

# Business Issues

## White Paper

From Mainstar Software Corporation



## Understanding Sarbanes-Oxley for z/OS

*By Colleen Gordon*

Even though the Sarbanes-Oxley (SOX) Act was passed in 2002, the implications are just beginning to trickle down to Systems Programmers and Storage Administrators in IT organizations across the US and abroad. The Act, written by Paul Sarbanes (D-MD) and Michael Oxley (R-OH), is officially referred to as the Public Company Accounting Reform and Investor Protection Act of 2002. It was signed by President Bush on July 30, 2002.

The SOX Act came about as a direct result of corporate failures of the past decade in which there were significant internal control failures associated with fraudulent financial statements. Section 404 of the Act specifically addresses IT controls and is just one part of a comprehensive set of requirements that includes the development of disclosure committees, certification of financial statements by both the CEO and CFO, the development of more financially literate and responsible audit committees, increased independence of the external auditor, and the implementation of fraud risk management processes. The legislation formed a new audit standards committee called the Public Accounting Oversight Board (PCAOB) to set auditing standards for public companies.

Hundreds of laws and regulations currently impact IT, but the SOX Act has by far the most direct impact upon IT departments responsible for acquiring, implementing, and managing infrastructure software. To date, Section 404 of the SOX Act has been the subject of hundreds of articles addressing the implications on IT departments and CIOs. This paper discusses the implications of the SOX Act, specifically Section 404, for z/OS Systems Programmers and Storage Administrators.

The internationally accepted set of guidance materials for SOX Section 404 is the IT Control Objectives for Sarbanes-Oxley (COBIT) written by the IT Governance Institute ([www.itgi.org](http://www.itgi.org)). Since IT systems are used to generate, change, house, and transport data assets, CIOs must build controls that ensure the information stands up to

audit scrutiny. They must now take on the challenges of enhancing their knowledge of internal control, understanding their organization's overall SOX compliance plan, developing a compliance plan to specifically address IT controls, and integrating this plan into the overall SOX compliance plan.

The COBIT document emphasizes that the SOX Act not only requires senior management and business process owners to establish and maintain adequate controls, but also requires them to assess their effectiveness on an annual basis. In addition, the business's annual report must contain a statement signed by the CEO and CFO attesting that the information contained in any SEC filing is accurate. The company must also submit to an audit to prove it has controls in place to assure the information is accurate. The cost of non-compliance can be devastating to an organization in terms of stock price and can even result in prison terms.

---

### Why the Need for IT Controls?

The work required to meet the requirements of the SOX Act should be regarded as an opportunity to establish better controls designed to ensure availability, accountability, and responsiveness to business requirements. As an analogy, consider an automotive repair shop. What ultimately matters is the quality of the repair job, but no responsible repair shop would allow themselves to be evaluated based solely on the credentials of the repair technician; they would also want to operate in a clean, orderly environment, provide quality parts and repair equipment, and deliver their product when promised. If the shop does not meet all of these requirements, why would anyone want to take their car to that shop for repairs? This is especially true in IT when failure means multi-million-dollar fines, ruined reputations, and possible prison terms for top executives.

Controls over the z/OS operating system, database management, and storage environment

are necessary to support the applications that depend on computer processes. When management realizes the cost of compliance with the SOX act, there will be an increased focus on automated controls. Why use a manual process to identify critical data assets for backup when an automated solution can do it more efficiently and accurately?

---

## **Service Level Agreements**

The process of defining and managing service levels addresses how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of the business. Roles and responsibilities are defined and an accountability and measurement model is used to ensure that services are delivered as required and that the environment is resilient to system outages. Deficiencies in this area can significantly impact financial reporting and disclosure of an entity. For instance, if systems are poorly managed or system functionality is not delivered as required, financial information may not be processed as intended.

IT management must ensure that before selecting a third party for IT processing, they thoroughly assess the third party's ability to deliver the required services and review their financial viability. Companies using a third party service must assess the risks, examine security controls and procedures, and regularly review security, availability, and processing integrity.

---

## **z/OS System Software**

To satisfy the demands of the SOX Act, most z/OS IT organizations will require significant changes. Enhancements to systems and processes will be required, including the design, documentation, retention control, and evaluation of the IT controls put into place. IT organizations must take a proactive approach to controls in the areas of computer operations, access to programs and data, program development, and program changes. These include controls over:

- The definition, acquisition, installation, configuration, integration, and maintenance of the z/OS infrastructure
- Day-to-day delivery of information services
- Service Level Agreement management
- Management of third party services
- System availability

- Customer relationship management
- Configuration and systems management
- Problem and incident management
- Scheduling
- Facilities management

The system software component includes controls over:

- Effective acquisition, implementation, configuration, and maintenance of operating system software, database management systems, communications software, security software, and infrastructure utilities that allow applications to function.
  - System software that provides incident tracking, system logging, and monitoring functions.
  - Software that reports on the use of utilities and powerful data altering functions to record their use.
- 

## **Data Access and Storage**

Access controls over programs and data is of great importance. Effective access controls and distribution of responsibilities can provide a reasonable level of assurance against inappropriate access and unauthorized system use. The SOX Act requires restricting privilege access only to authorized users that need them to do their jobs along with an appropriate division of duties, and frequent auditing of the user's activity. Furthermore, disgruntled or terminated employees should have their access revoked immediately to prevent unauthorized use of or change to the system.

Retention periods and storage terms need to be defined and documented for data, programs, reports, and messages along with the applications necessary to access the data. Management must implement a strategy for cyclical backup of data and programs. Procedures must exist to test the effectiveness and process of data restoration and the quality of the backup media. System event data must be retained to provide chronological information and logs to enable the review, examination, and reconstruction of system and data processing. System event data designed to provide reasonable assurance as to the completeness and timeliness of system and data processing must be retained and made accessible. Application software and data storage systems must be properly configured to provide

access based on the individuals demonstrated need to view, add, change, or delete data.

IT management must have established procedures to protect systems from unauthorized updates or access. Periodic tests must be performed to ensure that system software and network infrastructure is properly configured. IT must provide adequate audit trails for changes made to both system software, including infrastructure utility software and program changes. The problem management facility must have adequate audit trail facilities which allow tracing the incident back to the underlying cause.

---

## Program Development

The acquisition and implementation of new applications is an area with a high degree of failure. Often, these implementations are viewed to be outright failures as they do not fully meet the business requirements or customer expectations, or are not implemented on time or within budget. Standard software tools help IT departments develop methodologies and provide automation for system design, documentation requirements, testing, approvals, project management, and oversight. Application maintenance addresses ongoing implementation of new releases of software. Appropriate controls over changes to these systems should exist to ensure they are made properly and they can be reversed quickly should a problem exist. The change management process needs to be integrated with other IT processes including incident management, problem management, availability management, and infrastructure control.

---

## Mainstar's Solutions for SOX Compliance

### *z/OS System Software Changes*

To help IT organizations comply with the SOX Act and to provide for a resilient environment against system changes that have the potential to cause system outages, customers need automation to create 'before and after' copies of changes introduced into the environment.

Mainstar's **SYSchange** provides for a compliant, resilient z/OS environment by automatically backing up changed Partition Data Set (PDS) members of z/OS system and other key libraries. When a systems programmer changes a PDS member, a backup is immediately taken and stored in an inventory. Should the

systems programmer need to back out of that change for any reason, the backup is easily recovered. In addition, security can now be provided at the member level, allowing some systems programmers change authority to members or an entire PDS while others are not allowed. Furthermore, if an unauthorized or unscheduled change is made, **SYSchange** ensures that a backup is taken and audit information of that change is recorded. If the unauthorized change causes a problem, the change is easily identified and can be immediately backed out.

Upgrades to system software require a variety of changes to a number of key PDS members that support the operating system or utilities that are part of the system infrastructure. **SYSchange** provides packaging of multiple changes and scheduled implementation at a designated time. This packaging also provides for a complete back-out of all changes if necessary. Using **SYSchange**, accepted changes can be propagated to all other systems in the environment, including the recovery environment, to keep multiple systems in synchronization.

### *Data Availability*

The SOX Act describes the requirement for data availability as a strategy for cyclical backup of data and programs, and requires the documentation of procedures to test the effectiveness and process of data restoration and the quality of the backup media. In addition, there is renewed emphasis on resiliency to system or application outages requiring automated backup and recovery systems to augment data replication implementations.

Designed to provide a complete data asset backup and recovery system or to augment replication technologies such as IBM's Peer to Peer Remote Copy (PPRC) or Extended Remote Copy (XRC), Mainstar's backup and recovery solutions, including **ASAP** and **Backup & Recovery Manager Suite: ABARS Manager** and **All/Star** provide a truly resilient data asset protection program for the z/OS environment. These software solutions use automated processes that minimize setup and ongoing maintenance. **ASAP** identifies data assets used by applications and automatically maintains the list over time. IT organizations can use the automation **ASAP** provides to replace error-prone manual practices. **ASAP** uses reliable sources, such as System Measurement Facility (SMF) and data set records taken directly from the executing

job's job control language (JCL), to construct a list of all data assets utilized during execution. The list is then made immediately available to the backup system: either **ABARS Manager**, where all data belonging to that application is backed up as a single entity, or **All/Star**, where backups created within the application's batch execution can be directly compared with the **ASAP** generated list to ensure all data assets have a backup.

To provide for backup and restoration for IT data assets, **ABARS Manager** provides a backup and restoration system unique in many aspects. Built upon the DFSMSHsm data mover, Aggregate Backup and Recovery Support (ABARS), **ABARS Manager** can back up data from any level of the storage hierarchy, primary storage, migration level one (ML1), or migration level two (ML2) and from tape media, including virtual tape. Using this technology, all data belonging to an application can be backed up as a single entity called an aggregate. The data assets in the aggregate can be quickly recovered either individually or as an entire entity, such as in the case of recovering the application at an offsite location due to a catastrophic failure. In addition, each application having its unique aggregate can be recovered in a tier group fashion, from most critical to least. This methodology enables businesses to better meet recovery time objectives that are not so aggressive that they warrant replication and to meet the requirements of a truly resilient replicated environment in which data backups are easily accessible and data is quickly recovered.

**All/Star** completes the backup and recovery system management solution by providing an inventory of all backups performed by a variety of data movers within the data center. IT organizations that use **All/Star** now have visibility to all backups in their environment. This includes backups performed during the execution of production batch applications, full volume dumps, tape copies, and backups performed by DFSMSHsm, including **ABARS Manager** and ICF catalog backups performed by Mainstar's **Catalog RecoveryPlus (CR+)**. With all backups stored in one inventory database, **All/Star** can analyze all data in your environment and match that information to the inventory. The resulting report details all data assets in your environment that are not in the inventory or do not have a backup.

Without these types of facilities, IT organizations must determine what processes created the most recent backup and what utility was used to back it up, then create or modify

existing procedures to recover it. With no inventory of backups to reference, IT organizations may be unaware when a more recent backup copy exists, further jeopardizing their ability to recover from the loss.

Using **ABARS Manager** and **All/Star**, IT organizations can protect against data loss for replicated data, data housed on tape, and data in DFSMSHsm migration. If a replicated asset is destroyed or a miscompute produces incorrect results, you can quickly locate and recover from the most current backup copy quickly.

### ***DFSMSHsm Managed Asset Protection***

The IBM Data Facility Systems Managed Storage Hierarchical Storage Manager (DFSMSHsm) manages thousands of data assets, both critical and non-critical, in licensed IT environments. Like ICF catalogs, DFSMSHsm's Control Data Sets (CDSs) contain pointers to where data resides within the hierarchy, on primary storage or in ML1 or ML2. When these pointers become corrupted, data assets managed by DFSMSHsm become unavailable.

**HSM Reporter/Manager** and **FastAudit/390 Suite: HSM FastAudit** and **HSM FastAudit-MediaControls** are crucial to the health of the DFSMSHsm environment. These solutions audit the CDSs and automatically create corrective actions, including DFSMSHsm FIXCDS commands. The audit, corrective action, and reporting capabilities of these products enable customers to audit large DFSMSHsm environments and high-density tape media faster and more accurately.

### ***ICF Catalog Outages***

An ICF catalog outage can be a single point of failure in any z/OS environment, leading to hours of downtime for applications accessed through that catalog. For SOX compliance, IT organizations need utilities that help prevent system outages from occurring, and if they do occur, provide rapid recovery from backup. **CR+** provides a forward recovery command that recovers the catalog from backup and applies SMF records to bring the catalog current as of the last update. In addition, **CR+** enables the prevention of potential outages by executing catalog diagnostic commands on a regular basis. The **CR+** diagnostic command execution automatically creates corrective action commands to resolve known problems. These diagnostic commands also include the ability to check the integrity of the catalog structure itself and, in

many cases, fix known structural issues without the need to take the catalog out of service. **CR+** includes the capability to reorganize the ICF catalog while the catalog is open and active. This revolutionary functionality eliminates planned and unplanned catalog outages that have a negative impact on Service Level Agreements.

---

## Summary

IT organizations using Mainstar's business resiliency solutions in their environments found they were better equipped to meet the regulations in section 404 of the Sarbanes-Oxley Act regarding system change management, data asset protection, and recoverability. Mainstar's solutions provide for data asset management including: backup and recovery of changed data, PDS members and tape data including virtual tape, backup and audit of DFSMSHsm managed data, grouping backups of data assets by application, quick recovery in the event of data loss, and reporting on data sets that don't have a backup. In addition, customers reported they could proactively resolve issues that have the potential to cause an outage because the solutions provide performance enhanced alternatives to resource intensive preventative methods.

---

## References

*IT Control Objectives for Sarbanes-Oxley.* 2004. Rolling Meadows, IL: IT Governance Institute.

**Colleen Gordon – Professional Services Manager and SE Manager for Mainstar Software Corporation.**

*Colleen has an extensive background in Business Continuation and Storage Management and has worked with customers all over the world. Colleen is the co-author of the IBM Redbook, ABARS and Mainstar Solutions, and has written articles for Disaster Recovery Journal, Enterprise Systems Journal, and other industry magazines.*

Mainstar is a registered trademark and ABARS Manager, All/Star, ASAP, Backup and Recovery Manager, FastAudit/390 Suite, HSM Reporter/Manager, and Catalog RecoveryPlus are trademarks of Mainstar Software Corporation. SYChange is a registered trademark of Pristine Software.

IBM is a registered trademark of International Business Machines Corporation and the following terms are trademarks of International Business Machines Corporation in the United States, and/or other countries: DFSMSHsm, z/OS.