

SECURITY AND
COMPLIANCE
SOLUTIONS FOR
SARBANES
OXLEY AND COBIT®

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 (SOX) Section 404 as well as industry best practices such as the 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 database access in order to prevent internal and external intrusions and for enhancing database confidentiality, data integrity and availability.

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

- 1. Who has access to my SQL Server systems and data?**
- 2. How do I define a secure baseline and maintain it across my SQL Server environment?**
- 3. What has changed with SQL Server permissions, logins & access?**
- 4. How can I implement repeatable processes to help maintain the security standards?**
- 5. What is the best way for me to ensure not only ongoing compliance with federal regulations and standards but also help maintain reasonable security across my SQL Server databases?**

HOW DOES SQL SECURE ADDRESS THESE REQUIREMENTS?

A key course of action to comply with federal regulations is developing, maintaining and enforcing internal controls and procedures for your IT environment. IDERA SQL Secure is a necessary tool for establishing the right controls to meet those regulations. SQL Secure is a security analysis solution that identifies SQL Server security access 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.

SQL Secure helps IT organizations address the requirements of SOX 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.

HOW DOES SQL COMPLIANCE MANAGER ADDRESS THESE REQUIREMENTS?

SQL Compliance Manager is a comprehensive Microsoft 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" across your SQL Server environment. 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 objectives.

On the next page is a chart that details Sarbanes Oxley Section 404 objectives and shows how SQL Secure and SQL Compliance Manager help you to comply.

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.)

SQL Secure extracts existing login and access information, and provides a score card report identifying potential problems. The tool provides saved snapshots that report on what the SQL Server access settings are at a particular point in time. It also elivers an assessment feature that identifies changes in permissions, logins, configuration, access, surface area and data integrity and also provides reports for the auditors. SQL Compliance Manager 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.

For the process-based COBIT framework, IDERA solutions can help in the following areas to ensure that all intrinsic quality, contextual quality, and accessibility/security enabler goals are met:

- SQL Secure 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. All users of SQL Server (internal, external and temporary) can be uniquely identifiable with SQL Secure. 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, SQL Secure can confirm those changes. Users can be easily identified and their access rights can be enforced. Furthermore, SQL Compliance Manager monitors and audits all user activity to the SQL Server data and objects.
- SQL Secure 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 SQL Secure repository. The user can run reports on a periodic basis to confirm the permissions of all accounts and related privileges. SQL Secure helps you to define the right security settings to your SQL Server with IDERA-defined security checks. It also provides you with snapshot and assessment features to identify any abnormalities. In addition, SQL Compliance Manager can detect any changes in data and objects in real time. Abnormalities like failed logins for any selected database can be detected.
- Access to the SQL Secure repository is controlled by strict "segregation-of-duties" to administer user access. SQL Secure also helps to expose any security holes that may exist on your server. SQL Compliance Manager also provides a tamper-proof repository that can additionally send an alert if it is tampered with by an unauthorized user.

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 the COBIT framework. The bottom line is that you must establish the right baselines for Microsoft 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, as well as changes to data and database objects. IDERA's compliance solutions deliver the comprehensive reporting that auditors and regulators 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. Demonstrate compliance, protect your data, and most of all, prove it!

IDERA understands that IT doesn't run on the network – it runs on the data and databases that power your business. That's why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

I D E R A