

Business Resiliency

White Paper

From Mainstar Software Corporation



Business Resiliency Solutions from Mainstar

By Colleen Gordon

Preface: Any IT organization can testify that creating a resilient environment is not easy. Businesses require a number of solutions to solve business resiliency issues. But what exactly does business resiliency mean in a z/OS environment and what are the issues? This White Paper looks at several of these issues including single points of failure within the infrastructure and describes how businesses who utilize replication technologies for high availability and/or business continuity can augment those implementations using Mainstar's business resiliency solutions. These solutions enable z/OS customer environments to be more resistant to all types of outages.

Business Resiliency

Business resiliency is a relatively new term describing the ability of businesses to prevent failure by proactively ensuring service availability as well as their ability to quickly recover in the event of a failure. The types of failures vary and include inadvertent errors, human or otherwise, resulting in data loss (deletion) or corruption. To plan for the prevention of outages as well as recovery methods, businesses must consider the z/OS system infrastructure, hardware, applications, and human resources within the context of business resiliency.

Because business resiliency includes both responses to failure and preventative measures, the scope of data availability ranges from the recovery from a catastrophic failure at an offsite location (typically known as disaster recovery), to prevention measures such as discovering and correcting underlying problems in the infrastructure that can lead to an outage. In addition, the need for *automated* data asset identification and backup and recovery solutions in the z/OS environment increases as the sheer quantity of data prevents effective use of traditional manual processes and procedures. When businesses cannot easily locate backups of critical data assets or when backups simply don't

exist, the resulting application outage can be costly in terms of missed service level agreements, fines, non-compliance, and a loss of customer satisfaction. In extreme cases such as an entire IT environment disaster, the entire business can be at risk.

Technology Drivers

The mechanisms that drive selecting the right solution for data availability are Business Impact Analysis (BIA) and Service Level Agreements (SLA) for the z/OS infrastructure and the applications it supports. The BIA is the industry standard used to identify data processing requirements for each business unit. The BIA is a controlled method for determining the organization's critical business processes including how these processes are conducted. Once these processes are fully understood, business continuation planners can determine the likely impact in terms of cost, customer service and resources that a disaster could have on the business. Important deliverables of the BIA analysis are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application. The RTO determines how quickly the data must be made available and the RPO determines how current the data must be. Applications that demand an aggressive RTO warrant costly recovery solutions using synchronous or asynchronous data replication technologies. These technologies replicate data to another location, usually some distance away, to provide a redundant copy for recovery purposes. These technologies reduce the recovery time of an application to seconds or minutes rather than hours. However, simply replicating data assets does not ensure a resilient IT environment. Data assets that become corrupted, deleted, or otherwise unusable will be replicated. For these applications to be truly resilient, additional backups must be performed and made available for quick recovery.

Single points of failure must also be identified

and mitigated for a more resilient environment. As an example, ICF catalogs house the pointers to where data assets are located in a z/OS environment. When a catalog becomes unavailable due to corruption, human error, hardware issues, or software errors, all application data housed in the catalog becomes unavailable to the online user or batch processing. Depending on the applications affected, this unplanned outage can cost a business, such as a large financial institution, millions of dollars due to lost transactions and the impact on customer loyalty and satisfaction. This is another example of how data replication can't help. Replicating ICF catalogs without first validating data integrity does not provide recoverability: you have simply replicated an unusable catalog.

Process Ownership and Compliance

Crucial to the success of business resiliency and regulatory compliance is the correct ownership of the IT organization's responsibilities including staff size and skill set requirements.

Ownership is an issue seemingly resolved by the Sarbanes-Oxley Act. Who owns the responsibility for IT controls including business resiliency? The CIO does! Since IT systems are used to generate, change, house, and transport corporate assets, CIOs must build the controls that ensure they stand up to audit scrutiny. CIOs must take on the challenges of enhancing their knowledge of IT internal controls. In addition they must lead IT in, developing a compliance plan, and integrating this plan into the business's overall compliance plan. Yet three years after the passage of this act, many IT managers are still waiting for the effects to trickle down to their level and don't know exactly what it will mean to their overall day-to-day operations.

Customers have reported that when ownership is not clearly defined, there is a tendency for staff to own only part of the responsibility or relinquish the responsibility entirely. Using IT recovery as an example of this, systems programmers tend to own the responsibility for the z/OS system and third party software, but none of the responsibility for the application data. This is especially true for the customers whose IT processing is outsourced: it is common to find that the responsibility for backup and recovery of the application data is not owned by the outsourcer. Application developers unclear about ownership tend to rely heavily on

backups taken by systems programmers. During recovery testing, they are often surprised at the latency of the recovered data – if it was backed up at all.

Continued growth without proper IT staffing and skill growth won't meet the needs of regulatory requirements outlined in the Sarbanes-Oxley Act. The Act increases demands for staffing to allow for proper distribution of job responsibilities. Businesses have found it difficult to comply with security, audit, and other requirements of section 404 of the Act without skilled staff to support the various job responsibilities. In addition, the inability for small staffs to proactively plan and prepare for potential outages hinders their ability to accomplish resiliency goals. Customers are realizing that decentralization of ownership for the identification, backup, and recovery of data assets doesn't work. A centralized approach, using automated solutions which identify data assets used by each application and provide for backup management using an inventory database, is needed to ensure resiliency and compliance with the Sarbanes-Oxley Act.

Mainstar's Solutions for Business Resiliency and Compliance

Prevention and the ability to quickly recover from a variety of outages is the key to a resilient z/OS environment. To achieve this goal, a number of IT infrastructure solutions are required and Mainstar Software Corporation, established in 1978, provides software solutions across all industries.

ICF Catalog Outages

An ICF catalog outage can lead to hours of downtime for applications accessed through that catalog. It is a single point of failure in any z/OS environment. As an example, a Mainstar customer using a z/OS provided utility, IDCAMS, to manage their catalog environment experienced an outage when an ICF catalog failed to open. The most current backup was 12 hours old. After recovering the catalog from the backup, the catalog remained unavailable while the customer rebuilt the missing entries. In our customer's case, the total amount of time the catalog was unavailable to the applications was six hours and 32 minutes. In this same scenario, when the customer backed up the catalog using Mainstar's **Catalog RecoveryPlus (CR+)**, the outage was reduced to 27 minutes.

CR+ provides a forward recovery command that recovers the catalog from backup and applies System Measurement Facility (SMF) records to bring the catalog current as of the last update. In addition, **CR+** enables customers to prevent potential outages by executing catalog diagnostic commands on a regular basis. The **CR+** diagnostic command execution automatically creates corrective action commands to execute and 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 SLA.

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 (CDS) contain pointers to where data resides within the hierarchy, on primary storage, in migration level one (ML1) or migration level two (ML2). When these pointers become corrupted, data assets managed by DFSMSHsm become unavailable.

A customer recently reported that one of their outsourced accounts suffered a loss of their DFSMSHsm CDS due to an incorrect sharing option definition. When the outsourcer attempted to recover the CDS from backup, they found that the backup copies were also corrupted; the only good backup was two weeks old. The outsourcer recovered the CDS using the two-week-old backup and attempted to apply the journal data sets to bring the CDS current. However, applying the journal data requires an outage of the DFSMSHsm system which meant missing service level agreements with their customer. The outsourcer abandoned applying the journal files in order to make DFSMSHsm available. However, their customer found they could not access their data which was migrated by DFSMSHsm.

The outsourcer decided to audit the CDS using Mainstar's **FastAudit/390 Suite: HSM FastAudit**. The audit found over 19,000 corrupted entries. Using **HSM FastAudit**, the customer quickly reconciled these differences and built new CDS records to match the catalog

entries. This process was non-disruptive to their customer and within 24 hours, **HSM FastAudit** corrected most of the errors causing recall to fail.

HSM FastAudit also identified 7,000 ML2 tapes the outsourcer needed to audit. They attempted to audit one ML2 tape using the DFSMSHsm provided audit commands. These commands ran for five hours to reconcile entries. Using Mainstar's **FastAudit/390 Suite: HSM FastAudit-MediaControls**, the time to audit one ML2 tape was reduced to just 20 minutes, a savings of 280 minutes per tape or 32,666 hours (1,361 days) in total.

HSM FastAudit, **HSM FastAudit-MediaControls**, and **HSM Reporter/Manager** are crucial to the health of the DFSMSHsm environment. These solutions provide for auditing of the CDS and automatic creation of corrective actions, including DFSMSHsm FIXCDS commands. With emphasis on the word *fast*, the audit, corrective action, and reporting capabilities of these products are unmatched in the industry, enabling customers to audit large DFSMSHsm environments and high-density tape media faster and more accurately than all other solutions available.

Mainstar's Data Asset Backup and Recovery Solutions

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**, **SYSchange**, and **Backup & Recovery Manager Suite: ABARS Manager** and **All/Star**, support a truly resilient data asset protection program for the z/OS environment. These solutions use automated processes that minimize setup and ongoing maintenance. **ASAP** identifies data assets used by the applications and automatically maintains the list over time. This technology can be used to replace error-prone manual practices. **ASAP** uses reliable sources, such as SMF records 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 either **ABARS Manager**, where all data belonging to that application is backed up as a single entity, or to **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.

Recently, a customer conducted a study to determine the level of effort required to manually identify one application's critical data assets needed for recovery. The results of the study were then used to calculate the resource requirements needed to identify assets for all 200 applications. The study revealed it took 176 hours or one man-month to manually identify the assets. Calculated out, the total required time was estimated at 35,200 hours or 4,400 days. At a cost of fifty US dollars per hour, the customer estimated that the project would cost \$1,760,000.00 to create each of the 200 application's lists. In addition, when the customer's list was compared to the list **ASAP** created for the initial application, several critical files were missing from the manually created list. This customer found that manual identification was neither cost-effective nor accurate, and would not have met the industry regulations requiring proof that critical data assets are securely backed up and stored in an offsite location. The customer also noted that with **ASAP** implemented, changes to the application – adding new data assets to the logic flow or eliminating obsolete data – were automatically added to the list for backup, an aspect of the cost not included in their study.

To provide backup and recovery capabilities for data assets, Mainstar's **ABARS Manager** is 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, ML1, or 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 included in the aggregate can be quickly recovered 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. Customers

who 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, backups performed by DFSMSHsm, including **ABARS Manager**, and ICF catalog backups performed by **CR+**. With all backups stored in one inventory database, customers can use **All/Star** to perform an analysis of all the data in their environment and match that information to the inventory. The resulting report details all data assets in the environment that are not in the inventory and therefore do not have a backup or **All/Star** is not tracking the backup.

Without these types of facilities, businesses must determine which processes created the most recent backup which utility was used to back it up, and create or modify existing procedures to recover the backup. With no inventory of backups to reference, businesses may be unaware that a more recent backup copy exists, further jeopardizing their ability to recover from a loss.

Using **ABARS Manager** and **All/Star**, businesses can provide protection from data loss for replicated data, data housed on tape, and data in DFSMSHsm migration. In the event that a replicated asset is destroyed or a miscompute produces incorrect results, customers have a facility to quickly locate and recover from the most current backup copy.

z/OS Infrastructure Member Level Backup

With widespread reliance on IT systems, controls are needed over all such systems, large and small. IT controls commonly include controls over the IT environment, computer operations, access to programs and data, program development, and program changes. These controls apply to all systems, from the mainframe to client-server environments.

The system software component of section 404 of the Sarbanes-Oxley Act includes controls over the effective acquisition, implementation, configuration, and maintenance of operating system software including database management systems, security, and software utilities that allow applications to function.

In every IT organization using z/OS, changes occur in the systems programming department every day. Some of these changes are rather minor and transparent; others are major and have an impact on all users of IT services. To comply with the Sarbanes Oxley Act, and to provide an environment resilient against system changes that

can potentially cause system outages, businesses need automation to create before-and-after copies of changes introduced into the environment.

SYSchange provides features and functions in support of a compliant, resilient z/OS environment by backing up changed PDS members of z/OS system and other infrastructure libraries. When a systems programmer changes a PDS member, a backup is immediately taken and stored in a database. Should the systems programmer need to back out of that change for any reason, the backup is easily recovered. In addition, businesses can now provide security at the member level, allowing some systems programmers change access to members or an entire PDS, while others are not allowed.

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 for the packaging of multiple changes and scheduled implementation at a designated time. This packaging also provides for a complete back-out of all changes should it be 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.

Summary

Businesses using Mainstar's business resiliency solutions in their environments found they were better equipped to meet customer, industry, and government regulations, including the regulations in section 404 of the Sarbanes-Oxley Act, regarding data asset protection and recoverability. These solutions provide data asset backup, including changed data and PDS members, tape data including virtual tape, 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, Mainstar customers reported that they could proactively resolve issues that have the potential to cause an outage because the solutions provide performance enhanced alternatives to more resource intensive preventative methods.

**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 ASAP, ABARS Manager, All/Star, Backup & Recovery Manager Suite, Catalog RecoveryPlus, *FastAudit390* Suite, HSM *FastAudit-MediaControls*, HSM Reporter/Manager, and HSM *FastAudit*, are trademarks of Mainstar Software Corporation. SYSchange is a registered trademark of Pristine Software Corporation.

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: DFSMS, MVS, OS/390, DFSMSHsm.