

The PCI DSS (Payment Card Industry Data Security Standard v1.2.1) is a set of comprehensive requirements developed by the PCI Security Standards Council which includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to help standardize the broad adoption of consistent data security measures on a global basis. In addition, it also includes requirements for security management, policies, procedures, network architecture, software design and other safeguard measures. This standard is intended to help organizations to proactively secure customer data.

PCI data that resides on Microsoft SQL Server must adhere to these regulations. Database Administrators must ensure that payment account data is properly secured. 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 enhance SQL Server confidentiality, data integrity and availability.

In order to define the right baselines, audit database object/data changes and report those findings to auditors, you must be able answer the following questions:

1. Who has access to my "Payment Card" 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. How do I audit permission, object and data changes on my SQL Server?
6. 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 helps IT organizations identify SQL Server security violations and ensures that 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 PCI 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 appropriate security checks for your environment. In addition, it can also extract your permissions and 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.

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 provides continuous auditing of all SQL Server activity by identifying who did what, when, how and whether the event is initiated by privileged users or hackers. SQL compliance manager goes beyond traditional auditing approaches by providing custom real-time monitoring and auditing of all data access, updates, schema modifications and permission changes. Audited data is collected and securely stored for forensic analysis and reporting. It also provides tamper-proof data security features as well as methods for watching events without exposing account information. Additionally, SQL compliance manager provides a robust alerting engine that contains counters and trend graphs to identify activity level deviations often associated with suspect activities.

PCI DSS	Summary	Idera - Compliance
- Section 2	Do not use vendor supplied defaults for system passwords and other security parameters- Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.	SQLsecure provides 3 Idera defined templates that exceed the guidelines from SRR, CIS and Microsoft's Best Practices Analyzer(MSBPA). Vendor supplied defaults are identified as key items to change in order to reduce areas where a hacker can infiltrate payment card data.
- Section 2.1	Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	SQLsecure provides security checks that ensure that vendor supplied defaults are not used in the SQL Server environment. If they are used, an assessment can be run to quickly identify and report any exceptions.
- Section 2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	SQLsecure provides built-in policies that check your database server settings against best practice guidelines established by NIST(SRR) , CIS and MSBPA.
- Section 7.1, 7.2	Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	SQLsecure analyzes granted and inherited rights on tables containing cardholder data so you can instantly verify that access is limited to only those who should have it.
- Section 8	Assign a unique ID to each person with access ensures that actions taken on critical data and systems are performed by and can be traced to, known and authorized users.	SQLsecure shows all users, including "de-nesting " of groups both locally and within Active Directory, to help identify users that should not have certain accesses, but in fact do.
- Section 8.1,8.5.8	Identify all users with a unique user name before allowing them to access system components or card holder data. Do not use group, shared, or generic accounts and passwords.	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.
- Section 8.5.4	Immediately revoke access for any terminated users.	SQLsecure provides "snapshot" capabilities for a given point in time for all user accesses and permissions. Once a user is terminated an assessment report can be run to confirm and document that the user's access has been revoked.
- Section 10	Track and monitor all access to network resources and cardholder data- Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.	SQL compliance manager audits all user activity to PCI data. If there is an exception, you can easily track and report on the events that caused it and accelerate Mean-Time-To-Repair. All compliance alerting can be placed in the application event log.
- Section 10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	SQL compliance manager provides continuous auditing of all SQL Server activity, identifying who did what, when and how.
- Section 10.2	Implement automated audit trails for all system components to reconstruct the following events: <ul style="list-style-type: none"> - 10.2.1 - All individual user accesses to cardholder data - 10.2.2 - All actions taken by any individual with root or administrative privileges - 10.2.3 - Access to all audit trails - 10.2.4 - Invalid logical access attempts - 10.2.5 - Use of identification and authentication mechanisms - 10.2.6 - Initialization of audit logs - 10.2.7 - Creation and deletions of system-level objects 	SQL compliance manager audits all of the events required by section 10.2 and also provides detailed reports for internal and external auditors.

PCI DSS	Summary	Idera - Compliance
<ul style="list-style-type: none"> - Section 10.3 	<p>Record at least the following audit trail entries for all system components for each event:</p> <ul style="list-style-type: none"> - 10.3.1 - User identification - 10.3.2 - Type of event - 10.3.3 - Date and time - 10.3.4 - Success or failure indication - 10.3.5 - Origination of event - 10.3.6 - Identity or name of affected data, system component or resource 	<p>SQL compliance manager audits all of the events required by section 10.3 and also provides detailed reports for internal and external auditors.</p>
<ul style="list-style-type: none"> - Section 10.5 	<p>Secure audit trails so they cannot be altered.</p>	<p>SQL compliance manager provides an immutable audit trail of all SQL Server activity, including administrator activities. Any changes to the audit logs can be detected, and alerts can be configured to notify the appropriate personnel.</p>
<ul style="list-style-type: none"> - Section 10.7 	<p>Retain audit trail history for at least one year, with a minimum of three months online availability.</p>	<p>SQLsecure and SQL compliance manager store all audit data in a central repository which makes it easy to archive data for any length of time.</p>
<ul style="list-style-type: none"> - Section 12.2 	<p>Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).</p>	<p>SQLsecure and SQL compliance manager are used to standardize daily security procedures for auditing changes to SQL Server data and objects and also helping to define user permissions, accesses and maintaining them.</p>