

Understanding the basics of SQL Compliance Manager

By Elan Kol

INTRODUCTION

SQL Compliance Manager is a robust auditing and reporting tool for Microsoft SQL Server.

Most of the customers of SQL Compliance Manager use it to help them meet strict auditing and reporting guidelines from regulations such as CIS, DISA STIG, FERPA, GDPR, HIPAA, NERC, PCI DSS, and SOX.

Customers also find a lot of value in reviewing the activities that have occurred on their systems and ensuring that the activity coincides with their change management process.

Customers can use SQL Compliance Manager to review information forensically to paint a picture of user activity over a specified period. This is very useful when trying to identify what information users accessed with a data breach or disgruntled employee activity.

WHY IS SQL COMPLIANCE MANAGER SO IMPORTANT?

There have been almost 15 billion records breached since 2013. As companies collect more and more data, the number of breached records will continue to rise. Estimates show that the average cost of a data breach is \$3.8 million per breach. SQL Compliance Manager helps you audit your databases to see when information is being accessed. It also allows you to identify how many records a breach affected.

In addition, there are multiple regulations that are mandating how you should audit who is accessing your data. SQL Compliance Manager audits your databases in greater detail than any other tool on the market to meet these regulation guidelines.

WHICH REGULATORY GUIDELINES DOES SQL COMPLIANCE MANAGER SUPPORT

SQL Compliance Manager allows you to audit all the information that you may need to capture for any regulation that requires you to audit database activity. SQL Compliance Manager receives updates to incorporate changes in auditing standards across a variety of regulations.

SQL Compliance Manager can meet the audit and reporting needs of most regulatory guidelines. We have incorporated a regulation guideline wizard that provides a good template meeting the needs of these regulations:

- Center for Internet Security (CIS)
- Defense Information Security Agency (DISA STIG)
- Family Educational Rights and Privacy Act (FERPA)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC)
- Payment Card Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

SQL Compliance Manager also supports custom regulation templates that allow you to apply the regulatory standards defined by your organization.

As each organization is different, meet with your legal counsel and data protection officers to define the needs of your organization and how it plans to meet the challenges of database audit and reporting. Then adjust SQL Compliance Manager to meet those needs.

WHAT DOES SQL COMPLIANCE MANAGER AUDIT?

SQL Compliance Manager audits a variety of elements at the server level and the database level. For each setting you should decide if you want to track that information across all databases, for only specific users, for only specific databases, or for only specific users on specific databases.

Trusted users versus privileged users

Trusted users are users where you have decided that collecting their activity is just noise. This refers to your service accounts or other accounts that already have security safeguards in place. Identifying a user, domain group or service group as a trusted user turns off all auditing activity for that entity.

Privileged users are users who have an elevated level of access to your system. This includes your database administrators, system administrators, and developers. They are your human users and not your systems. Identifying a user, domain group or service group as a privileged user allows you to further refine the activity that you want to track for this entity.

The screenshot shows the 'Audited Database Properties' dialog box with the 'Privileged User Auditing' tab selected. The 'Privileged users and roles to be audited:' list contains 'sa' and 'WIN-S34NVR7D795\Administrator'. The 'Audited Activity' section has 'Audit selected activities done by privileged users' selected. The following activities are checked: Logins, Logouts, Failed logins, Security changes, Administrative Actions, Database Definition (DDL), Database Modification (DML), and Filter events based on access check: Passed. The following activities are unchecked: Database SELECT operations and User Defined Events. A note at the bottom states: 'Note: Selected items that are disabled have been enabled at the server level. Deselected items that are disabled are waiting for other settings to be applied before you can use them.' There is a link for 'Learn how to optimize performance with audit settings.' and 'OK' and 'Cancel' buttons at the bottom.

Audited Database Properties

Before-After Data | Sensitive Columns | Trusted Users | **Privileged User Auditing**

Privileged users and roles to be audited:

- sa
- WIN-S34NVR7D795\Administrator

Buttons: Add..., Remove

Audited Activity

Audit all activities done by privileged users

Audit selected activities done by privileged users

<input checked="" type="checkbox"/> Logins	<input checked="" type="checkbox"/> Security changes	<input checked="" type="checkbox"/> Database Modification (DML)
<input checked="" type="checkbox"/> Logouts	<input checked="" type="checkbox"/> Administrative Actions	<input type="checkbox"/> Database SELECT operations
<input checked="" type="checkbox"/> Failed logins	<input checked="" type="checkbox"/> Database Definition (DDL)	<input type="checkbox"/> User Defined Events

Filter events based on access check: Passed Failed

Capture SQL statements for DML and SELECT activities.

Capture Transaction Status for DML Activity

Capture SQL statements for DDL and Security Changes.

Note: Selected items that are disabled have been enabled at the server level. Deselected items that are disabled are waiting for other settings to be applied before you can use them.

[Learn how to optimize performance with audit settings.](#)

Buttons: OK, Cancel

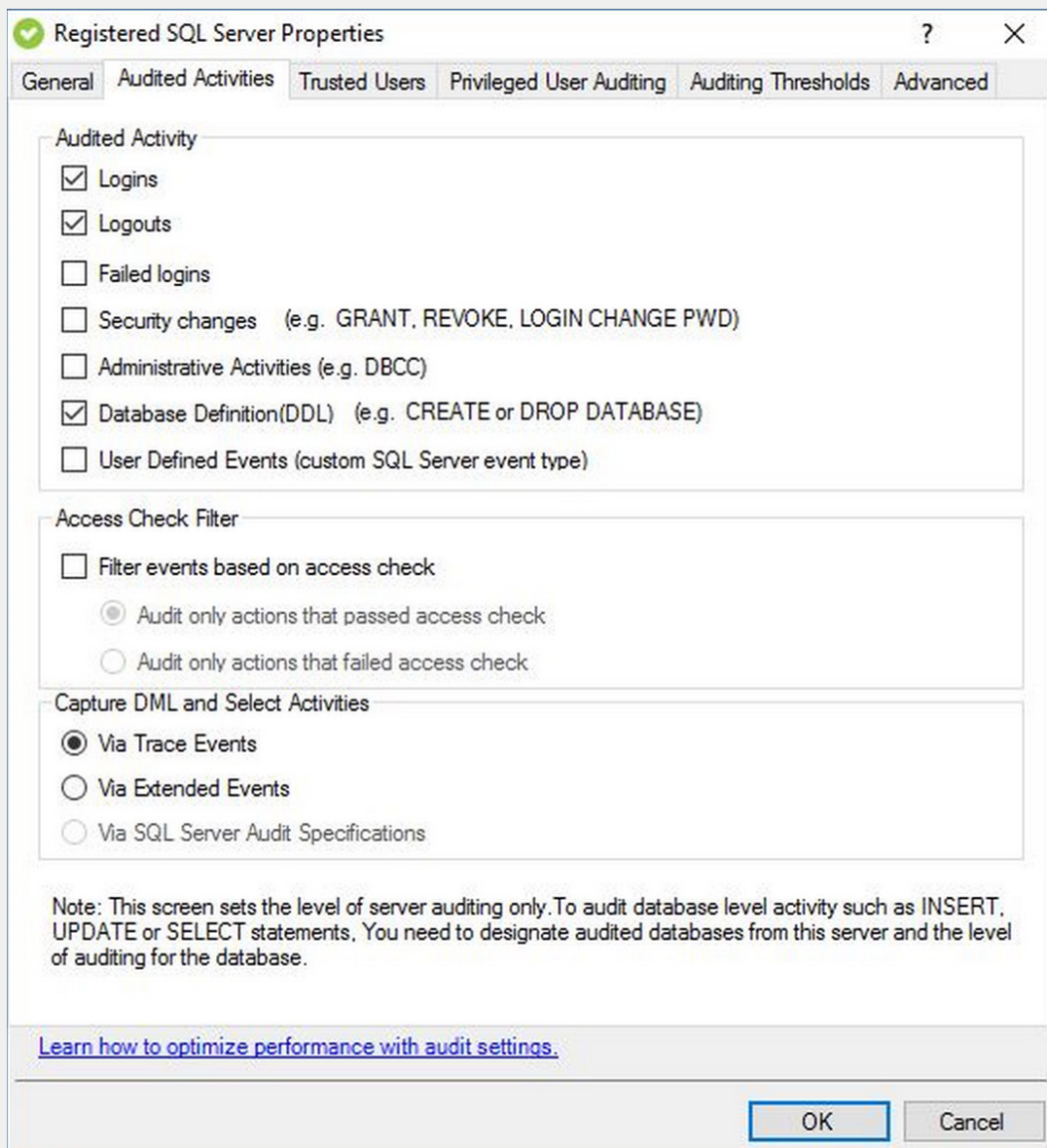
Logins, logouts, and failed logins

SQL Compliance Manager captures login, logout, and failed login events to gain insight into who accesses or tries to access your systems.

Logins and logouts

Capturing login and logout events is a great way to identify who has been accessing your system and when they had access to it.

The login and logout events may not always be a one-to-one relationship with your SQL Server logins, depending on how you define your settings and applications. For example, if you are tracking these events at the server or database level, then you may capture a great abundance of activity from an application that logs in and out of the server for every transaction. For this reason, we suggest you may only want to capture logins and logouts for specified privileged users at the server level.



Failed logins

Failed logins could be a powerful indicator that someone is trying to access data they should not. SQL Compliance Manager allows you to audit all of your failed login attempts and take action if you see an abnormal amount of activity.

Security changes

Security changes may be one of the major reasons you want to audit your database administrators. This setting allows you to track who has been adding new accounts and who has been adding, updating, and revoking privileges.

Database activities

SQL Compliance Manager capture database activities including DDL, DML, SELECT operations, sensitive columns, and before-after data.

Database definition language language (DDL)

SQL Compliance Manager allows you to capture information about your changing schema. It can track when you create a new index, a new database, or a new table. You can choose whether you want to capture the actual SQL statements associated with these changes or not.

Database modification language (DML)

SQL Compliance Manager allows you to capture information about modifications that occur on your database. It can track inserts, updates, and deletes. You can choose whether you want to capture the actual SQL statements associated with the changes or not. You can also choose whether you want to track the transaction activity including begin, rollback, and commit.

While you can set this value at the database level, because this setting can create a lot of volume, we recommend setting it at the privileged user level. You can also further refine the data that is captured by only enabling specified tables.

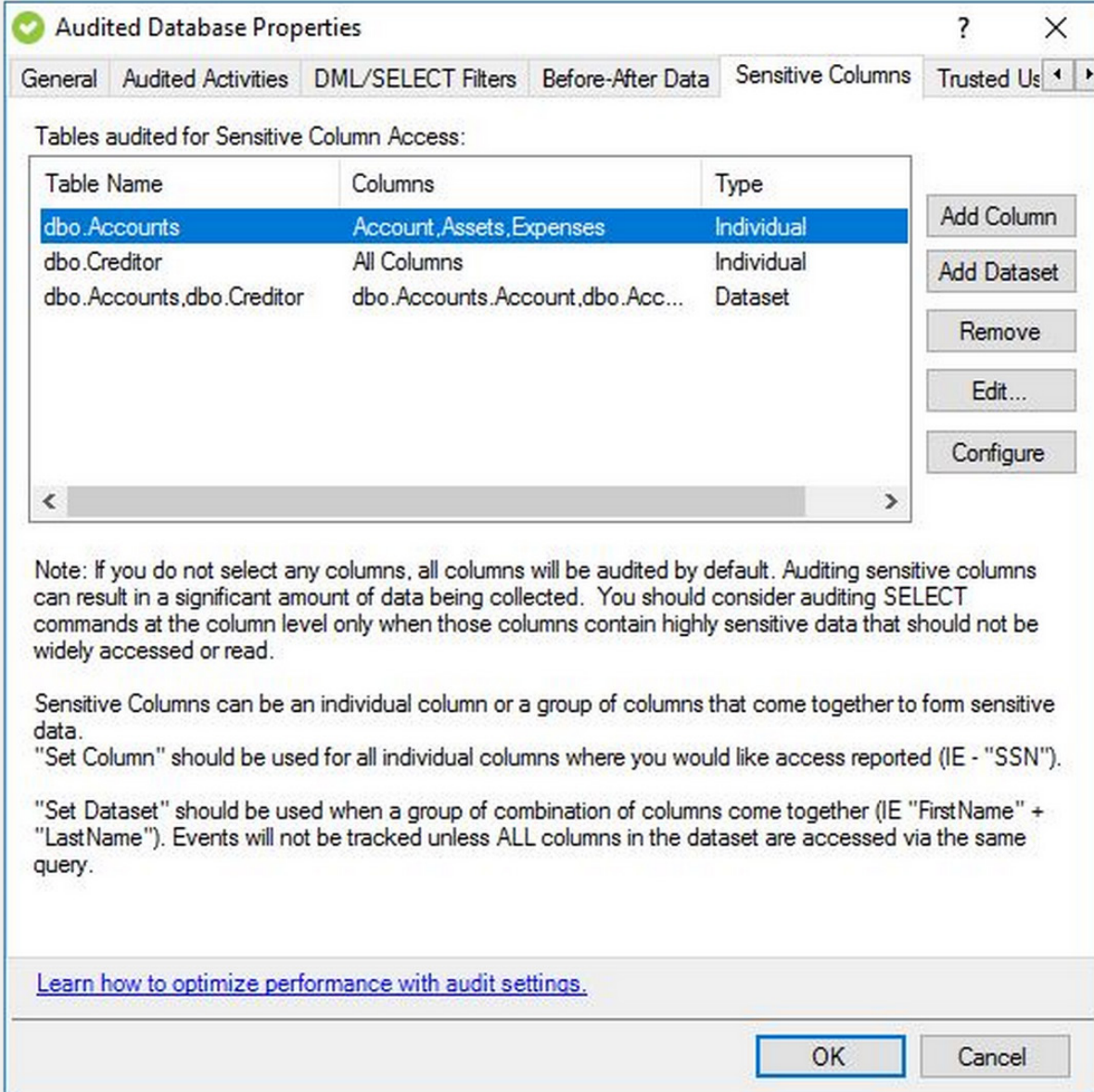
Database SELECT operations

SQL Compliance Manager allows you to capture SELECT operations. Because of the volume that this might create, we recommend you set it at the privileged user level.

Sensitive columns and before-after data

Many regulations require you to audit how users are interacting with personally identifiable information (PII). SQL Compliance Manager allows you to track this information via its sensitive column and before-after data (BAD) activity functionality.

The sensitive columns functionality allows you to capture audit information every time there is a select that is registered on the specified table or column. BAD allows you to capture audit information every time there is a modification (that is, insert, update, or delete) registered on the specified table or column. Detection can happen at the table level, the column level, or for a combination of tables and columns.



The screenshot shows the 'Audited Database Properties' dialog box with the 'Sensitive Columns' tab selected. The 'Tables audited for Sensitive Column Access' section contains a table with three rows. The first row is selected and highlighted in blue. To the right of the table are five buttons: 'Add Column', 'Add Dataset', 'Remove', 'Edit...', and 'Configure'. Below the table is a horizontal scrollbar. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Table Name	Columns	Type
dbo.Accounts	Account,Assets,Expenses	Individual
dbo.Creditor	All Columns	Individual
dbo.Accounts,dbo.Creditor	dbo.Accounts.Account,dbo.Acc...	Dataset

Note: If you do not select any columns, all columns will be audited by default. Auditing sensitive columns can result in a significant amount of data being collected. You should consider auditing SELECT commands at the column level only when those columns contain highly sensitive data that should not be widely accessed or read.

Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data.
"Set Column" should be used for all individual columns where you would like access reported (IE - "SSN").
"Set Dataset" should be used when a group of combination of columns come together (IE "FirstName" + "LastName"). Events will not be tracked unless ALL columns in the dataset are accessed via the same query.

[Learn how to optimize performance with audit settings.](#)

Administrative actions

Administrative actions are maintenance activities, such as backing up a database. For auditing reasons, most auditors do not care to capture this information. If you need to confirm that maintenance has taken place or you have had some abnormal behavior reported, then capturing and reviewing administrative actions can be very helpful in troubleshooting that activity.

User defined events

SQL Compliance Manager can also track events that are created by users using Transact-SQL (T-SQL) code.

IDERA's default configuration settings

When you are first implementing SQL Compliance Manager, the amount of data that you collect can overwhelm you if you decide you want to track that information for all your servers and databases. We encourage you to adjust settings to accommodate the needs of your organization. As a starting point, IDERA recommends you start with these default settings:

Server level:

- Failed logins

Server level - privileged users:

- Logins
- Security changes
- Database definition language (DDL)

Database level (on the databases you want to monitor):

- Security changes
- Database modification language (DML)

Database level - privileged users:

- Database SELECT operations

You can find additional information on SQL Compliance Manager settings at "<https://www.idera.com/resourcecentral/videos/sql-compliance-manager-audit-settings>".

WHAT INFORMATION CAN I REPORT ON?

Out of the box, SQL Compliance Manager allows you to report on:

- Agent activity
- Alert details
- Application activities
- Audit updates
- Backup activity
- BAD and sensitive column activity
- Configuration settings
- Host activity
- Integrity checks
- Login and permissions history
- Regulatory configuration settings
- Rowcount activity
- Schema changes
- User activity

Any information that you capture with SQL Compliance Manager, you can also send out to an SQL Server Reporting Services (SSRS) report.

WHAT DO I DO WITH MY DATA AFTER AN AUDIT?

If the data you have collected has grown too large, SQL Compliance Manager allows you to groom off data that you no longer find necessary. It also can archive off information into a separate repository.

WHAT VERSIONS OF SQL SERVER DOES SQL COMPLIANCE MANAGER SUPPORT?

As of SQL Compliance Manager version 5.8, it supports:

- SQL Server 2005 (SQL Compliance Manager's agent only)
- SQL Server 2008 (SP1 and R2)
- SQL Server 2012 (SP1)
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

SQL Compliance Manager also supports clustered server configurations and availability groups.

For cloud implementations, SQL Compliance Manager supports the above SQL Servers on cloud virtual machines such as Azure Virtual Machine (VM) and Amazon Elastic Compute Cloud (EC2). We plan to add support for Azure SQL Database and Amazon Relational Database Service (RDS) with an upcoming release.

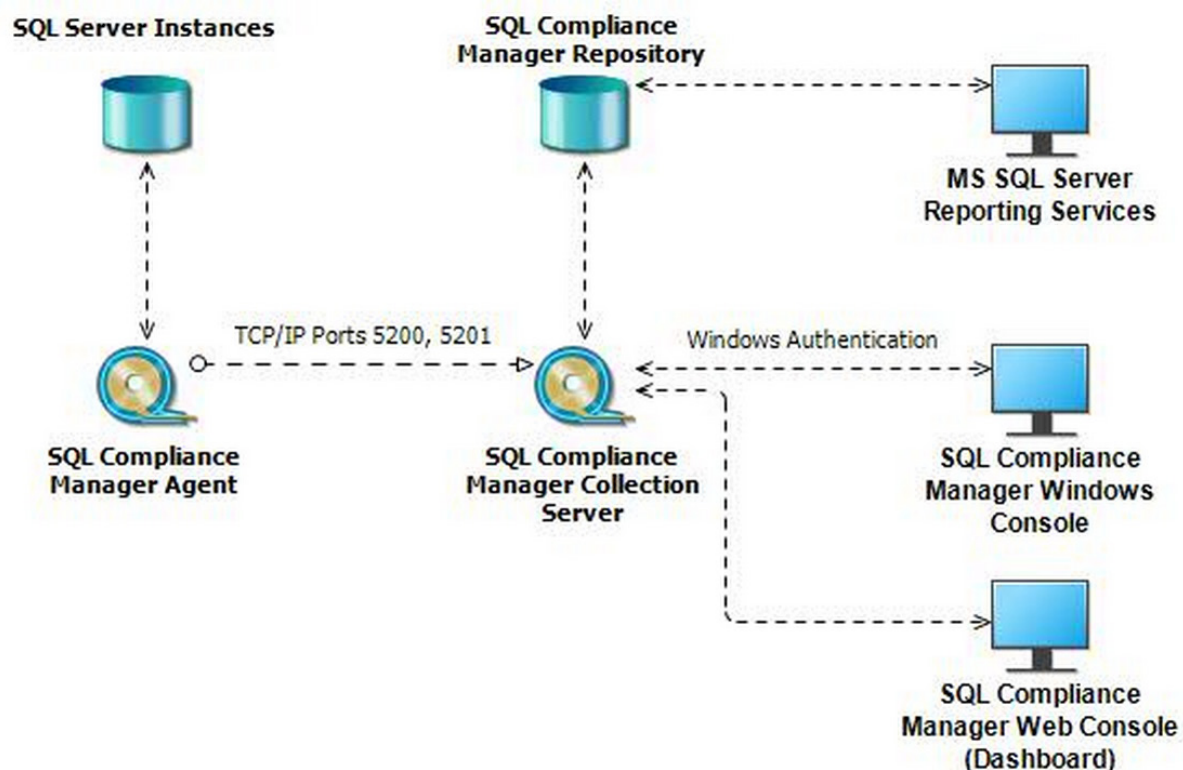


WHAT IS THE SYSTEM INFRASTRUCTURE FOR SQL COMPLIANCE MANAGER

SQL Compliance Manager does not consume a large footprint on your infrastructure. It's easy to install. The lightweight data collection agent minimizes the server impact.

These are the major aspects of SQL Compliance Manager:

- SQL Compliance Manager's console (Windows desktop and web-based via IDERA's Dashboard) allows you to adjust settings and view the data that was collected.
- SQL Compliance Manager's repository stores the data that is used by SQL Compliance Manager.
- SQL Compliance Manager's agent sits on audited servers and collects trace files it sends over to the collection service
- SQL Compliance Manager's collection service takes in the information from the agent and then converts it into audited data you can review via the console.
- IDERA Dashboard's repository stores information for the web console. This does not apply when you did not install the web console via IDERA Dashboard.



WHAT ARE SOME ADDITIONAL RESOURCES?

For additional information about SQL Compliance Manager, you can access the following resources:

Download product installation files

Existing customers can access the latest version of IDERA's products via IDERA's customer portal at "<https://idera.secure.force.com/>".

New customers can download a trial version of SQL Compliance Manager at "<https://www.idera.com/productsolutions/sqlserver/sqlcompliancemanager#getStartedForm>".

Attend product demonstration

New users can request a personalized product demonstration at "<https://www.idera.com/productsolutions/sqlserver/sqlcompliancemanager/RequestADemo>".

New users can also register for a regularly schedule live demonstration on IDERA's events web page at "<https://www.idera.com/events>".

Product documentation

The product documentation is available via the documentation wiki at "<http://wiki.idera.com/display/SQLCM/>".

The release notes for SQL Compliance Manager are available at "<http://wiki.idera.com/display/SQLCM/SQL+Compliance+Manager+Release+Notes>".

The list of known issues for SQL Compliance Manager is available at "<http://wiki.idera.com/display/SQLCM/Known+issues>".

User community

The user community forum for SQL Compliance Manager is available at "<https://community.idera.com/database-tools/database-management/security--compliance>".

General information

The product page for SQL Compliance Manager is available at [“https://www.idera.com/productsolutions/sqlserver/sqlcompliancemanager”](https://www.idera.com/productsolutions/sqlserver/sqlcompliancemanager).

The datasheet for SQL Compliance Manager is available at [“https://www.idera.com/~media/corporate/files/datasheets/idera-sql-compliance-manager-datasheet.pdf”](https://www.idera.com/~media/corporate/files/datasheets/idera-sql-compliance-manager-datasheet.pdf).

New users can access the getting started guide for SQL Compliance Manager at [“https://www.idera.com/~media/corporate/files/solution-briefs/getting-started-guide-sql-compliance-manager.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/getting-started-guide-sql-compliance-manager.pdf).

Audit for regulatory compliance standards

For more information on how SQL Compliance Manager can help with FERPA, refer to the solution brief at [“https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_compliancesolutionsforhipaa.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_compliancesolutionsforhipaa.pdf).

For more information on how SQL Compliance Manager can help with GDPR, refer to the solution brief at [“https://www.idera.com/~media/corporate/files/solution-briefs/iderawp-areyoureadyforgdpr.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/iderawp-areyoureadyforgdpr.pdf).

For more information on how SQL Compliance Manager can help with HIPAA, refer to the solution brief at [“https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_compliancesolutionsforhipaa.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_compliancesolutionsforhipaa.pdf).

For more information on how SQL Compliance Manager can help with PCI DSS, refer to the solution brief at [“https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_complianceforpci.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-security_complianceforpci.pdf).

For more information on how SQL Compliance Manager can help with SOX and COBIT, refer to the solution brief at [“https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-solutionsforsarbanesoxley_cobit.pdf”](https://www.idera.com/~media/corporate/files/solution-briefs/idera-wp-sql-solutionsforsarbanesoxley_cobit.pdf).

Case study

To see how a medium healthcare enterprise in the USA ensured compliance to make their auditors happy with SQL Compliance Manager, read the case study at [“https://www.idera.com/~media/corporate/files/casestudies/hangerorthopedic_casestudy.pdf”](https://www.idera.com/~media/corporate/files/casestudies/hangerorthopedic_casestudy.pdf).

ABOUT THE AUTHOR

Elan Kol is a senior product manager at IDERA Software. His major focus is on the SQL Server auditing, security, optimization, and database administrator productivity product lines. Elan brings over ten years of experience in the financial technology, Information Technology security, and game development industries. His passion is building, delivering, managing, and optimizing products with great market fit through data driven and market backed facts.