IDERA®

SQL Server Whitepaper

WHAT YOU NEED TO KNOW ABOUT COMPLIANCE AUDITS

COMPLIANCE AUDITS

Compliance audits are an inescapable part of the information technology world we live in. A compliance audit is a detailed review that is conducted regarding the degree to which an organization is following specific regulatory guidelines or terms of a contract. The audit can address service level agreements (SLAs) made with clients or regulatory requirements mandated by industry or governmental agencies.

This whitepaper will discuss the reasons that compliance is important and outline the steps required for organizations to respond successfully when called upon to engage in an audit. While there are differences in how various entities may perform an audit and the focus of their queries, the methods for passing one are essentially the same.

THE INCREASED EMPHASIS ON COMPLIANCE

Concerns surrounding the privacy and security of personally identifiable information (PII) and other forms of sensitive data are becoming more important every day. The problem of data breaches and the associated risks of compromised private information are issues that show no sign of slowing down anytime soon. As big data and other digital information streams are incorporated into enterprise databases, the issue will continue to increase in significance to organizations and the individuals with whom they interact.

Data breaches are not the only problem surrounding the collection of personal data by corporations around the world. Citizens have well-founded reasons to question how organizations make use of the information they gather about individuals. They are demanding more control over how this data is collected, used, and shared.

These demands have given rise to more stringent compliance standards in many parts of the world. The European Union (EU) is leading the way with the introduction in 2018 of the General Data Protection Regulation (GDPR). It addresses many of the problems inherent in the way personal data is collected and affords the citizens of the EU methods that can be used to limit the amount of personal information retained by an organization.

A patchwork of data privacy regulations exists in the United States, but no overriding policy equivalent to the GDPR is yet in place. The California Consumer Privacy Act is modeled after the GDPR and may eventually result in nationwide privacy guidelines being enacted. For now, companies operating in the United States of America may be faced with staying compliant with numerous and diverse sets of regulations.

Businesses that have customers in jurisdictions with electronic data privacy laws are subject to the local guidelines no matter where the corporation is located. Physical boundaries are often irrelevant in the world of e-commerce, with companies supplying goods and services to individuals spread across the globe. This means that most businesses need to comply with multiple regulations or risk the penalties associated with noncompliance.

TYPES OF COMPLIANCE AUDITS

Audits are usually performed by external entities who are certified by the organization responsible for the compliance regulations. They can also be conducted by internal teams either in preparation for a more formal audit or with the motivation to identify and close gaps in their procedures. Various types of compliance audits focus on different aspects of an enterprise's operations and data resources.

Industry-specific compliance audits are mandatory across many sectors. Failure to pass these audits may result in the loss of business or financial penalties. Examples include those designed to enforce Health Insurance Portability and Accountability Act (HIPAA) regulations by enterprises with ties to the healthcare industry or the Payment Card Industry (PCI) Data Security Standard that pertains to financial and payment processing institutions.

Sarbanes-Oxley (SOX) is a set of regulations designed to protect shareholders from accounting and reporting errors from publicly owned companies. It contains regulations that are aimed at a company's Information Technology (IT) operations, specifically on how data is encrypted and securely stored.

GDPR audits are often done at the request of an organization to identify problems that need to be addressed to avoid the financial penalties that are prescribed by the regulations. Whereas an enterprise may be subject to yearly SOX audits to satisfy regulators, there are currently no such schedules related to ensuring a company remains compliant with GDPR. In many cases, it is not an issue until a data breach occurs when it is too late to take corrective actions.

WHY COMPLIANCE AUDITS ARE IMPORTANT

Audits are important for a variety of reasons. Left to their own devices, some businesses would be content to roll the dice and deal with the repercussions of a data breach after the fact. Audits on enterprises with this mindset will often be performed to hold them accountable for the lax policies and procedures that resulted in personal data being compromised. Punitive financial penalties can be enforced by the governing bodies behind the regulations. Additionally, significant damage to an organization's reputation can follow revelations that they have failed an audit by a regulatory agency.

More enlightened organizations may engage in audits covering the same principles to strengthen their privacy policies and avoid running afoul of regulatory agencies. These proactive audits are designed to ensure that lesser penalties will be levied in the case that a data breach does occur. If it can be shown that the breach was not the result of lax compliance practices, the enterprise will not be vilified in the same way as one that has ignored the opportunity to take preemptive action.

Compliance audits can also serve as a method of demonstrating to customers or partners that a business is capable of conforming to the standards set forth in specific regulations. An example is when a private company is planning to go public with an Initial Public Offering (IPO). Successfully going through a Sarbanes-Oxley (SOX) audit to verify its financial policies and data handling procedures will increase the confidence of investors and potential clients that the company is being run effectively.

THE COMPOSITION OF A COMPLIANCE AUDIT

Internal audits may be done in a relaxed manner as a company strives to improve its procedures and afford better data privacy and security for its customers. Audits conducted by outside entities will be more formal and introduce increased levels of stress for the organization under review and its employees. Here are the steps that can be expected in an audit and the actions which should be taken to ensure a successful outcome.

Notification

The organization will be notified by the agency responsible for the audit regarding when it will commence and what is in scope. In this initial phase of the audit, its general direction should be understood by the enterprise being audited. Specific systems may be identified as targets for review and changes that impact the areas being audited should be put on hold. The purpose of an audit is to discover the real extent of a company's compliance with a set of standards, not their ability to address deficiencies. There will be plenty of time for this later in the process. For this reason, compliance is an issue that should be uppermost in the mind of an organization throughout the year, not just when an audit is announced.

Planning

After a notification is given, the audit team will engage in planning the strategy that will be used to perform the review. While the audited organization will not have access to the details of this strategy, it will have a general idea of what will be required during the audit. The teams or individuals who will interact with the auditors should be identified and reporting procedures tested to ensure that timely responses can be supplied to the audit team.

Initial Meeting

Auditors will have an initial meeting with upper management where the ensuing process will be explained in detail. Scheduling conflicts or other concerns can be brought up and resolved in this meeting to ensure that both sides are in agreement as the process unfolds.

Fieldwork

This is the phase of the audit in which real work is done. Based on the outcome of the planning and initial meeting, interviews of key personnel will be conducted as the business processes and procedures are reviewed. Auditors will want to speak with first-line employees who work with the systems being investigated rather than just supervisory or management figures. Random requests for documents that provide proof of corporate policies may be made and will need to be met within a timeframe dictated by the auditors.

The importance of choosing the right people to work with the audit team is highlighted in this step. Database administrators (DBAs) and system administrators who work with the systems under review are essential organizational resources for performing the fieldwork necessary to meet the auditors' requirements. There will often be ongoing communication between the auditors and enterprise employees to clarify what information is needed and how it should be presented.

Draft Audit

A draft audit represents the culmination of the reviews performed during the fieldwork phase of the process. The draft is prepared by the audit team and will include the findings and unresolved issues they have identified. Findings point to specific deficiencies or areas of concern that need to be addressed to satisfy the requirements of the audit. For example, the identification of shared, privileged accounts will often lead to findings that indicate a problem with the security of the systems they can access. Unencrypted data, non-expiring passwords, and dormant identifiers are also items that will be brought to light through audit findings.

Management Response

After auditors complete their draft audit, it will be presented to management. They will be charged with reviewing and responding to the draft. Management will be required to agree or disagree with the findings. They will also be responsible for communicating the plans and timeline that will be used to address deficiencies to the audit team.

Exit Meeting

A final meeting between auditors and management is normally scheduled to discuss the response to the audit and clear up any lingering questions regarding the process.

Final Audit Report and Feedback

The completed audit report is shared with the pertinent stakeholders so they can implement the changes needed to resolve the findings. There may be supplementary testing by the audit team to see if the organization has made the proper changes to address the findings. This can be an ongoing process that continues until the next audit is announced.

TIPS ON RESPONDING TO AUDITORS' REQUESTS

There is a right and a wrong way to answer the questions posed by auditors. The personnel interviewed by the audit team are often individuals who are technically proficient regarding the systems or processes under investigation. They are usually excellent at in-depth explanations about how specific procedures are performed but their technical expertise can get them in trouble when responding to the auditors' requests. Here are some points to keep in mind when talking with auditors.

Answer the questions truthfully. This may seem obvious, but when faced with potential findings that will negatively affect the outcome of the audit, there may be a temptation to attempt to obscure unflattering facts. As is the case in many other areas of life, the coverup will end up being worse than the original transgression. Accept the findings and move on to make the corrections required to address deficiencies identified during the audit.

Questions should be answered directly without embellishment or the inclusion of unnecessary or additional information. Expansive answers can pique an auditor's interest in other areas that were not in the original scope of the investigation. Provide answers which deliver the facts that were requested. If further information is required, the auditor can make a supplementary request.

The same discretion should be exercised when providing documents or reports that are requested during an audit. If the focus of the audit is on a few specific servers, the evidence that is supplied should encompass only those systems. Supplying reports that address servers that are not in scope may result in additions to the audit which will further complicate the process.

PREPARING FOR A COMPLIANCE AUDIT

Knowledge of the regulations that affect a particular business or industry is the most valuable commodity when preparing for an audit. This practice should be incorporated into the everyday workings of an enterprise so that there are no surprises when an audit is announced. At the very least, someone in the organization should be monitoring compliance websites to stay apprised of new developments that may affect the ability to negotiate an audit successfully. As the compliance landscape continues to evolve, this may necessitate a full-time role for an individual or team.

Trust is a valuable commodity in many aspects of a business but is not sufficient when dealing with compliance auditors. They will want to see evidence of compliance in the form of documents and reports. The best way to prepare for this certainty is for an organization to perform internal audits that verify documents and procedures. It should also test the reporting capabilities to confirm that the necessary proof of compliance will be readily available when the time comes.

Large corporations often have dedicated internal audit teams who focus on different areas of the business throughout the year. Smaller organizations may not have the need or resources for this type of team, but an ad hoc audit based on the knowledge gained by keeping abreast of compliance standards can and should be performed in any size enterprise. It is the best defense against failing the more formalized audits that are an integral part of the IT world.

Audits should not be seen as a confrontation between a company and the auditing entity. Rather, it should be received as an opportunity to identify processes and procedures that need to be strengthened to meet the compliance standards of the specific business being audited. Issues that are not adequately addressed in the aftermath of an audit will come back and cause larger problems for the organization down the road.

IDERA'S SOLUTION

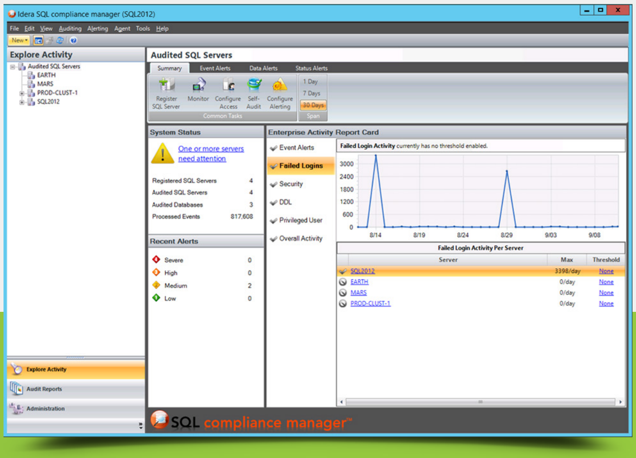
SQL COMPLIANCE MANAGER

Monitor, audit, and alert on user activity and data changes in SQL Server databases.

Simplify your SQL Server audits. SQL Compliance Manager is a comprehensive auditing solution that monitors and tracks changes to SQL Server objects and data, and sends alerts on suspicious activity. Obtain detailed visibility to determine who did "what", "when", "where", and "how", whether the event is initiated by privileged users or hackers. SQL Compliance Manager also helps ensure compliance with industry regulatory and data security requirements. SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.

Start a free, fully-functional, 14-day trial today!

Start for FREE



Registered SQL Servers	4
Audited SQL Servers	4
Audited Databases	3
Processed Events	817,608

Severe	0
High	0
Medium	2
Low	0

Failed Login Activity currently has no threshold enabled.

Failed Login Activity Per Server

Server	Max	Threshold
SQL2012	3398/day	None
EARTH	0/day	None
MARS	0/day	None
PROD-CLUST-1	0/day	None