Data Governance, Inc.

What Execs Must Know About Sarbanes-Oxley Mainframe Compliance

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. Mainframe compliance and database compliance have always been expensive and hard to prove. This paper describes a low-risk, automated alternative.

As a Business or IT executive, you've learned a lot about Sarbanes-Oxley Section 404 compliance requirements. You know these requirements apply to all IT systems that handle financial data, including mainframe databases.

You already know:

- You need to have a Section 404 audit.
- This will require a certain amount of testing.
- Your testing must be compliant.
- Aside from compliance, you can't let this testing affect your business – that is, a failed test can't bring your production systems down.

What You Need to Find Out

Here's what you need to ask:

- How many mainframe databases are at your company?
  They're attached to legacy applications, SAP, PeopleSoft, or other systems.
- How many copies of each database exist?
  IT needs exact copies for testing, business intelligence and reporting, development, data warehouses, or other purposes.
- How often are copies created?

And here's the really big question…

- Can your IT department guarantee that copies are exact?

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.

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. Traditionally, this is a manual process that takes up to two days.

Unfortunately, each step in this manual process is a potential point of error: updates can be overlooked, and typos can slip through and not be detected.

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. Controls must be in place somewhere in the company – either controls in the IT department to prevent an error, or other controls in Finance or other groups to detect the error later.

If it hasn't happened yet, expect your CIO to ask you to make a choice between three options:

1. Authorize extensive, expensive processes to detect data errors
2. Skip these processes and hope the company doesn't fail its Sarbanes-Oxley (SOX) Section 404 audit because of the omission
3. Spring for a mainframe compliance tool to automate the database copy process.

What You Need to Know About Mainframe Compliance and Segregation of Duties

You've probably heard a lot about Segregation of Duties. Sarbanes-Oxley guidance issued by the government continues to stress its importance. It means duties are divided, or segregated, among different people to reduce risk of error or inappropriate actions. No one person has control over all aspects of any financial transaction.

The reasoning is sound: it's a deterrent to certain types of internal fraud and collusion if a single individual is not allowed to perform tasks that could contribute to fraud and also those that could cover it up.

But what about IT? You need to ask whether your IT department has single-person coverage of key mainframe databases. If they do, what are they doing to achieve mainframe compliance, short of adding staff?

Ask whether they're automating tasks where possible. If they are, when the company has pairs of tasks that fall under Separation of Duty requirements, at least one of the pair can be handled by IT staff other than your mainframe expert.

Many executives are seeing the reduction of risk through automation as an important compliance strategy. Added benefits are savings to IT departments and IT staff that have more time for value-add activities.

What You Need to Know About Mainframe Compliance and Change Management

Once your Auditors have "blessed" a system or database as being Sarbanes-Oxley compliant, it will be up to IT to avoid doing anything to take it out of compliance. You can't expect your IT department to stop making copies of mainframe databases. But you can expect them to support compliance through rigorous Change Management.

Your company is probably re-examining its definition of IT Governance and its relationship to Security, Risk, and Compliance. In the past, some IT services such as Change Management may have been limited in scope. Expect your CIO to suggest expanding their scope to ensure ongoing Sarbanes-Oxley compliance.

ComplianceCopy – An Automated Alternative for Mainframe Databases

A mature, proven alternative for mainframe compliance exists. 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 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.