IDERA® | SQL Compliance Manager

PROTECT AND AUDIT YOUR SQL SERVERS

WITH SQL COMPLIANCE MANAGER

BY GREG ROBIDOUX

INTRODUCTION

Data is vital for a business to run day-to-day operations and as a strategic advantage over competitors. Aside from the need to collect and process data, important business decisions are based on data and therefore data needs to be safeguarded and treated as one of the most valuable assets of a company.

Some issues with data are incompleteness, inaccuracies, update mistakes, malicious activities (such as data destruction or stealing data and using it to cause harm) and more. Every company needs to put in place mechanisms to safeguard their data and databases. This can be physical security, network security, database security, application security, etc. By creating opportunities for malicious activities, or worse, not knowing they exist, this creates a potential situation where valuable data becomes worthless or leaked data could cause reputation harm and legal consequences.

Most organizations follow methods and procedures to ensure databases are secure, but the problem is that you do not know what you do not know. It can help to build an environment to create and collect metadata. It provides the ability to catch harmful activity right away or at least provides the mechanism to go back in time to identify what happened, when it occurred, and how it occurred.

So how do you audit your database systems and where can you collect data from? There are several methods for collecting data one can use for analysis, including:

- System logs, like operating system and Microsoft SQL Server
- Build custom logging tables in the database
- Build custom applications for logging
- Use database snapshots to compare before and after values
- Apply Microsoft SQL Server policies
- Log failed login attempts
- Build tight security around database objects and data access
- Use change data capture to get old and new values
- Create triggers on tables to capture data changes

These options work, but as you read through the list, you can observe that there is not one option that will do everything. The option you pick may handle a specific area, but unless you use these methods or some combination, you can never capture the needed data to answer the questions of who, what, when and where.

WHAT THINGS DO YOU NEED TO AUDIT?

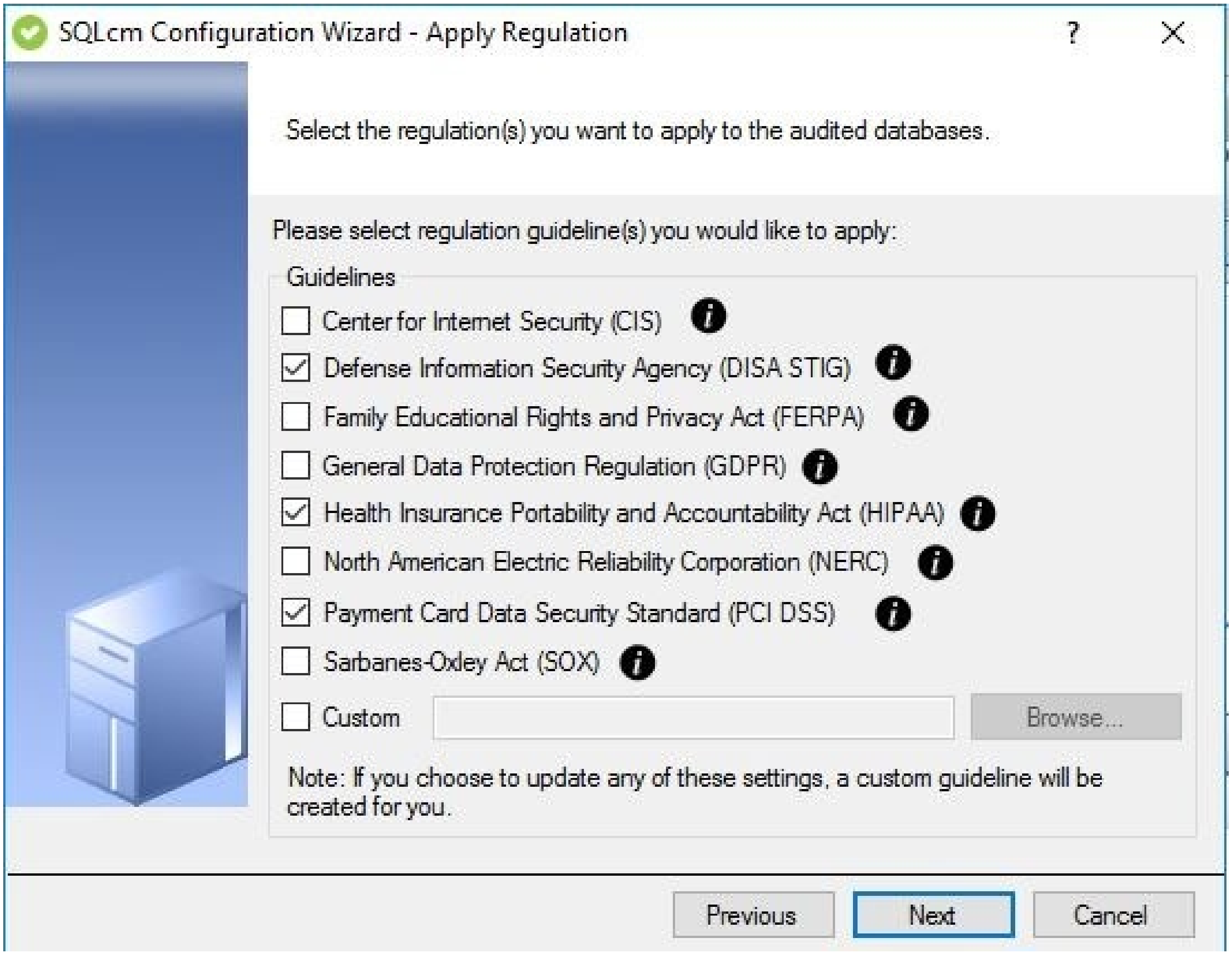
Well, this depends on the organization, and the data that is stored in your databases. Some data require stricter guidelines, while other data may not be an issue when comprised or lost. Here are is a starting list of some things to consider when implementing an auditing solution:

- Regulations - this is the driver for putting an auditing solution in place. Some of these regulations include HIPAA, SOX, GDPR, PCI DSS, and FERPA. You already heard about this from others in your organization if you need to implement a solution for one of these items. Now it is up to you as a data professional to figure out what needs to be done and how it needs to be done. This can consume a significant amount of your time.
- Failed login attempts
- Identify creation or deletion of database objects
- Know when server configuration changes occur
- Successful login attempts: When, who, and how
- Data changes: Before and after values
- Knowledge of who viewed data
- Database backups that occur outside regular backup schedules
- Someone disabling triggers
- Creation of new logins
- Security access changes

As you can see, the list is pretty long and not is this a complete list. So how do you capture the data to either alert you right away of a potential issue or provide the forensics you need to find and recreate a potential data breach? Well, the first approach is always to build your own solution. There is a specific need and technique you want to implement. The downside is this may cover one or maybe a couple of scenarios, but what about the things you did not think of? How do you handle those situations? This is where SQL Compliance Manager comes into play. SQL Compliance Manager is a tool built with these things in mind. There is a team of people at Idera that are polling multiple customers to determine what they need and staying current with regulations that need to be followed.

REGULATORY COMPLIANCE

As mentioned earlier, the driving factor for an auditing solution is to comply with some regulation. Well, SQL Compliance Manager already has this figured out and has templates you can deploy for the following regulations:



SQLcm Configuration Wizard - Apply Regulation

Select the regulation(s) you want to apply to the audited databases.

Please select regulation guideline(s) you would like to apply:

Guidelines

- □ 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)
- □ Custom

Note: If you choose to update any of these settings, a custom guideline will be created for you.

As you can see from the list above, someone has already taken the time and effort to build the collection methods needed to meet regulation guidelines when using Microsoft SQL Server. This also helps you streamline the implementation without the need to study the guidelines and then figure out how to implement various techniques for data collection, analysis, and reporting.

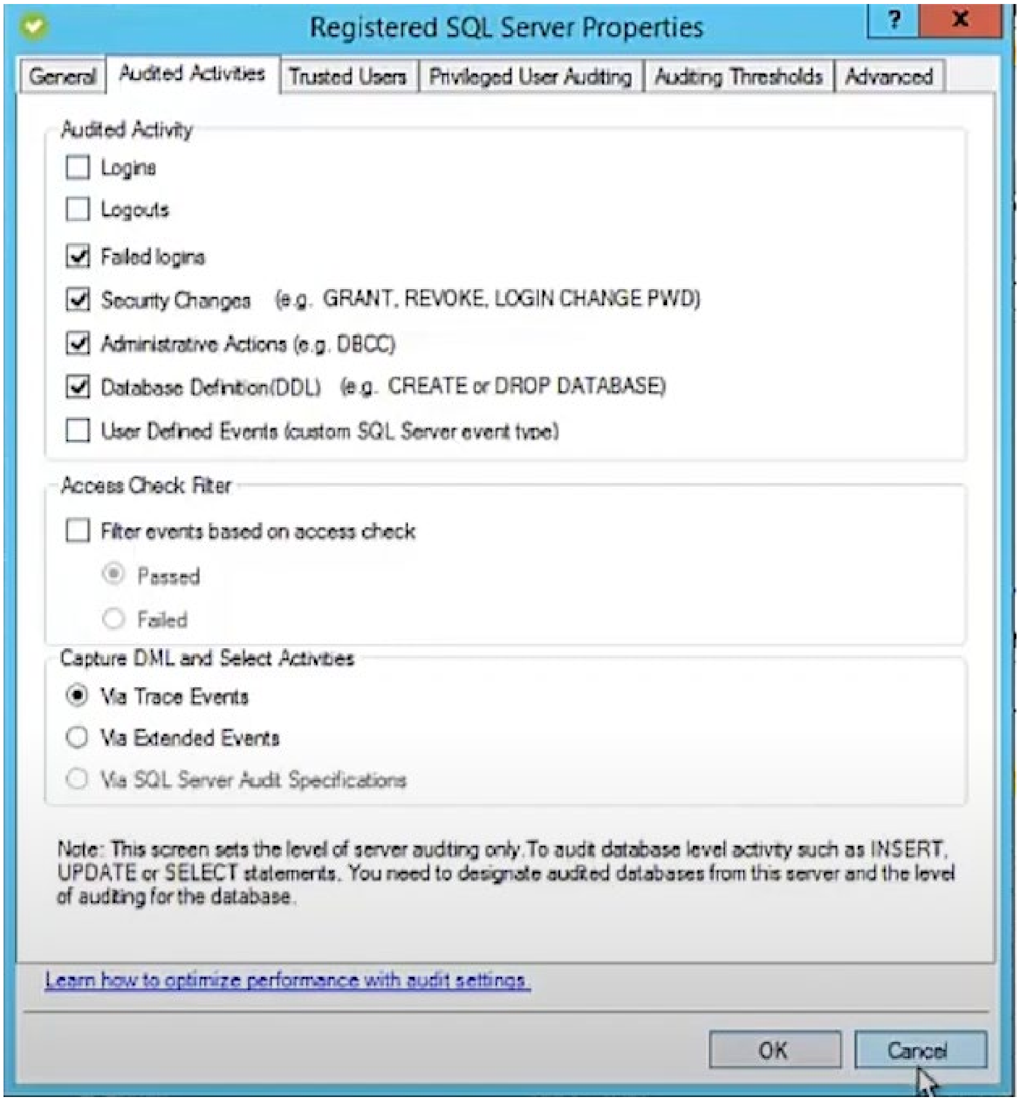
SQL Compliance Manager is the obvious choice if you need to implement an auditing solution to meet one of these guidelines. Do not waste your time and effort building something that already exists.

In the previous sections, we described the obvious reason you should use SQL Compliance Manager. So what are the reasons you would use SQL Compliance Manager if you did not need to follow a regulation guideline? Well, there are still plenty of things that could go wrong. You may not need to pay a regulatory fine, but what if a data breach occurs causing application downtime, or leaked data causes current or future problems? Here are some reasons an auditing solution is important.

SECURITY

Microsoft SQL Server can become pretty complex when dealing with security. First, you need to think about the server installation and the service accounts used to run Microsoft SQL Server. Next, you can use two methods of access to Microsoft SQL Server: SQL logins and Windows Authentication. Then, within Microsoft SQL Server, you have server roles and individual permissions that you can grant to objects. Then, at the database level, you have database roles and also the ability to grant permissions on individual objects. As you can see, there are several levels that can you can change. This creates an opportunity for access that should not be available to a user and the ability to change and elevate permissions to access certain data for a moment in time. If you are not tracking these access changes, you may never know who has access at any point in time.

Here is a list of some things SQL Compliance Manager can audit.



Audited Activity

□ Logins
□ Logouts
☑ Failed logins
☑ Security Changes (e.g. GRANT, REVOKE, LOGIN CHANGE PWD)
☑ Administrative Actions (e.g. DBCC)
☑ Database Definition(DDL) (e.g. CREATE or DROP DATABASE)
□ User Defined Events (custom SQL Server event type)

Access Check Filter

□ Filter events based on access check
● Passed
○ Failed

Capture DML and Select Activities

● Via Trace Events
○ Via Extended Events
○ Via SQL Server Audit Specifications

Note: This screen sets the level of server auditing only. To audit database level activity such as INSERT, UPDATE or SELECT statements. You need to designate audited databases from this server and the level of auditing for the database.

Learn how to optimize performance with audit settings.

WHO DID WHAT, WHEN AND HOW

Another area to think about is when a data change causes issues with the database or applications. Are you able to track down before and after values? Can you figure out when a change occurred and what user or application made the change? These could be critical pieces of information for when something goes wrong or worse yet a malicious actor gets access to your systems and causes harm to your data.

AUDITING

SQL Compliance Manager will allow you to set up measures to collect the data and generate reports, whether you need to follow and implement an industry standard regulation or you need internal auditing. As mentioned, you can implement one of several home-grown methods to capture the data you think you need, but what do you do when the data you need did not collect? Therefore, it makes sense to use all the auditing features of SQL Compliance Manager to meet your auditing goals.

WHO VIEWED THE DATA

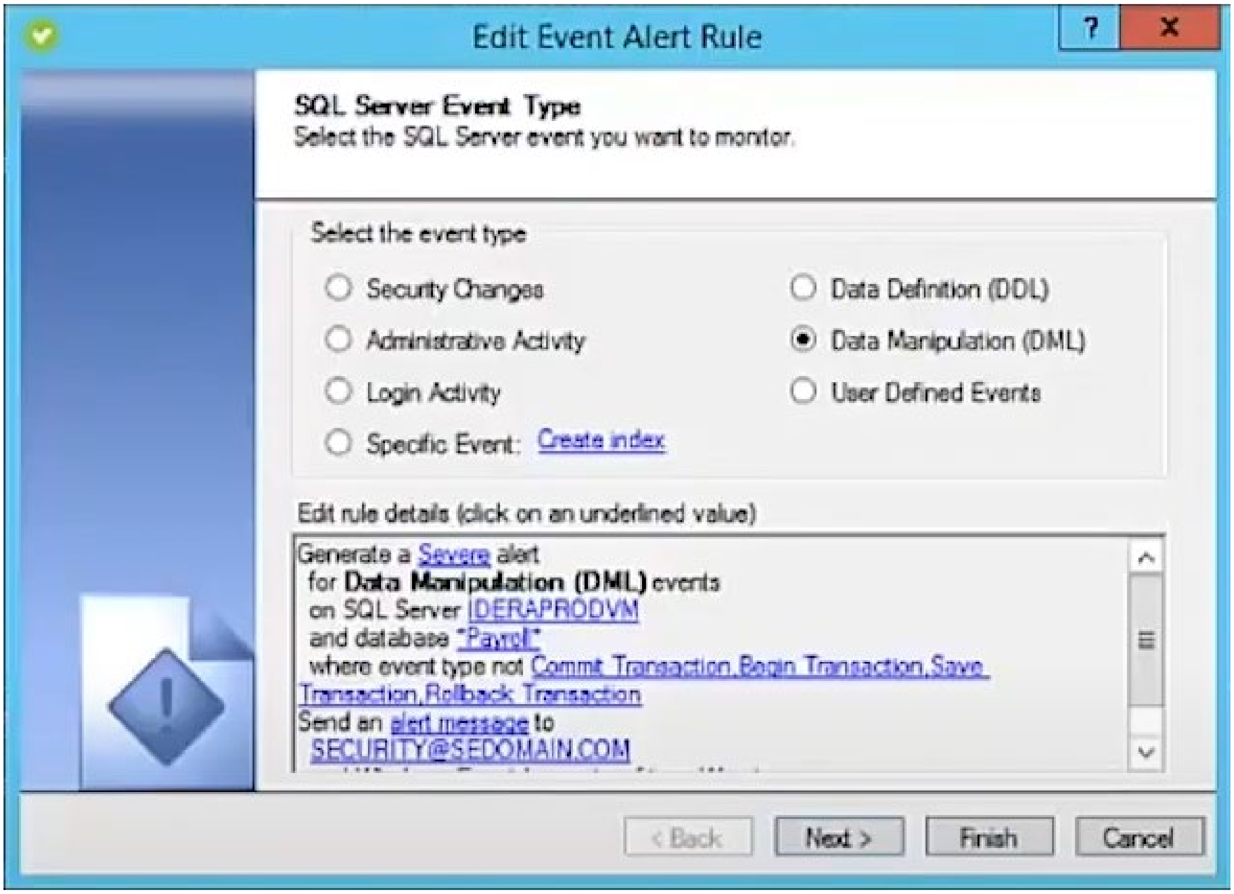
Most implementations for auditing collect before and after data so you can see what people changed and when. What if you have sensitive data, such as medical records or confidential employee data? How do you know that someone is not looking at this data that requires safeguarding and should be secure and not accessible to people that should not have access? This is another area where you can configure SQL Compliance Manager to capture data about what people viewed and who viewed the data. Instead of capturing every select statement that occurred, you can customize this to capture only when people access data you determined is a potential issue.

MANAGING COLLECTED DATA

Collecting data on your data and all the changes that occur could become quite overwhelming at some point. Over time, this data store can become quite large and require the need to figure out ways to prune and archive older data that may not be of importance anymore. If you build your own solution, you would need to build this into your plans, but often people do not think of future needs like this and take on a life of their own. The great thing about SQL Compliance Manager is that the vendor already built this feature into the solution, so you can keep the collected data to a manageable size with just a few configuration settings.

NOTIFICATIONS AND ALERTS

Being notified right away when a potential threat occurs or a change takes place that is not allowed or an unexpected change occurs is very important. This allows you to address the issue as soon as possible instead of having to wait to review reports to determine if an event occurred that should not happen. SQL Compliance Manager allows you to build alerts for various activities that take place, as shown below. You then also can configure an action to take place when the event occurs.



SQL Server Event Type
Select the SQL Server event you want to monitor.

Select the event type

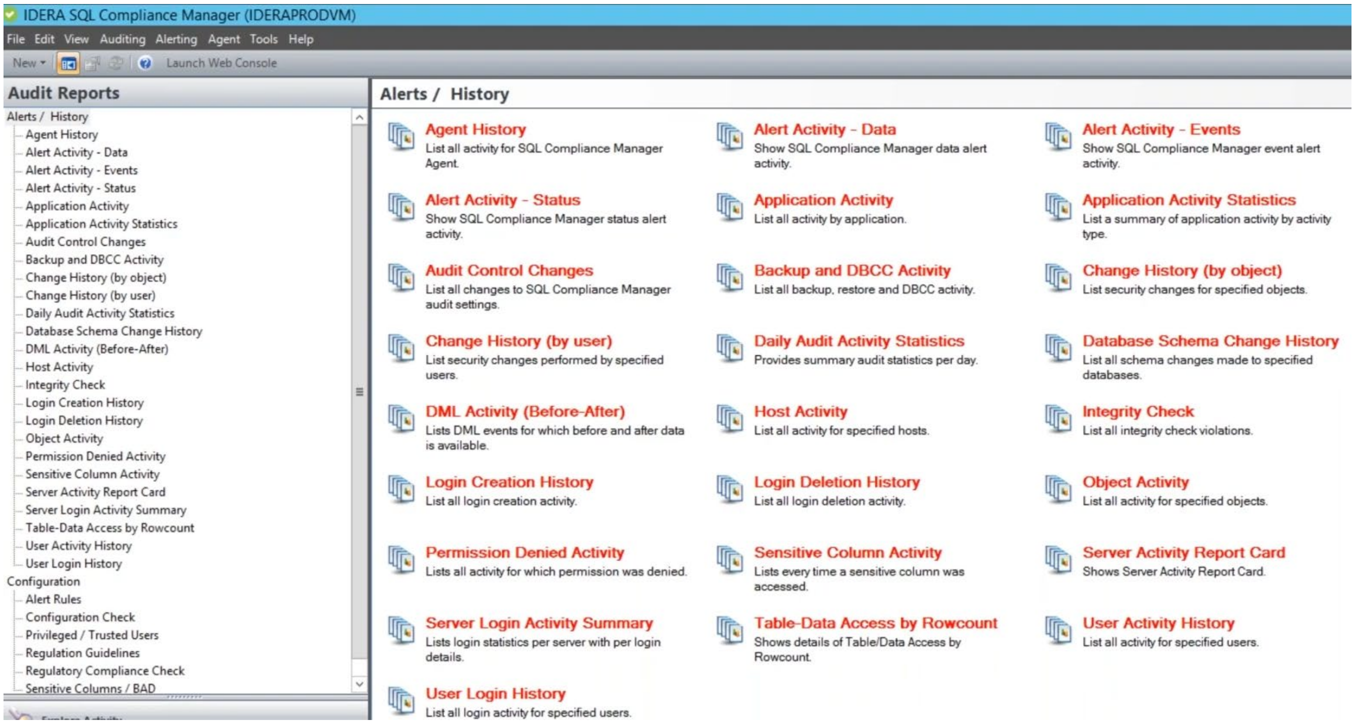
○ Security Changes
○ Administrative Activity
○ Login Activity
○ Specific Event: Create index
○ Data Definition (DDL)
● Data Manipulation (DML)
○ User Defined Events

Edit rule details (click on an underlined value)

Generate a Severe alert
for **Data Manipulation (DML)** events
on SQL Server IDERAPRODVM
and database "Payroll"
where event type not Commit Transaction,Begin Transaction,Save Transaction,Rollback Transaction
Send an alert message to
SECURITY@SEDOMAIN.COM

REPORTING

The result for any auditing solution is to use the data to answer your auditing questions. It is great that you have data that can answer these questions, but it often takes time to build queries and reports that could satisfy internal, customer, and regulatory compliance needs. SQL Compliance Manager offers many built-in reports:


IDERA SQL Compliance Manager (IDERAPRODVM)
File Edit View Auditing Alerting Agent Tools Help
New
Launch Web Console

Audit Reports

Alerts / History
- Agent History
- Alert Activity - Data
- Alert Activity - Events
- Alert Activity - Status
- Application Activity
- Application Activity Statistics
- Audit Control Changes
- Backup and DBCC Activity
- Change History (by object)
- Change History (by user)
- Daily Audit Activity Statistics
- Database Schema Change History
- DML Activity (Before-After)
- Host Activity
- Integrity Check
- Login Creation History
- Login Deletion History
- Object Activity
- Permission Denied Activity
- Sensitive Column Activity
- Server Activity Report Card
- Server Login Activity Summary
- Table-Data Access by Rowcount
- User Activity History
- User Login History

Configuration
- Alert Rules
- Configuration Check
- Privileged / Trusted Users
- Regulation Guidelines
- Regulatory Compliance Check
- Sensitive Columns / BAD

Alerts / History

Agent History
List all activity for SQL Compliance Manager Agent.

Alert Activity - Data
Show SQL Compliance Manager data alert activity.

Alert Activity - Events
Show SQL Compliance Manager event alert activity.

Alert Activity - Status
Show SQL Compliance Manager status alert activity.

Application Activity
List all activity by application.

Application Activity Statistics
List a summary of application activity by activity type.

Audit Control Changes
List all changes to SQL Compliance Manager audit settings.

Backup and DBCC Activity
List all backup, restore and DBCC activity.

Change History (by object)
List security changes for specified objects.

Change History (by user)
List security changes performed by specified users.

Daily Audit Activity Statistics
Provides summary audit statistics per day.

Database Schema Change History
List all schema changes made to specified databases.

DML Activity (Before-After)
Lists DML events for which before and after data is available.

Host Activity
List all activity for specified hosts.

Integrity Check
List all integrity check violations.

Login Creation History
List all login creation activity.

Login Deletion History
List all login deletion activity.

Object Activity
List all activity for specified objects.

Permission Denied Activity
Lists all activity for which permission was denied.

Sensitive Column Activity
Lists every time a sensitive column was accessed.

Server Activity Report Card
Shows Server Activity Report Card.

Server Login Activity Summary
Lists login statistics per server with per login details.

Table-Data Access by Rowcount
Shows details of Table/Data Access by Rowcount.

User Activity History
List all activity for specified users.

User Login History
List all login activity for specified users.

WORK SMARTER, NOT HARDER

As a database professional, you deal with many competing priorities. When tasked with a request, it would make sense to take the time to do research to determine if someone already created what is being requested. It also helps to determine how you can take advantage of what exists versus starting at the beginning. With auditing, this can be a very complex topic and include many nuances and requirements that may exist on the first day or someone requests at a future date. Instead of building one-off solutions to meet an individual need, look to SQL Compliance Manager as your solution to allow you to answer your auditing questions from the first day.

ABOUT THE AUTHOR

Greg Robidoux is the President and founder of Edgewood Solutions, a technology services company delivering services and solutions for Microsoft SQL Server. Greg is also a co-founder of MSSQLTips.com. He has been working with Microsoft SQL Server since 1999 and has authored many articles and delivered several presentations online and at local and national Microsoft SQL Server events.

Start for Free