White Paper

Reducing the Time and Costs Associated with Sarbanes-Oxley Compliance

Using Modern Database Management Tools to Simplify and Streamline SOX Compliance

Embarcadero Technologies

February 2009

Corporate Headquarters
100 California Street, 12th Floor
San Francisco, California 94111

EMEA Headquarters
York House
18 York Road
Maidenhead, Berkshire
SL6 1SF, United Kingdom

Asia-Pacific Headquarters
L7. 313 La Trobe Street
Melbourne VIC 3000
Australia

INTRODUCTION

In the years preceding the 90's client-server revolution and the Dot Com bubble, financial system security, availability and scalability were the focal points of IT concern and measurement. Generally, these systems were managed by large, stable main frame systems established decades prior with stabilizing policies around system data. The situation changed during the mid to late 90's when industry at large had nearly limitless access to new computing technologies and the capital to build them. The watchword of the day was 'growth' and the World Wide Web changed everything. Rapid growth and acquisition of customers through new web-based and other progressive technologies led to glaring oversights of data governance: Who has access to sensitive data, what happens to data from the time it is created to the time it is deleted, how are the final financial numbers computed, and from what sources with what controls?

An unfortunate series of well publicized fall outs demonstrated that the unbelievable growth these companies were achieving was inflated. The problem traced back to weak or virtually no governance on how companies managed and reported earnings and other critical financial measurements to Wall Street. Earnings could be enhanced as easily as a DBA could access data and manipulate it directly where it is stored within the database. Moreover, the growth and propagation of all these new systems bypassed many of the traditional mainframe controls and policy governance, making it fairly trivial for non-authorized personnel to gain access to data.

A means to regulate institutions, normalize accounting practices, and govern institutions managing sensitive and critical financial data was required, and by July 2002, the Public Company Accounting Reform and Investor Protection Act of 2002—commonly referred to as Sarbanes Oxley Act or "SOX"—was passed into law by the United States Federal Government.

Today, the Sarbanes-Oxley Act has significantly impacted most US publicly-traded companies, as well as companies across the globe. The Sarbanes-Oxley Act mandates executive responsibility for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. Although SOX doesn't explicitly mention the impact on IT systems, the requirements spelled out in Section 404 are used to derive the IT plans used to ensure compliance.

IT is the foundation of "an adequate internal control structure and procedures for financial reporting" for most organizations. Unfortunately, it is also where the costs of compliance start to add up. Much of the cost of compliance has come from the requirements of Section 404 – reportedly down to an average of $1.7M per company in 2007. At 180 words that comes out to a cost of almost $9500 per word.

This paper addresses two aspects of Sarbanes-Oxley Act compliance as it relates to Embarcadero's database tools: how the tools help with compliance and how the tools themselves are compliant.

THE RIGHT TOOLS FOR THE JOB

Because SOX doesn't explicitly spell out IT requirements for compliance, companies have turned to existing IT governance frameworks for guidance. The most common controls framework used in SOX compliance is the Control Objectives for Information and related Technologies, or "COBIT".

This paper maps specific aspects of COBIT compliance that pertain to SOX to Embarcadero's database tools. Embarcadero's easy-to-use solutions are easily implemented across your enterprise and can play a significant role in reducing the costs of SOX compliance.

ER/STUDIO ENTERPRISE: DOCUMENTING DATABASES AND BUSINESS PROCESSES

Embarcadero ER/Studio, an industry-leading data modeling tool, helps companies discover, document, and re-use data assets. With round-trip database support, data architects have the power to easily reverse-engineer, analyze, and optimize existing databases. Productivity gains and enforcement of organizational standards can be achieved with ER/Studio's strong collaboration capabilities.

IMPLEMENTING SOX CONTROLS WITH ER/STUDIO

ER/Studio assists you in maintaining the following controls:

- Define the Information Architecture
- Data Classification Scheme
- Integrity Management
- Business and Technical Requirements

DEFINE THE INFORMATION ARCHITECTURE (COBIT PO2)

ER/Studio Enterprise Edition includes a business process modeling tool and a central model repository. The process modeling tool is used for creating a graphical representation of your business from the core concepts that describe the business, to the processes that detail how your business operates and how those processes use data.

ER/Studio Repository provides organizations using the award-winning ER/Studio data modeling application with a scalable, server-based, model management system. It is designed to enable real-time concurrent access to data models between team members, implement security to protect models and components from unwanted access and change, facilitate component sharing and re-use across projects and offer extensive model version management.

One of the many powerful ways customers use the repository is to create and enforce an enterprise-wide data dictionary for better consistency, control, and integration

when developing new databases. The Enterprise Data Dictionary provides additional productivity by giving managers complete control over their ongoing projects with pre-defined data dictionaries that can be re-used and globally updated throughout the repository. This approach lessens the likelihood of modelers reinventing the wheel by defining attributes and data types across models.

DATA CLASSIFICATION SCHEME (COBIT PO2.3)

Out-of-the box, ER/Studio offers metadata tags for both information security and data privacy classification schemes. This metadata can be applied to entire models, certain tables, or even specific columns. Embarcadero typically recommends a three- or four-level classification scheme, but ER/Studio supports as many levels as are needed. With reverse engineering, ER/Studio can be used to quickly document existing databases and add data classification labels where needed.

INTEGRITY MANAGEMENT (COBIT2.4)

Knowledge workers can spend significant amounts of time looking through data sources, researching what information means, and find that it is not being used appropriately. ER/Studio helps data architects define and reuse common data elements and modeling components across projects to establish standards in their modeling practices. By enforcing standards, and being able to analyze and document data elements, organizations can better understand and utilize their data, reduce redundancy, and build consistency.

BUSINESS AND TECHNICAL REQUIREMENTS (COBIT AI1, AI2.2, AND AI2.2)

Data modeling is a great way to capture end-user requirements and ensure that the design matches the organization's needs. With ER/Studio you can easily move from very high-level conceptual models to logical data models to platform-specific physical models and even auto-generate the necessary SQL or XML to create the desired schema.

As the scope of data modeling projects grows, so does the project complexity and overhead needed for coordination and quality control. ER/Studio Repository offers a sophisticated means to help stabilize this potential management nightmare through a server-based model management system that allows real-time collaboration and notification from modelers working on data models down to the model object level.

EMBARCADERO CHANGE MANAGER: CONTROLLING DATABASE CHANGES

Embarcadero Change Manager offers database administrators and developers a powerful set of tools to simplify and automate the database change management lifecycle. Change Manager's schema compare and alter, data compare and synchronization, and configuration auditing capabilities report on database changes, roll out new releases, and pinpoint database performance problems that result from both planned and unplanned changes.

IMPLEMENTING SOX CONTROLS WITH CHANGE MANAGER

Change Manager enables you to use the following COBIT controls to comply with SOX:

- Manage Changes
- Install and Accredit Solutions and Changes
- Manage the Configuration

MANAGE CHANGES (COBIT A16)

Use Change Manager to capture archives and then compare live databases against those archives to track changes or diagnose problems in production. Simply schedule regular schema archives using the flexible object selection features to make sure you capture exactly what you need to track.

INSTALL AND ACCREDIT SOLUTIONS AND CHANGES (COBIT A17)

Schedule regular compare jobs to track schema and database configuration changes, then review the comparison reports. Reports can easily be forwarded to other systems such as a source code control system.

MANAGE THE CONFIGURATION (COBIT DS9)

Create a configuration baseline or take a snapshot of an existing database to create a "gold standard" baseline, and then compare other systems to this baseline. With the "compliance" setting, reports can be generated with pass/warn/fail designations and percentage compliant for each system assessed.

By comparing a live database to a schema or configuration "snapshot", administrators can quickly identify changes and correct problems in less time. By monitoring configuration settings, DBAs can ensure compliance with regulatory policies and performance standards, and maintain overall database performance and availability. With its synchronization capabilities, Change Manager can also easily correct schema and data changes that are out of compliance.

DBARTISAN: DATABASE ADMINISTRATION

Embarcadero DBArtisan, the leading cross-platform database administration tool, helps DBAs maximize availability, performance and security. DBArtisan's comprehensive graphical editors and wizards boost productivity, streamline routine tasks and reduce errors so DBAs can manage larger, more complex databases. DBArtisan supports all major database platforms allowing organizations to standardize on one solution.

IMPLEMENTING SOX CONTROLS WITH DBARTISAN

DBArtisan assists you in implementing the following COBIT controls:

- Performance and Capacity Planning
- Identity Management
- User Account Management

MANAGE PERFORMANCE AND CAPACITY (COBIT DS3)

DBArtisan Performance Analyst is perfect for DBAs who need more performance details. It provides intelligent database and OS diagnostic information and strong drill-down details to help you pinpoint the cause of performance degradation. It is a powerful client-side database monitor that runs inside the DBArtisan console, so you can fix any found performance problems within a few mouse clicks.

Capacity Analyst makes capacity planning easier and forecasting mechanisms allow you to predict when you'll run out of space. It lets you track key database metadata and performance metrics over time so you can perform trend analysis on key areas like database growth, object fragmentation, database I/O and session load.

Space Analyst contains sophisticated diagnostics to help you pinpoint all space-related problems in your database, as well as an intelligent reorganization wizard that can reorganize all or selected parts of your database.

IDENTITY MANAGEMENT AND USER ACCOUNT MANAGEMENT (COBIT DS5.3 AND DS5.4)

DBArtisan will also help you effectively establish and maintain database security throughout your environment. DBArtisan allows DBAs to manage users, roles, privileges and password security, and migrate accounts between the same or different database platforms. Because DBArtisan manages database security across platforms, you can take a consistent, simplified approach to security even in the most complex environments.

By providing a common, easy-to-use interface for all major DBMS platforms, DBArtisan boosts productivity, lowers costs, and simplifies database administration in complex environments.
DBArtisan automates and streamlines the day-to-day tasks of DBAs by providing a rich, intuitive feature set including utilities for schema, SQL, job, and data management. It enables DBAs to concurrently manage multiple databases from a single interface, creating dramatic productivity gains for both experienced and novice database professionals.

EMBARCADERO PERFORMANCE CENTER: 24X7 DATABASE MONITORING

Embarcadero Performance center is a 24x7 database monitoring tool that helps ensure database availability and performance throughout the enterprise. Customizable alert thresholds, notifications and escalation paths let administrators access historical performance analysis data as well as identify and diagnose problems occurring in real-time. The Performance Center "Health Index" provides a single, at-a-glance, indicator that shows the overall performance level of every monitored database.

IMPLEMENTING SOX CONTROLS WITH PERFORMANCE CENTER

Performance Center assists you with the following controls:

- Define and Manage Service Levels
- Monitoring and Reporting
- Identify and Allocate Costs

DEFINE AND MANAGE SERVICE LEVELS (COBIT DS1)

Performance Center also offers detailed performance reports that are highly customizable for different audiences including CIOs, IT managers as well as business unit managers for assessing SLA and performance requirements.

The Embarcadero Health Index is a single indicator that communicates the overall performance level of every monitored database. By sampling critical statistics such as memory, I/O, contention, space, network, objects, users, and SQL, Performance Center quickly determines a database's complete performance picture. You can customize each database's Health Index, establishing individualized thresholds and measurements that apply to each unique database scenario.

MONITORING AND REPORTING (COBIT DS3.5)

Database professionals need clear and concise methods to ensure the viability of every database they manage. Performance Center helps DBAs spot performance issues impacting an organization's bottom line. In real-time, DBAs can observe IBM® DB2® LUW, Microsoft® SQL Server, Oracle®, and Sybase® databases in a single view to see how databases are performing at any point in time. DBAs can then quickly drill down into every detail of a database's performance to determine the root cause of any response problems.

With 24x7 coverage issues are detected in real-time—before they threaten a database's health. DBAs can initiate an unattended, "lights out" monitoring schedule for early problem detection and notification. Blackout schedules will prohibit threshold checking during busy periods. You can also directly embed a stored procedure for dynamic stop-and-start data source monitoring into nightly backup scripts.

IDENTIFY AND ALLOCATE COSTS (COBIT DS6)

Performance Center's flexible reporting has specific fields to provide the information necessary for allocating database usage back to business cost centers.

EMBARCADERO TOOLS SOX COMPLIANCE

COBIT controls are also used to determine whether the tools that you use are also SOX-compliant. The COBIT controls most applicable to database tools are:

- Application Security and Availability (AI2.5)
- Configuration and Implementation of Acquired Application Software (DS5.3)

- Identity Management (DS5.3)
- User Account Management (DS5.4)

Most Embarcadero database tools are client-side only, running on Windows desktops. This means that they rely entirely on the O/S controls (like Microsoft Word for example), which is outside the scope of this document. For best practices in O/S security, we recommend the Center for Internet Security's benchmarks (http://www.cisecurity.org/bench.html) or the Department of Defense's DISA Security Technical Implementation Guides (http://iase.disa.mil/stigs/index.html). In addition, Embarcadero's Database Gear products require database access, relying on the access controls and user management in place for the databases being accessed.

PERFORMANCE CENTER SOX COMPLIANCE

Performance Center is a server-side tool that does not require installation of agents on the monitored databases. Performance Center includes role-based access control to restrict who can manage the Performance Center repository. From there Performance Center relies on the database controls of the monitored databases.

ER/STUDIO SOX COMPLIANCE

When analyzing product compliance with Sarbanes-Oxley, it is also important to remember the scope of the regulation. SOX only applies to systems affecting financial statements, so with a few exceptions, ER/Studio is not likely to be in scope because it deals with data models rather than directly changing production databases that affect financial statements. However, different organizations have different interpretations of what is in scope, so this section describes ER/Studio's security features.

ER/Studio is offered under several configurations. The desktop version falls under the security model described above. But for collaboration, searching, building an enterprise data dictionary, and leveraging metadata, a centralized repository is needed. This introduces the need for access controls. As stated above, each organization will have their own specific parameters for third party applications; here are the configuration options for ER/Studio Enterprise:

- Role-based access control specifies which objects (models, projects, data dictionary, etc.) a user can access and what levels of access that user has (view, modify, delete, etc.)
- Account management features allow administrators to easily create, modify, deactivate, reactivate, and delete users

SUMMARY

Sarbanes-Oxley requirements for IT controls are extensive and wide-ranging, but no matter what aspect of database management or what database platform –

Embarcadero has you covered. And you can rest assured that your existing desktop and database access controls will secure your use of Embarcadero's tools for enforcing data standards, managing changes, and administering users and other database security controls, proper performance and capacity planning, and meeting SLAs.

ABOUT EMBARCADERO

Embarcadero Technologies, Inc. is a leading provider of award-winning tools for application developers and database professionals so they can design systems right, build them faster and run them better, regardless of their platform or programming language. Ninety of the Fortune 100 and an active community of more than three million users worldwide rely on Embarcadero products to increase productivity, reduce costs, simplify change management and compliance and accelerate innovation. The company's flagship tools include: Embarcadero® Change Manager™, CodeGear™ RAD Studio, DBArtisan®, Delphi®, ER/Studio®, JBuilder® and Rapid SQL®. Founded in 1993, Embarcadero is headquartered in San Francisco, with offices located around the world. Embarcadero is online at www.embarcadero.com.