SOX Accelerator
for Database Compliance

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002, known as the Sarbanes-Oxley Act (SOX), is designed to reduce fraud and conflicts of interests, while increasing financial transparency and public confidence in the markets. Under the act, companies must maintain proven auditing practices and assure integrity and timeliness of data.

SOX necessitates monitoring and securing financial systems, as well as other systems that manage critical corporate data (ERP, CRM, and SCM). Therefore, while compliance is primarily the responsibility of the CEO and CFO, the CIO and other IT professionals must also implement strategies to support the explicit and implied integrity, security, credibility, and transparency requirements defined in SOX.

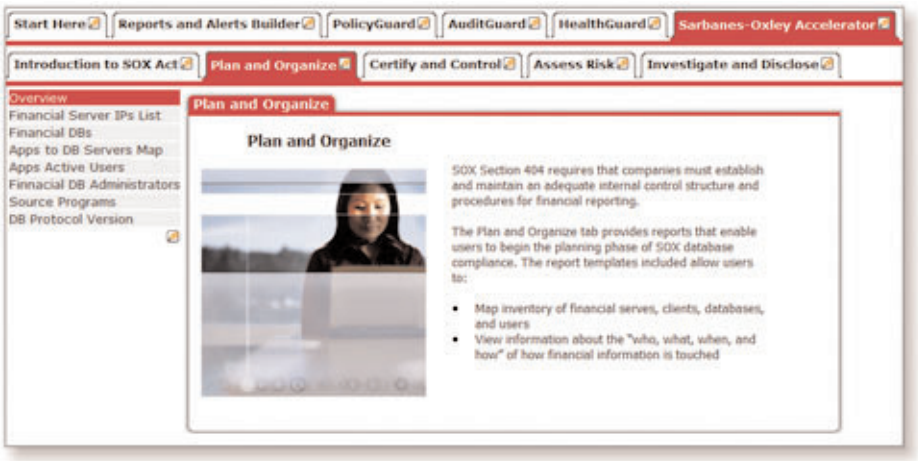
Sections 302, 404, and 409 in particular touch IT organizations, requiring:

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

Accelerating the process

Guardium's SOX Accelerator for Database Compliance simplifies the impractical and sometimes impossible task of continual auditing and compliance. As part of Guardium's growing array of database compliance accelerators, the SOX Accelerator simplifies the organizational processes needed to support these mandates and allow for financial database security.

Regulatory compliance requires advanced access control, auditing, and reporting features, all of which Guardium delivers through the SOX Accelerator and the SQL Guard database security platform. The Guardium solution documents and alerts on anomalous events. Predefined report templates increase visibility into database activities while simplifying discovery of issues that need a closer look. At the same time, the Guardium solution audits database activities and helps establish an environment of accountability.



Guardium's Solutions

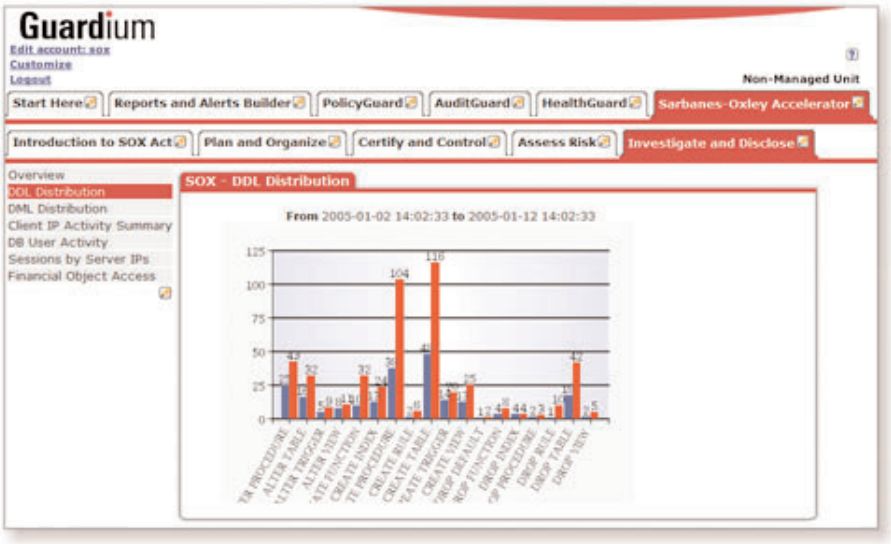
Working in conjunction with Guardium's other solutions, the SOX Accelerator speeds compliance by providing:

- **Financial Applications Access Map**
  A graphical map of access between financial applications database clients and servers using advanced visualization technology. This map provides an at-a-glance view of activities by access type, content, and frequency.
- **SOX Compliance Report Card**
  A detailed view of financial database access security health that automates the SOX compliance assessment processes with continuous real time snapshots customizable for user defined tests, weights, and assessments.
- **Comprehensive Audit Trail**
  The non-intrusive generation of a full audit trail for data usage and modifications required by regulatory compliance.
- **Automated Scheduling**
  Automated scheduling of SOX workflows, audit tasks, and dissemination of information to responsible parties across the company while securing organizational accountability.

Providing the tools to speed 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. You can access these templates using the tabs provided:

TAB	BENEFIT
Plan and Organize	Provides reports that enable users to begin the planning phase of SOX database compliance. The report templates included allow users to view information about who and what touches financial information, which financial servers and databases are available, and more.
Certify and Control	Enables users to 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. Information provided includes a "to do" list of audit tasks, as well as a variety of reports on such topics as financial system exceptions and failed user logins, user activity audit trails, SQL errors on financial data, and financial data access by unauthorized applications.
Assess Risk	Offers information that can be used to gauge possible risks, with emphasis on those areas referred to in the database requirements of SOX. These reports cover such categories as users employing multiple client IPs to access financial data, after hours activities on financial database servers, access to financial data by unrecognized users, attempts to access financial data by a non-recognized client, and a variety of commands executed on financial databases.
Investigate and Disclose	Supplies the means for digging 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. Reports offered include DDL and DML distribution on financial databases, client IP and database user activity on financial data, details about sessions by a financial server IP, and detailed activity on financial objects.



Guardium®
SAFEGUARDING DATABASES™

230 Third Avenue • Waltham, MA 02451 USA • T: 781 487 9400 • F: 781 487 7900 • www.guardium.com