Meeting Sarbanes-Oxley Requirements with DB Audit

Introduction

In the wake of numerous corporate accounting scandals our Nation's law makers have responded with a backlash of regulatory oversight. Today most enterprises must contend with new laws designed to make internal processes more visible to investors and protect personal information from being shared without the owner's consent. Perhaps the best known regulation introduced in the past decade, the Sarbanes-Oxley (SOX) Act of 2002 regulates how financial data must be handled and protected, and imposes new requirements for firms publicly traded on US markets to validate the accuracy and integrity of their financial statements.

SOX addresses the handling of all financial data, including electronic data as well as the processing of that data. Section 404 of the Act requires the annual evaluation and documentation of the internal controls and procedures in place to produce financial statements. Internal controls must be documented, and a system must be implemented to monitor their effectiveness. Section 302 requires the CEO and CFO to quarterly certify the existence of internal controls and to sign off on the veracity of the company's financial statements

Penalties for non-compliance with the Sarbanes-Oxley Act include stiff fines and potential prison terms for individual executives. Perhaps more importantly, other risks of non-compliance can jeopardize the viability of the enterprise as a business entity. In an information-based economy the failure to sufficiently protect information can lead to dire consequences – from misstated financial statements to losses through fraud to making decisions based on bad information. The potential for digital leakage of trade secrets, shareholder lawsuits, brand erosion, loss of customer confidence, and de-listing from stock exchanges can cripple or destroy what had taken years to build.

Information Technology Plays a Crucial Role

Information technology provides the tools to develop an effective system of internal controls and is crucial to achieving Sarbanes-Oxley compliance. Reliable information systems and effective access control procedures provide a foundation for companies to generate trusted financial reports and attest to the accuracy of the reported information as SOX requires.

While the role of IT may seem obvious, in many organizations the initial focus of SOX compliance has been with finance and legal departments, with IT viewed as a supporting player at best. The problem with this approach is that process control and data integrity – key issues for SOX and many other regulations - are not items that can provided as an afterthought or in reaction to a new law. They need to be established as part of enterprise security policy and part of the fabric of the IT infrastructure. Process control

and data integrity cannot be viewed as a veneer, but as a strategic element of everything IT builds or manages. At stake is a variety of risks, from economic penalty, through loss of business due to damaged reputation, to the incarceration of key executives.

There is no questioning the importance or intent of Sarbanes-Oxley, but the absence of specifics has left many companies scrambling to comply. The need for practical guidance as to how to maintain control over electronically stored data can be a source of frustration and concern. The first step in defining a system of internal controls involves working with the internal and/or external audit team to understand the controls required to support the established internal or external audit standards. Specific attention should be paid to what is required to be audited by applications and what is required to be audited at the database level.

A number of paradigms exist, including COSO Internal Control Framework, COBIT and regulatory guidance. Regardless of the approach, we can categorize IT general controls into four broad groups:

1. Controls over program development
2. Controls over program changes
3. Controls over computer operations
4. Computer security

While IT general control effectiveness varies from company to company, most organizations have a mature system development lifecycle which governs program development and program change management. This isn't meant to imply that breakdowns in design or operation don't occur, because they do. But the more serious risks are typically attributed to inadequate security where improper access to data or programs can wreak havoc.

The Need for Data Auditing

Once an understanding of the controls has been obtained the next step is to design how the controls will be turned into actual auditing rules used to monitor compliance. While COBIT, the Control Objectives of Information and related Technology, has emerged as the auditor's bible for understanding what is required in a SOX audit, COBIT merely provides a set of objectives but no directives. Still, many organizations are basing the development of their internal controls procedures on the areas COBIT identifies as essential for monitoring and reporting:

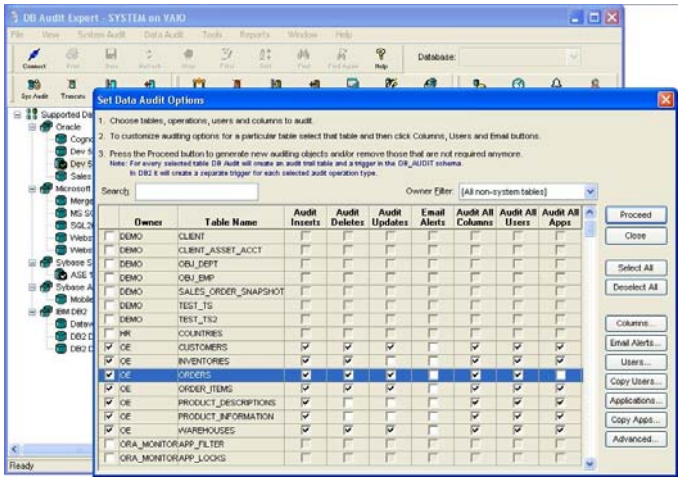
- Account management controls
- Audit policy changes
- Successful logon tracking
- Failed logon tracking and alerting
- File Access controls and notification

- User privileges tracking
- General System Security via event logs
- Security Systems Performance and Stability ensuring continuous availability

We live in an information economy; enterprises today are dependent on database technology to run their business. The mission-critical data assets in their databases need to be protected from inappropriate access and data changes. In that most of the information that comprises an organization's financial reports is also stored and maintained in databases, it is essential that their databases be subject to a continuous audit. The persistent auditing of database access and data changes is the only sure way to validate what is actually happening and to monitor the preventative controls intended to ensure data integrity. The combination of preventative controls with continuous monitoring will provide executives and auditors with the ability to attest that internal controls and procedures are in place to produce the organization's financial statements.

SoftTree Technologies® DB Audit Expert™ for SOX Compliance

DB Audit Expert is an enterprise database auditing solution enabling the establishment of a system of database internal controls and procedures for Sarbanes-Oxley compliance. DB Audit Expert can track and analyze any database activity, including database security, access and usage, data creation, change, or deletion. The Product addresses key database security concerns that include database security and vulnerabilities assessment, database access and user activity auditing, business and regulatory compliance. DB Audit Expert also addresses business process tracking issues that include business data change tracking, user and application activities monitoring, and data access patterns monitoring.



DB Audit monitors database events in the following categories:

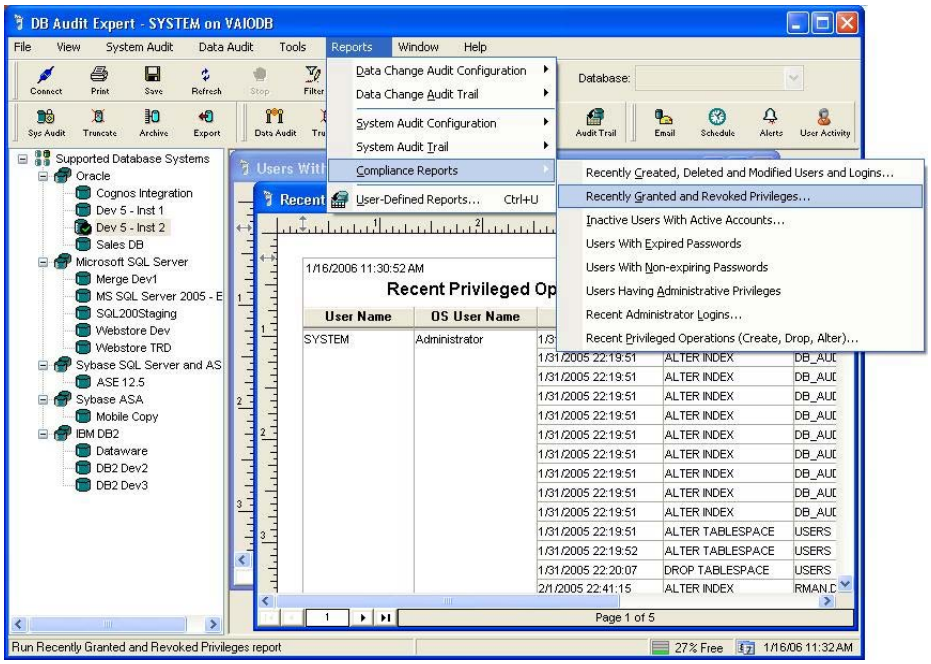
- Logon events
- Account logon events
- Object access events
- Privilege use events
- Policy change events

DB Audit Expert provides for the tracking and analysis of any database activity including database access, logons, security breaches, user and application activities, data creation, change or deletion. Providing a comprehensive audit trail of database

security gives the organization unparalleled visibility into who did what to which data, when, and by what means. Specifically, DB Audit Expert:

- Provides an audit trail of database activity capable of withstanding repudiation so that executives can attest to the integrity of the data.
- Provides totally transparent system-level and data-change auditing of databases for unauthorized changes and approved changes by privileged users that occur outside of the application's control.
- Provides the ability to ascertain whether unauthorized access to sensitive information has occurred; improving system security and ensuring system accountability to safeguard data integrity.
- Features centralized auditing control of multiple database systems from a single location to augment current preventative security measures by tracking what actually happened to the data that form the basis of your financial reports.
- Provides eight SOX Compliance Reports that reduce large amounts of audit data into comprehensive summaries and help comply with the SOX regulations:

    1. Recently created, deleted, or modified users and logins
    2. Inactive users with active accounts
    3. Users with expired passwords
    4. Users with non-expiring passwords
    5. Users having administrative privileges
    6. Recent administrator logins
    7. Recent privileged operations
    8. Recent granted and revoked privileges



SoftTree Technologies' DB Audit Expert satisfies the objectives specified in COBIT and is exactly what your auditor's require to prove the existence of effective control over access to financial data, including changes to the user accounts of those with access and the ability to raise a red flag when a breach in procedures is encountered. DB Audit Expert's data-change audit functions can be used to capture data-change events in database tables and to record the "before" and "after" values as well as who, when and how the changes were made. DB Audit Expert also allows for real-time automated email alerts to notify data owners about the data-change events.

DB Audit Expert provides a practical solution for the management of database events; the ability to monitor events in real time; identify the events that are required for reporting and provide a means to automatically respond to events that require immediate attention. Additionally, DB Audit Expert automates the process of archiving audit trails from critical servers and workstations that contain financial data.

Summary

Sarbanes-Oxley compliance initiatives should be considered an opportunity to implement much needed data integrity, internal control, and security improvements within the enterprise. Improving internal controls enables the organization to conform with SOX requirements but also results in enhancing the organization's ability to manage risk, reduce operational costs and increase shareholder confidence.

DB Audit Expert provides the best measure to monitor and audit database access and data changes. A comprehensive solution for the configuration of SOX audit functions, DB Audit Expert will record various events that have or will occur in the monitored database, primarily for improving system security, detecting penetration of the system and identifying misuse of resources.

Visit SoftTree Technologies' website for more information about DB Audit Expert solutions and to download a free trial version http://www.softtreetech.com/dbaudit/