Data Governance, Inc.

Mainframe Compliance – the Unspoken Sarbanes-Oxley Problem

by Gwen Thomas

Because of the need for Sarbanes-Oxley compliance, certain manual IT processes that were considered acceptable in the past are now seen as too high-risk. They are being replaced by lower-risk, automated processes that map to formal control frameworks. This paper describes a low-risk, automated alternative for mainframe compliance.

Sarbanes-Oxley Section 404 compliance requirements apply to all IT systems that handle financial data, including mainframe databases. But not much has been written about mainframe compliance. Why? Because members of compliance teams may not have been aware of a good solution.

The Problem

Most large public companies use mainframe databases. The databases may be attached to legacy applications, SAP, PeopleSoft, or other systems. Usually there are multiple copies, since IT needs exact copies for testing, business intelligence, development, data warehouses, or other purposes.

Making a copy isn't hard, but the copy isn't usable until it is given a unique name. Then, hundreds or even thousands of database pointers must be updated. The traditional process for making the copy usable is manual and can take up to two days.

Unfortunately, each step is a potential point of error: updates can be overlooked, and typos can slip through and not be detected. The database may operate even with some errors, and the application using the database may even return correct data for some transactions, even though other problems still exist.

Sarbanes-Oxley Compliance

Passed in 2002 as a response to corporate financial scandals, the Sarbanes-Oxley Act (SOX) requires changes in corporate governance that affect corporate boards, executives, internal and external auditors, and others in the company that deal with financial data. Section 404 requires that CEOs and CFOs, under the threat of civil fines and even imprisonment, attest to the adequacy of controls over financial data across the organization. These controls must be in line with industry standard frameworks. As a result, certain manual IT processes that were considered acceptable in the past are now seen as too high-risk and are giving way to lower-risk, automated processes that map to formal controls.

In the past, the company may have been willing to accept the risk that errors were introduced during the copy process. But Sarbanes-Oxley has raised the stakes. Section 404 means that the company CEO and CFO must acknowledge risks and attest that controls are in place to manage them.

The Bottom Line

Traditional, manual processes used to copy mainframe databases are missing controls to prevent the introduction of new issues. However, Sarbanes-Oxley (SOX) compliance requires that controls be in place somewhere in the company. If controls aren't in place in the IT department to prevent a problem, they must be in place in Finance or other groups to detect the problem later.

SOX compliance is forcing companies with mainframe databases to make a choice: They can implement extensive, expensive downstream processes and controls to detect whether their manual database copy process has introduced new errors, or they can skip these processes and hope they don't fail their Sarbanes-Oxley (SOX) Section 404 audit because of the omission.

Rising Costs of Compliance

Why hasn't the seriousness of this issue been written about? Most auditors have long been aware of mainframe compliance and database compliance challenges. However, automated tools have not been available. Auditors and DBAs have had to factor these expensive, time-consuming processes into the cost of initial SOX compliance. They've had to warn management that these costs will affect future IT and auditing budgets, since SOX compliance is ongoing.

Executives Are Making the Choice

Today's CEOs and CFOs are getting more involved in IT decisions, since they personally face financial and legal consequences for noncompliance.
Sarbanes-Oxley Section 404 requires that they attest that adequate controls over financial data exist throughout the enterprise.

No executive wants to hear that what's standing between them and a jail cell is a complicated, manual process with few or no preventative controls. They want to be able to make informed decisions between all alternatives. Often, they see reducing risk through automation as an important compliance strategy. Savings to IT departments is an added benefit.

Today, decisions whether to automate manual processes may be made in executive offices rather than in IT departments.

An Automated Alternative

A mature, proven alternative for mainframe compliance does exist. ComplianceCopy, offered by ESAI, is based on existing technology currently in place in Fortune 500 companies, domestically and internationally. IT departments have purchased the technology based on its ability to ease time demands on stressed IT resources, since it reduces data availability time from days to minutes. Now it is solving problems for compliance departments looking for automation and controls.

ComplianceCopy – An Automated Alternative for Mainframe Databases

A mature, proven alternative for mainframe compliance exists. ComplianceCopy, offered by ESAI, is an out-of-the box solution based on existing technology currently in place in Fortune 500 companies, domestically and internationally. IT departments have purchased the technology based on its ability to ease time demands on stressed IT resources, since it reduces data availability times from days to minutes. Now it is solving problems for compliance departments looking for automation and controls.

ComplianceKit

ComplianceCopy is packaged with ComplianceKit materials designed to assist internal compliance groups with SOX 404 attestation efforts. These include a mapping of key ComplianceCopy control points to the COBIT framework and the COSO framework, which are the defacto standards for Sarbanes-Oxley compliance. Also included are suggestions for integrating the tool into the company's:

- Information Life Cycle Management policies, standards, and processes
- Software Development Life Cycle policies, standards, and processes
- Testing and Quality Assurance policies, standards, and processes
- Software Change Management policies, standards, and processes
- Data governance policies, standards, and processes.

ComplianceKit for ComplianceCopy also comes with reusable templates and checklists that can be employed by IT to help document and prove their ongoing mainframe compliance and database compliance efforts. They can be used for multiple compliance initiatives: Sarbanes-Oxley, Basel II, HIPPA, U.S. Patriot Act, and others.

Gwen Thomas is a Principal with Data Governance, Inc. She's helped numerous Fortune 500 companies implement governance and compliance in the areas of structured data, unstructured content, and meta data. She's also the editor of SOX-online, the world's largest vendor-neutral Sarbanes-Oxley Site.

Visit SOX-online at www.sox-online.com or contact Gwen at gwen.thomas@sox-online.com. You can call her at 321-438-0774.

Enterprise Systems Associates, Inc. (ESAI) is a leading provider of complete infrastructure solutions for medium to large IT organizations, providing support at the strategic, tactical and pragmatic levels. They provide enterprise tools, SOX tools, and professional services.

Visit the ESAI website at http://www.soxtools.com, or call them at 1-877-SOX-TOOLS or 1-877-769-8665.