Data Governance, Inc.

Sarbanes-Oxley Compliance Teams: Four Discussions You Need to Have About Mainframe Databases

by Gwen Thomas

Because of the need for Sarbanes-Oxley compliance, companies may not be able to accept the risk associated with certain manual IT processes. These processes are being replaced by lower-risk, automated processes that map to formal control frameworks. This paper describes mainframe compliance trends that affect compliance professionals.

As a member of your company's Sarbanes-Oxley (SOX) Compliance team or audit staff, you're helping your CEO and CFO prepare for their Sarbanes-Oxley Section 404 Attestation. Since SOX requires that the controls used by execs must be in line with industry standard frameworks, they're counting on your team to help ensure the right compliance frameworks and controls are used. They're trusting that any attestation-related testing won't bring down the company's production systems. You're involved in research, analysis, and the facilitation of numerous discussions between management, IT, and auditing. Here are four such conversations you should have.

1. The "Mainframe Database Compliance" Discussion

How many mainframe databases does your company have? 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.

> Can IT promise that copies of mainframe databases containing financial data are exact copies?

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.

The process is tedious and boring. Each step is a potential point of error, and it would be possible for errors to slip through undetected. There's no easy way to check all your steps, so IT assures you that they're very, very careful when they do this. Even so, they can't promise you that what they've created are exact copies of the originals.

In the past, the IT department may have been willing to accept the risk that errors were introduced during the copy process. But Sarbanes-Oxley has raised the stakes. Since Section 404 means that the company CEO and CFO must acknowledge risks and attest that controls are in place to manage them, they're expecting to provide input into the levels of risk they're willing to accept.

They're also expecting you to provide expertise. They're looking to you to spell out their alternatives. Here are the alternatives for mainframe compliance for database copying:

1. Keep the manual processes and hope the company doesn't fail its Sarbanes-Oxley (SOX) Section 404 audit because of lack of controls.
2. Implement extensive, expensive downstream processes and controls to detect data errors.
3. Implement a mainframe compliance tool to automate the database copy process.

These days, you and your execs may be considering automation as an important compliance strategy. If the automation tool saves money for IT, frees IT staff from a tedious, boring task, or allows them to create new copies more often – those are added benefits.

2. The "It's Not Enough" Discussion

If they don't already realize it, it might be up to you to inform the IT Department that the Wild West Days of IT are over. They need to understand that in the post-Sarbanes-Oxley world, it's not enough to just 'do' IT tasks – even if they're successful and everything works as designed. Now, it's necessary to Control it, Do it, Document it, and Prove it.

Is IT ready to:

- Control a process
- Do it
- Document it
- Prove compliant processes were followed?

You may have to explain what adequate controls look like. You'll no doubt be involved in setting standards for documenting control and audit activities. You'll help your company organize and store records to prove that compliance steps have been taken.

IT may ask for guidance for non-automated tasks. One approach may be to document processes and to complete detailed reports or checklist each time the task is completed. This could produce auditable proof that risks were acknowledged, controls were in place to manage the risk, and these controls were actually executed.

Your IT Department might tell you it would take longer to document the completion of a task than to perform it, creating an undue burden. You'll want to ask questions:

- Does the task involve tedious and repetitive non-value-add work?
- Is it a lengthy, manual process with multiple points of error?
- Does an automated alternative exist?

Automated solutions may have been rejected in the past, it they were evaluated merely on ROI within a small group. You may be asked to help reframe the value statement to include compliance criteria.

3. The "Segregation of Duties" Discussion

Sarbanes-Oxley guidance issued by the government stresses the importance of Segregation of Duties. You may be asked to help explain how duties can be divided, or segregated, among different people to reduce risk of error or inappropriate actions. You may have to describe the flow of financial processes, clarifying roles and ensuring that no one person has control over all aspects of any financial transaction.

How is IT maintaining segregation of duties for systems and databases with single-person coverage?

But what if your company has single-person coverage of key mainframe databases? Short of hiring extra staff, what can be done to achieve mainframe compliance?

You may need to recommend the automation of tasks where possible. That way, when IT has pairs of tasks that fall under Separation of Duty requirements, at least one of the pair can be handled by someone other than the mainframe expert.

4. The "Change Management" Discussion

Is the scope of IT Change Management adequate?

Once a system or database has been deemed Sarbanes-Oxley compliant, it will be up to IT to avoid doing anything to take it out of compliance. You may need to encourage IT to broaden the scope of its Change Management efforts. They may be used to focusing on newer systems, using less formal processes to manage legacy systems and mature databases. You may need to remind them that all systems and databases are included in compliance requirements – including mainframe systems and databases.

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 time 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.