MAINSTAR

Achieving z/OS Sarbanes-Oxley Compliance with SYSchange

By Michael Madani

Impact of the Sarbanes-Oxley Act on Today's Organizations

Since the Sarbanes-Oxley Act was passed in July 2003, corporations both public and private have conducted a wrenching self-examination of the integrity and auditability of their systems and application software. Under the Act, companies must take every measure to prevent loss of service, avoid data loss, reject unauthorized change, and improve the overall security of their systems software. CEOs and CFOs are now held responsible for the accuracy of their change control processes and audit reporting capabilities, so they'll be breathing down the necks of their subordinate managers and administrators more than ever to ensure that their systems are secure from unauthorized changes and can produce accurate audit reports on demand. This is true even for outsourced data centers, since the owners are still under the jurisdiction of this Act and are just as liable for compliance as before. 'Best Practices' and paper audit trails cannot adequately achieve these goals; specialized software solutions are needed to control changes and provide an audit trail of change activities.

According to a survey by AMR Research Inc., $2.5 billion dollars were spent in 2003 alone on projects and software to help ensure compliance with the requirements of the Sarbanes-Oxley Act. Clearly, concerns about data security, integrity, audit reporting capability, and business continuity readiness are now some of the top priorities for data centers. A recent Gartner Group survey found that 80% of businesses without a verified disaster recovery plan went bankrupt within one year of suffering a significant data loss. Traditionally, only large corporations had the financial and technical resources to properly address these issues. Small and medium enterprises often lack the capital or expertise to successfully manage a comprehensive disaster recovery solution and thus are often not well protected.

How SYSchange Helps

With **SYSchange** deployed on your z/OS systems, compliance with the Sarbanes-Oxley Act need not be a daunting task. **SYSchange** provides cost-effective systems software protection for large, medium, and small businesses with a streamlined and accountable process for safely introducing system software changes. **SYSchange** is easy to learn, and offers many powerful functions for addressing the mandates of the Sarbanes-Oxley Act.

Objectives for Organizations	SYSchange Solution
Auditability: The ability to globally audit.	Running transparently in the system, the **SYSchange** Started Task (STC) records all change activities occurring in the system, as well as any activities conducted by a **SYSchange** Administrator. The STC assures organizations that no unauthorized changes are allowed and that any allowed changes are recorded. Changes are logged in a Control File and can be audited online at any time.
Security: The ability to identify and control changes even at member-level.	With **SYSchange,** critical systems assets (libraries) can be protected with the LOCK=YES feature, which automatically rejects any unauthorized attempts to introduce changes to the library.
Availability: Improved overall systems availability with minimal downtime.	**SYSchange** provides the ability to use Restore Packages and to pinpoint backup member versions for online recovery, resulting in less downtime for your systems.
Reduced Costs: Minimal human resource involvement with maximal automation.	**SYSchange** is the first truly affordable and innovative change management software for z/OS, offering the highest levels of automation and transparency; **SYSchange** requires minimal installation and learning overhead, and has no impact on existing methodologies.
Improved Asset Management: Translates to more secure systems and higher customer confidence levels.	With **SYSchange**, your organization's assets will be protected, and changes will be verifiable and recoverable. Application software and systems software integrity will be dramatically improved. This translates to less downtime, increased customer confidence, and greater ROI.
Introduction of Non-standard Changes: Certain types of changes (such as zapping a load library) occur outside of change management products. These changes are harder to detect and often go unnoticed at organizations' expense. Organizations seek solutions that are capable of addressing this type of vulnerability as well.	With **SYSchange**, even non-standard changes can be detected. Using SYSchange Tokenization technology, standard and non-standard changes introduced to large software environments are both identifiable.

Objectives for Organizations	SYSchange Solution
Identifying Changes (Multiple LPARs:) Organizations usually have multiple LPARs. These organizations need a reliable and efficient method for ensuring that these differing environments are at the same level of software at all times.	**SYSchange** is able to compare local or remote environments, even if they are not connected in any way. Using Tokens as the representation of the base (gold) environment, the software at several different LPARs can be verified for integrity, and differences are quickly identified. This same technique can be used to ensure that a disaster recovery site is at the same level as a production site.
Process for Change Propagation: Today's complex environments undergo regular changes. At the end of a certain cycle, a tool is sought which can quickly package only the changes and propagate them to other systems, local or remote.	**SYSchange** provides the MODS identification and packaging feature to address this need. The MODS identification first identifies what changes have occurred to your environment over a certain time period. The MODS Packaging feature then quickly packages all the changes that have occurred on your system, and makes the Change Package ready for distribution to other systems. **SYSchange** goes a step further by providing the flexibility of building your own Custom Package which can be used to transfer only those components you wish to transfer.

Conclusion

SYSchange is the first truly robust and affordable systems software change management solution for z/OS, helping you achieve Sarbanes-Oxley compliance on your z/OS systems. **SYSchange** goes beyond the basic requirements by providing flexible functions that automate everyday tasks.

With the STC running, data centers can be assured that their critical assets are protected around-the-clock. By rejecting unauthorized changes, the STC is able to ensure the highest levels of integrity, recoverability, and auditability for your systems. Even non-standard changes will be identifiable using **SYSchange** Tokenization technology. Since the STC is 'aware' of all change activities in the system, any time a change is introduced to a protected library component, the member is automatically backed up with a system-generated (or user-supplied) descriptive comment for easy problem resolution in the future.

In addition to providing a more automated and proactive change management solution with audit reporting capabilities, **SYSchange** replaces traditionally manual change management tasks with more automated and reliable ones. Ultimately, the benefits offered by **SYSchange** translate to higher productivity, higher customer satisfaction, reduced risks, and a higher return on investment for your organization.

Michael Madani – Pristine Software
Michael Madani is the Founder and Chief Architect at Pristine Software. Pristine has provided corporations around the world with leading-edge software solutions, with a focus on Automating System Software Change Management, since 1989. Michael's career has spanned more than 25 years in mainframe software development.