Sarbanes-Oxley and Mainframe Compliance: What Database Professionals Need to Know

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 mainframe compliance trends that affect database professionals.

You've been working with mainframe databases for how long now? Forever, it seems. You know your stuff. You could do it in your sleep. But don't get too settled, because Sarbanes-Oxley Act compliance might require you to "fix" how you do some things – even if they don't appear to be broken.

Why? The Sarbanes-Oxley Act of 2002 (SOX), which was passed as a response to corporate financial scandals, requires corporate governance changes that affect many roles in publicly traded companies: corporate boards, executives, auditors, and others who deal with financial data. Section 404 of the act 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.

As a result, execs are paying more attention to financial processes and the IT systems and processes that touch financial data. Since SOX requires that the controls used by execs must be in line with industry standard frameworks, company Sarbanes-Oxley compliance teams are working to define what "adequate controls" look like.

What does this have to do with mainframes and database professionals? Following are five things you need to know about how SOX could affect you:

1. You may need to change processes – even if they're not broken.
2. It's no longer enough to "do" IT
3. It's all about Segregation of Duties
4. Ongoing Sarbanes-Oxley compliance requires vigilant Change Management
5. Justifying IT costs just might be easier.

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.

1. The Need to Change Processes

To be compliant, Business and IT processes that deal with financial data must have controls to manage data-related risk. Controls to prevent problems are preferred, but it they're not in place, the company will have to compensate by having downstream controls to detect problems later.

If your compliance team has not yet talked to you about how you do your job, they will. Be prepared: they might not like your answers. Why? What was acceptable IT practice last year may be seen as unacceptable from a compliance viewpoint.

Here's an example:

> *You work with the mainframe databases for your mainframe applications, SAP, PeopleSoft, or other systems. You regularly create new instances for testing, business intelligence, development, data warehouses, or other purposes. The copy isn't usable until it is given a unique name and is updated to be addressable. The traditional process for making the database copy usable is manual, and it can take up to two days.*
>
> *The process is tedious and boring, but you have to be alert, since 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 you're very, very careful.*
>
> *This has always been acceptable IT practice. But Sarbanes-Oxley has raised the stakes. Your compliance team won't want to tell your CEO and CFO that what's standing between them and a jail cell is a complicated, manual process with few or no preventative controls. Instead, they'll want to be able to offer alternatives.*
>
> *What are the alternatives to a manual database copy process without preventative controls?*
>
> 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, your execs may be considering automation as an important compliance strategy. If the automation tool saves money for IT, or frees you from a tedious, boring task, or allows you to create new instances more often – those are added benefits.*

2. It's Not Enough to "Do" It

Forget the Wild West days of IT. In the post-Sarbanes-Oxley world, it's not enough to do IT tasks – even if they're successful and everything works as designed.

Yes, you're a skilled profession, and auditors will recognize this – to some extent. Still, in the new world of compliant processes, you need to Control it, Do it, Document it, and Prove it.

The bad news: You may be asked to help create detailed processes for your non-automated tasks. You may be asked to complete detailed reports or checklist each time you complete the task, so there's auditable proof that risks were acknowledged, controls were in place to manage the risk, and these controls were actually executed.

The good news: If this means it might take longer to document a task than to perform it, and if this is an undue burden, then your management and compliance teams will probably be ready to explore alternatives with you. 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?

Let them know. Even if the proposed automation solution has been rejected in the past, it may be approved now that compliance criteria are in play.

3. Segregation of Duties

Sarbanes-Oxley guidance issued by the government stresses the importance of Segregation of Duties. This 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 if you have single-person coverage of key mainframe databases? Short of hiring extra staff, what can you do to achieve mainframe compliance?

Automate tasks where possible. That way, when you have pairs of tasks that fall under Separation of Duty requirements, at least one of the pair can be handled by someone other than your mainframe expert.

4. Vigilant 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 expect Change Management efforts in IT to broaden in scope and become more compliance focused. Back to our mainframe example:

> *Suppose your auditors have looked at your mainframe database and believe it's in good shape from a compliance viewpoint. But now you need another instance – for testing, reporting, to support an application in development, or for other purposes. You know the traditional, manual method is designed to create an exact copy, and the person making the copy usable will do a good job, if they don't die of boredom in the process. But there's no way to absolutely guarantee they've created an exact copy, since controls to prevent mistakes just don't exist. Strictly speaking, to solve the compliance problem, your auditors might expect the person doing the task to document every step, then have someone else come behind them, verifying every key stroke.*
>
> *This seems pretty extreme for a tedious, repetitive task. On the other hand, if this process of copying a mainframe database and making it usable were automated, then Change Management would be simplified. Change Management documentation would be easy. IT would be happy, because the new database would be ready in minutes rather than days. And Compliance would be happy, because the copy would be guaranteed to be an exact copy of the original.*

5. Justifying IT Costs

You're probably used to having to justify IT expenses on an ROI basis. You may even have a wish list of IT solutions you haven't had been able to purchase because you couldn't justify their expense based on IT gains alone.

Sarbanes-Oxley may have changed the equations used by decision-makers in your company. Look at the items on your wish list again. Will they remove risk for the company? Will they replace error-prone manual processes with error-free, automated processes? Will they introduce preventative controls and free the company from the burden of downstream error detection and correction? Will they introduce easy-to-document, easy-to-prove controls? Will they help you CEO and CFO sleep easier at night?

If so, draft a new business case that includes these factors. It might get you a new solution. At the very worst, you'll have demonstrated an instance of Business – IT alignment.

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.