

## Product Overview

Companies looking to meet compliancy standards can benefit from solutions which enable them to effectively control their IT environments. They must define auditable procedures and detailed directives to control and manage changes in complex z/OS environments, thus complying with government regulations. Such activities constitute a significant operational burden and require automated tools.

## Mainframe Compliance and Change Management

SYSChange is a System Software Change Control and Management solution for the z/OS, designed to address large-scale compliance requirements. It controls and manages system software changes, identifies and reports systemwide changes, and provides advanced tools to deploy the changes across environments.

SYSChange empowers customers to automate these tasks and establish effective controls in a data center. It minimizes the risk of security threats and ad-hoc changes on business operations, while providing the evidence required to confirm the status of security and compliance.

Competitive pressures and demanding customers require rapid delivery of enhancement requests. At the same time, the process of deploying changes must be carefully managed, controlled and verified. SYSChange provides a sustainable **compliance and deployment** capability, enabling Change and Configuration Management to be integrated into the day-to-day operations of the IT department.

## Central Point of Control

SYSChange maximizes productivity by providing managers a central point of control for all software changes. By using an innovative started task that intercepts z/OS systems routines, any change introduced to protected libraries is automatically controlled and managed. Covering the entire spectrum, the "tokenization" technology of SYSChange identifies and reports changes in other non-protected libraries.

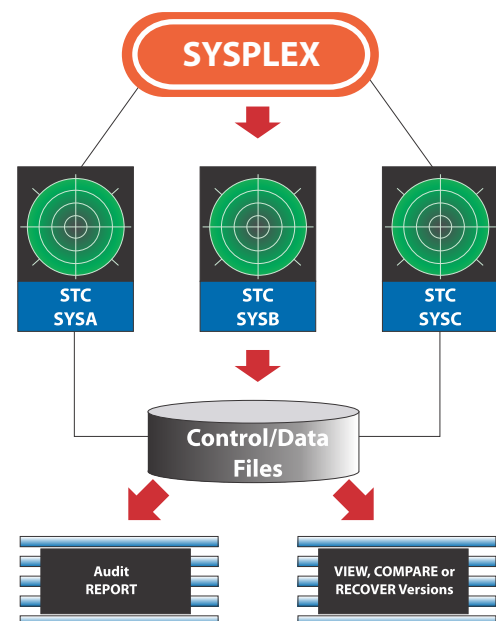
## SYSChange Integrated Components

SYSChange has two integrated components in the areas of systems software and application software change control and management: the Compliance and Deployment Management, and the Developers Workspace.

## SYSChange Compliancy and Deployment Management

The **Compliance Management** enables data centers to protect their critical systems' libraries. Once a library is "protected", every time a library member is updated, the SYSChange Started Task (STC) automatically captures the changed member and stores it in the SYSChange repository.

The SYSChange STC is set up on each system controlling the changes to the libraries in its protection list. Once a change is committed, the information of the user who is committing the change is stored in the SYSChange Control File. At the same time, the changed member is compressed and stored in the SYSChange Data File creating a new version for the member.



By capturing member-level changes automatically and in real time, users will be able to revert to a prior member version by recovering it from the SYSchange online repository. Collected member versions are displayed online, where users can compare any two versions to see the change details and determine the desired version for recovery. With a single click, the selected version is recovered to an intermediate library. Multiple versions may also be selected for recovery.

SYSchange provides systems administrators a non-intrusive process to effortlessly document their work just prior to saving an edited member of a protected library. The user-supplied notes for the introduced changes are automatically augmented to the created member version and stored in the SYSchange repository, viewable at any time in the future.

The **Configuration and Change Control** features in this component of SYSchange enables systems administrators and operations control managers to control update access to library members. For example, this feature designates a specific user to update certain critical library members – and stops any other user from updating such members. Highly critical libraries may be shared amongst different groups of users, where each group may be authorized to only update their pre-designated members or member groups.

All components of the z/OS operating system (including IMS, DB2, CICS, vendors software), in addition to any programs that run the systems and applications, are protected by SYSchange STC around the clock.

The **Deployment Management** on the other hand, enables data centers to automatically identify and package the changed components introduced in a software environment over time. The changed components are packaged automatically and deployed to the target environments.

Using this technology, environments of any size and configuration (multiple systems, multiple LPARs and SYSPLEXes) are synchronized. Automated synchronization of software environments is needed to protect the state of production environments and ensure that changes are correctly and consistently deployed.

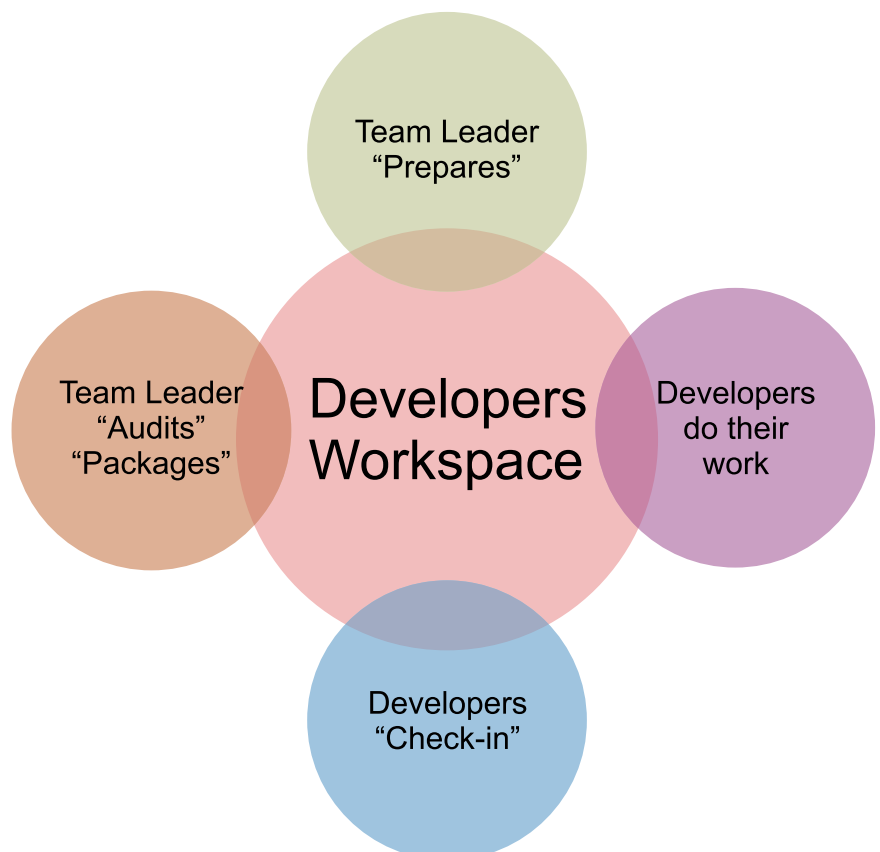
By propagating changes to multiple local or remote software environments, management is assured that designated systems at all sites remain current and synchronized.

The **Compliance and Deployment Management** component is used by medium and large data centers with multiple LPARs and SYSPLEXEs to control and manage their system-wide changes and to synchronize their local or remote environments. The “Advanced Deployment” capabilities in this component of SYSchange have been effectively used by data centers to complement their traditional ALM software in order to flexibly deploy software changes across environments with accountability and control. This component is specifically designed for the z/OS to create a more resilient IT environment and to provide cost-effective solutions in the data center operations.

### **SYSchange “Developers Workspace”**

This component of SYSchange enables application developers to develop code in a secured environment, and then deliver the developed application to multiple environments via the SYSchange “Packaging” and “Promotion Processes.”

The Developers Workspace is used by mainframe development shops who seek replacements for their CA/Librarian, CA/Panvalet, CA/Endevor, their home-grown Change Management solutions, and other ALM products.





## Features

- Protecting critical system libraries for real-time change tracking and backup of changed members
- Recovering from an undesired change by ascertaining the right version and then recovering online
- Ability to document changes to protected library members at the time of Edit and Save
- Assigning responsibility and defining who is going to implement a planned change (CR process)
- Automatically collect the evidence to prove that desired security and compliance standards are met
- Avoid business disruptions by synchronizing software between a production site and the DR site
- Use library "protection" features to designate a specific user to update critical library members
- Compare software on two entire DASD volumes, or two software environments local or remote (z/OS and USS)
- Detect software changes introduced in any environment over time (z/OS and USS)
- Ability to identify and package software changes in an environment and deploy them
- Verify the success of deployed software changes at local or remote environments
- "Developers Workspace" streamlines lifecycle management; use it to replace other high cost ALM products
- Online query and audit reporting functions
- **NEW** - VSAM Change Manager component enables the identification and reporting of record-level changes in VSAM clusters
- **NEW** - Email Alert notifying of changes to critical libraries

## z/OS Software Deployment and Compliance for the 21st Century



## Benefits

- Automating IT controls to address the complexity of regulatory and operational compliance
- Minimize the risk of security threats and ad-hoc changes on business operations
- Reduce the cost of compliance and detect and correct IT issues before they affect your business.
- Consistent control and accuracy in packaging and deploying software changes
- Prevent catastrophes caused by missing or regressing change
- Free up your scarce resources and enable them to focus on more strategic tasks
- Fully automated and verifiable audit trail along with records of the deployed changes
- Invoke procedures to roll back to an original configuration from undesired deployed software
- Reduce systems down time and simplify identification of culprits should disaster strike
- Enhanced security and control by granting exclusive ownership over library members
- Ensure software integrity of any environment (z/OS or USS)



### Supported Environment

SYSchange runs on all levels of z/OS including the latest release 2.1.

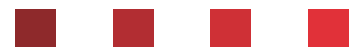
All standard z/OS data sets and USS files are supported.



### GFS Software Company Overview

GFS Software is an Advanced-level IBM Business Partner and a leading developer of tape management software for the IBM z/OS environment. Founded in 1988, GFS has over 25 years of experience in developing quality software solutions that produce measurable cost savings while increasing software efficiency.

Some of the largest z/OS installations, with the largest tape storage-environments, rely on GFS solutions to maintain and improve operational optimization, including financial services, telecommunications, and governmental organizations.



GFS Software, Inc. is an authorized distributor of SYSchange. SYSchange is a product of Pristine Software Company LLC.



[www.gfssoftware.com](http://www.gfssoftware.com)

### GFS Software, Inc.

1133 Broadway, Suite 310  
New York, NY 10010  
Phone +1 212 659-2220  
Fax +1 646 786-4174

e-mail: [gfs@gfssoftware.com](mailto:gfs@gfssoftware.com)  
[www.gfssoftware.com](http://www.gfssoftware.com)



December 2015