Reduce audit data to optimize performance

Use the following checklist to help you optimize IDERA SQL Compliance Manager performance by fine tuning your auditing settings to prevent excess data collection.

As SQL Compliance Manager collects audit data and stores this information in the Repository, the event databases grow. When SQL Compliance Manager is configured to audit all SQL Server events, the event databases can grow very large (up to several gigabytes) in a single 24-hour period, especially in larger environments or environments with high-volume traffic. For more information about event databases in the Repository, see Product components and architecture.

	Follow these steps ...
✓	Archive or groom stale audit data from the event databases on a regular basis. Archiving allows you to move older events whereas grooming allows you to delete older events. For more information, see How archives work and How grooming works.
✓	Re-index and shrink each event database from which you have archived or groomed data. You can use native Microsoft SQL Server tools or other third-party tools such as IDERA SQL Defrag Manager.
✓	Carefully choose the events you need to audit. The growth and overall size of the event databases is a direct result of the auditing configuration you define. For more information, see Fine tune your audit settings.
✓	Consider configuring Event Filters. Event filters prevent collection and storage of unwanted events. For example, you can use Event Filters to exclude specific applications and operations that perform benign activities, and therefore do not require auditing, from your audit trial. For more information, see Event Filters.
✓	Consider configuring trusted user filters. Trusted user filters sift out events initiated by specific user accounts on an individual database. In general, a trusted user filter will be more resource-efficient than an event filter when excluding non-useful or benign events from your audit data collection.