SQL Server. Furthermore, SQL compliance manager delivers real-time monitoring and auditing of all data access, "before and after" updates, schema modifications and permission changes.

SQL compliance manager provides alerts to inform you about who has accessed your data and delivers the "reports" that auditors demand! With SQL compliance manager you can comply with the Sarbanes-Oxley-Section 404 regulation and the COBIT 4.1 objectives.

Listed below is a chart that details Sarbanes Oxley section 404 and the COBIT® 4.1 framework objectives and shows how SQL secure and SQL compliance manager help you to comply.

Sarbanes-Oxley	Summary	Idera - Solutions
<p><b>Section 404</b></p>	<p>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.)</p>	<p><b>SQL secure</b> 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. <b>SQL compliance manager</b> provides a means to track all access to SQL Server data and objects which make it a key component for establishing the right internal controls and procedures that auditors demand</p>

### Confidential and Proprietary

Idera, SQLsecure, SQL compliance manager are trademarks of BBS Technologies Inc. All other product and company names herein may be trademarks of their respective owners.

COBIT Objective	Summary	Idera - Solutions
<p><b>COBIT Objective Deliver &amp; Support 5.1</b></p>	<p><b>Management of IT Security</b></p> <p>Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements.</p>	<p><b>SQL secure</b> 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.</p>
<p><b>COBIT Objective Deliver &amp; Support Identity Management 5.3</b></p>	<p><b>Identity Management</b></p> <p>Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.</p>	<p>All users of SQL Server (internal, external and temporary) can be uniquely identifiable with <b>SQL secure</b>. Should their access or 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, <b>SQL secure</b> can confirm those changes. Users can be easily identified and their access rights can be enforced. Furthermore <b>SQL compliance</b> manager audits all user activity to the SQL Server data and objects</p>

**Confidential and Proprietary**

COBIT Objective	Summary	Idera - Solutions
<p><b>COBIT Objective Deliver &amp; Support User Account Management 5.4</b></p>	<p><b>User Account Management</b></p> <p>Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.</p>	<p><b>SQL secure</b> Provides a means to confirm that employees who are granted or revoked access rights are validated 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 <b>SQL secure</b> repository. The user can run reports on a periodic basis to confirm the permissions of all accounts and related privileges.</p>
<p><b>COBIT Objective Deliver &amp; Support Security Testing, Surveillance and Monitoring 5.5</b></p>	<p><b>Security Testing, Surveillance and Monitoring</b></p> <p>“Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.</p>	<p><b>SQL secure</b> 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 <b>SQL compliance manager</b> can detect any changes in data and objects in real-time. Abnormalities like failed logins for any selected database can be detected.</p>
<p><b>COBIT Objective Deliver &amp; Support Protection of Security Technology 5.7</b></p>	<p><b>Protection of Security Technology</b></p> <p>Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.</p>	<p>Access to the repository is controlled by strict "segregation-of-duties" to administer user access. <b>SQL secure</b> also helps to expose any security holes that may exist on your server. <b>SQL compliance manager</b> also provides a tamperproof repository that can additionally send an alert if it is tampered with by an unauthorized user</p>

**Confidential and Proprietary**



## Solution Summary

Complying with the Sarbanes Oxley section 404 regulation is no easy task. The same holds true for IT organizations that leverage the good practices of COBIT® 4.1 framework. The bottom line is that you must establish the right baselines for SQL Server permissions and be able to identify the changes. You must also be able to track changes to SQL Server, alert on any anomalies and deliver reports to the auditors. The combination of SQL secure and SQL compliance manager provides immutable proof to auditors that SQL Server permissions are established and monitored for change, as well as changes to data and database objects. Idera's compliance solutions deliver the comprehensive reporting that IT auditors require. Idera's compliance solutions help you to solidify and protect your SQL Server environment from intrusions and failed audits which are costly and have an adverse effect on your business. You must develop, maintain and enforce the internal controls and procedures for a more secure SQL Server environment. Show compliance; protect your data and most of all "Prove it"!

## In the News- Failure to Comply, Protect, Audit

Sony - [Hack of Playstation Network Threatens Personal Data of 77million Users](#)

Federal Government - [Continuous Monitoring Still a Long Way Off for the Feds](#)

Verizon - [Breach Report Shows Database Security Not Just About Credit Cards Anymore](#)

State of Texas - [Big Texas Breach a Hard Lesson in Database Discovery](#)

### **Confidential and Proprietary**

Idera, SQLsecure, SQL compliance manager are trademarks of BBS Technologies Inc. All other product and company names herein may be trademarks of their respective owners.