Guardium®
SAFEGUARDING DATABASES™

Sarbanes–Oxley Database Compliance

White Paper

Introduction

Over the last few years, numerous prominent and headline-grabbing accounting scandals have taken place in major corporations. As a result, the Sarbanes-Oxley Act (SOX) was designed in the hopes of reducing fraud and conflicts of interests, while increasing financial transparency and public confidence in the markets. SOX defines a framework that makes it harder for executives to claim that they were unaware if information is compromised. Under the act, companies must maintain proven auditing practices and assure integrity and timeliness of data.

While these stipulations might seem straightforward in theory, the reality is that they can be relatively difficult to meet. Most enterprises store financial records on relational database repositories. Access to these records is usually restricted to authorized personnel via corporate applications such ERP, CRM, and SCM. However, authorized staff may also use other clients (e.g. Excel spreadsheets) to access or update financial records. An inadvertent mistake made to the records can be completely invisible to the financial and auditing teams responsible for attesting to the records' accuracy. A worse scenario is that of malicious activity perpetrated by a person who has the knowledge to bypass the perimeter firewall or who has local access (e.g., using telnet, direct console, or a developer/DBA tool) to critical financial databases.

Internal auditors facing these issues need application access visibility and effective controls to support compliance initiatives, because, in addition to monitoring and securing financial systems, SOX requirements necessitate comprehensive tracking and management of systems that handle critical corporate data. The bottom line is that while SOX compliance is primarily the responsibility of the CEO and CFO, the CIO and other IT professionals also need to implement strategies that support the explicit and implied integrity, security, credibility, and transparency requirements defined in this act.

Sections 302, 404, and 409 in particular affect IT organizations, requiring:

- Internal control
- Ongoing assessment (i.e., governance, measurement, and record keeping)
- Disclosure (i.e., investigation, reporting, and certification)

These requirements embody logical best practices. Even so, they can be difficult to follow, in particular since the technology available until now has generally not been adequate to meet rising compliance needs.

Traditional database audit limitations

The task of constant manual database auditing and compliance is impractical and sometimes even impossible. Continuous, real time visibility to database access activities is difficult for security personnel to achieve because few products offer granular monitoring capabilities that provide an understanding of the who, what, when, where, and how of all database access activities.

Most database administrators are reluctant to turn on database logging facilities because of the resulting impact on performance and disc space. Even if they do turn various logging and auditing facilities, the data generated requires a tedious data reduction effort. This endeavor is like the proverbial search for a needle in a haystack – just imagine looking through three months of logs in support of a quarterly statement. Additionally, anyone with access to these database logs could potentially change records and remove any audit trail of this activity, perpetrating the intrusive event.

Database auditing requirements

To accelerate your database compliance, as well as to safeguard your databases, you need a solution that provides a means for comprehensive database activity visibility. In addition, the solution must have advanced reporting, alerting, access control, and auditing features. These capabilities help establish an environment of accountability as required by sections 302, 404, and 409 of SOX act, ensuring that you can:

- Achieve ongoing security health assessment
- Maintain privacy through internal controls
- Prove claims
- Implement full disclosure when needed

To discover and document existing organizational policies, the solution selected should be able to automate a process of report production that covers such topics as planning and organizing for database compliance, certification and control of database activities, risk assessment, and investigation and disclosure of any exceptions. Having access to report templates that were built to address SOX implementations creates an ideal situation, since such templates do not require a great deal of setup but still have the flexibility to be customized to company needs.

All database requests must be able to be logged and a full audit trail should be easily and automatically extractable from this information. This audit trail needs to contain such information as which data was accessed, by whom, when, how, and from where. The exportable information can be maintained for as many years as necessary and submitted to the proper authorities as required. Automated scheduling of SOX workflows and audit tasks and dissemination of relevant information to responsible parties across your organization are also great time savers, helping to increase audit process efficiency.

When potential anomalies arise, the response must be instantaneous. Automatic alerts and access control help you handle situations in a timely and responsible manner. Database access protection needs can be met if there is flexibility in the type of alerts generated by the solution: real time, threshold-triggered, or policy-based. If an alert is triggered, you should be able to immediately ensure that all relevant parties are notified and block any further suspicious activities, in particular to sensitive data (such as social security or credit card numbers).

Other applications that are useful for SOX database compliance include a means for mapping access between financial applications database clients and servers and a detailed view of financial database access activities with continuous real time snapshots. These options provide an easy means for ongoing assessment of database access health, again increasing the atmosphere of accountability as required by SOX.

Guardium

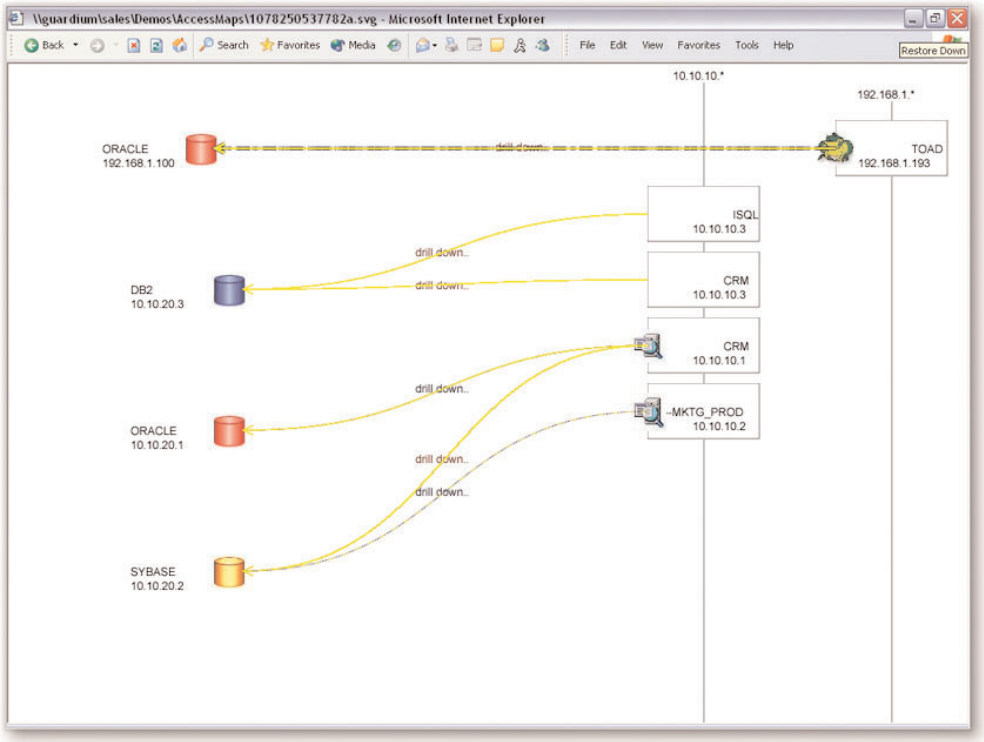
Guardium's SOX Accelerator

Guardium has simplified the task of continual auditing and compliance by developing the SOX Accelerator for Database Compliance. Tailored to address financial system monitoring of an organization, the SOX Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. These templates are divided into specific categories to help increase visibility into database activities while simplifying discovery of issues that need a closer look:

- *Plan and Organize* – View information about who and what touches financial information, which financial servers and databases are available, and more, to help with the planning phase of SOX database compliance.
- *Certify and Control* – Certify that all database access activities are above-board and that those that fall outside of SOX required parameters can either be rectified or explored further.
- *Assess Risk* – Receive information that can be used to gauge possible risks, with emphasis on those areas referred to in the database requirements of SOX.
- *Investigate and Disclose* – Dig deeper into any possible exceptions to discover the origin of any exceptions, as well as whether or not they are issues that warrant further handling.

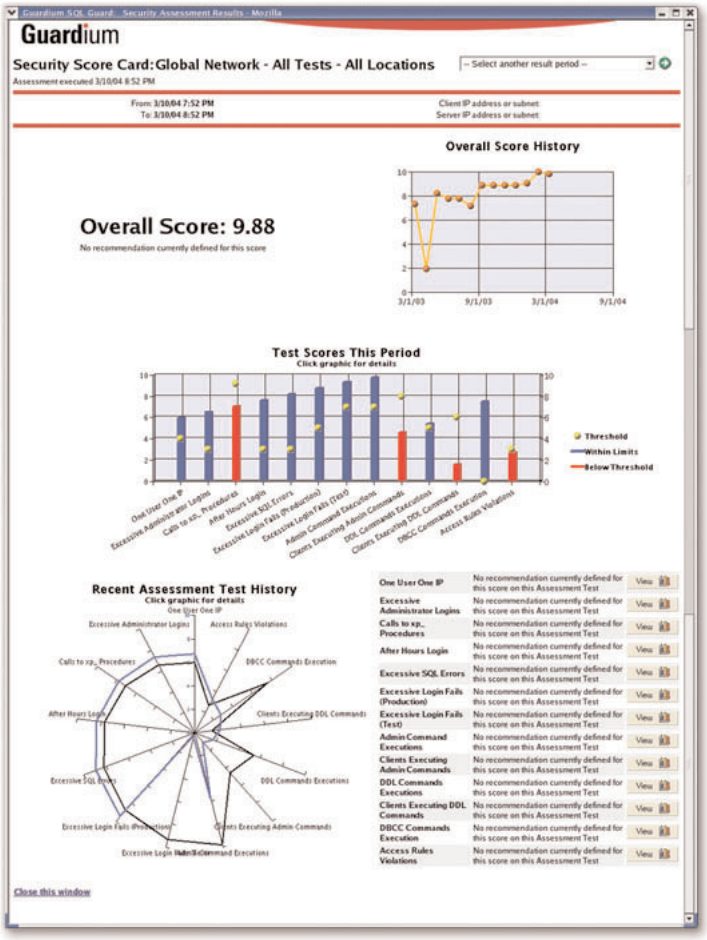
Other tools help to audit database activities, with the resulting data saved into an easily downloadable format:

- *Financial Applications Access Map* – Easily view access between financial applications database clients and servers using advanced visualization technology. This graphical map provides an at-a-glance view of activities by access type, content, and frequency.



> Financial Applications Access Map

- *SOX Compliance Report Card* – Automate the SOX compliance assessment process using a detailed view of financial databases access security health that contains continuous real time snapshots customizable for user defined tests, weights, and assessments.



> Compliance Report Card

- *Full Audit Trail* – Swiftly and non-intrusively generate a full audit trail for data usage and modifications required by regulatory compliance.
- *Automated Scheduling* – Streamline scheduling of SOX work flows, audit tasks, and dissemination of information to responsible parties across the organization.

Guardium®

Summary

The Sarbanes-Oxley Act requires that companies monitor and secure financial and other systems, such as ERP, CRM, and SCM, which monitor corporate data. To effectively accomplish this process, you are best off investing in a technology solution that can comprehensively cover your reporting and auditing needs while providing you with the power to respond swiftly should any incidences occur.

The solution you select should be flexible – able to monitor and protect your databases, regardless of the actual applications and systems using financial and customer information. Investing in more comprehensive database protection technologies produces tremendous cost savings over limited point solution tools.

In addition, keep in mind that while addressing the requirements of SOX, you can take a broader look at compliance issues in general, considering both the possibility of new compliance issues that could arise in the near future and stipulations mentioned in such acts as HIPPA, GLBA, and SB 1386. Investigate technology solutions that can help you improve your overall security health, while also being applied to a variety of database security auditing situations.

About Guardium, Inc.

Headquartered in Waltham, MA, Guardium develops and delivers innovative database security solutions that remove complexity, and provide visibility and effective controls over database access activities for IBM, Oracle, Microsoft, and Sybase environments. Guardium's family of non-intrusive, robust applications addresses key database security concerns such as security assessment, access policy control and enforcement, auditing, and regulatory compliance. Guardium's growing customer base includes some of the world's most technically advanced organizations representing a wide range of industries. Financial services, telecommunications, media, pharmaceutical, healthcare, and government organizations trust Guardium's solutions to protect their mission critical data. Guardium investors include the Cedar Fund, Veritas Venture Partners, and StageOne Ventures.

Guardium®

Prospect Place • 230 Third Avenue • Waltham, MA 02451 • T: 781 487 9400 • F: 781 487 7900

www.guardium.com