

# **Sarbanes Oxley, COBIT and ITIL Compliance** *eventACTION and ussACTION* **are the Solution for the z/OS Systems environment**

## **Summary**

ITIL and “Best Practices” are no longer sufficient to conform to the Sarbanes Oxley and COBIT requirements. There are many products on the market that claim they can track changes, that they can control/manage changes or that they can audit the use of products and the changes made to systems. Almost all of the Change Management products are either “Electronic Paper” (i.e. they cannot prevent unauthorised changes from being made) or they react after the event based on cyclic comparisons of the various datasets. The time between the cyclic comparisons is an open door for anyone trying to manipulate the systems, and paper based systems offer no protection at all.

Under Sarbanes Oxley the organisation is obliged to do all it can to prevent loss of service, loss of data, data manipulation and to improve security. This cannot be achieved using “Best Practices”, it can only be achieved by system driven products or systems based controls that have the ability to track and control changes.

The main objectives of organisations must include:

- **Improved Auditability** – this is the heart of the Sarbanes Oxley Act. Currently most IT systems suffer from huge audit exposures as the changes cannot and are not sufficiently controlled or tracked.
- **Improved Security** – detect and control access/changes down to the member level
- **Improved Availability** – localise the cause of problems and fix them in the shortest possible time, and through the use of controls, actively prevent such problems or outages from occurring.
- **Reduced Costs** – any product that can automate tasks or can speed up the retrieval of data inevitably reduces costs.
- **Improved IT Image** – reducing application and system outages results in a better corporate image.
- **Improved Asset Management** – now the auditors can confirm that software products are only being run on licensed systems.

Also, an organization must understand that it is still responsible for its data and systems even if they have been outsourced. Outsourcing the systems, both hardware and the running of the software (z/OS and proprietary products), does **NOT** absolve the organization from complying with Sarbanes Oxley. The use of SLA's (Service Level Agreements) only define the level of support required by the organization and penalties are, more often than not, defined should the outsourcer fail to meet these service levels. However, under the Sarbanes Oxley Act, the organization is ultimately responsible for **all** aspects of its systems and data. Thus, should a loss of service or loss of data occur, the organization will be held accountable and not the outsourcer. It is clearly imperative that the organization does all it can to prevent such problems, even if it means that additional products be installed under the auspices of the outsourcer to ensure that the SOX requirements are met.

The following tables show how Action Software’s products **eventACTION** and **ussACTION** enhance the z/OS environment and allow organisations to meet and exceed the requirements laid down by Sarbanes Oxley and COBIT.

For the tables below:

**eventACTION** – is a product that tracks and controls various events in an MVS (z/OS) environment.

**ussACTION** – is a product that tracks and controls various events in a USS (Unix System Services) environment under z/OS.

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How eventACTION and/or ussACTION can improve compliance
Are you Sarbanes Oxley / COBIT compliant?	Is your z/OS System Sarbanes Oxley and COBIT compliant?	Almost certainly not, especially in the Systems area. System controls are the strong point of <b>eventACTION</b> and <b>ussACTION</b> .
Have you outsourced your mainframe systems?	Is your outsourced z/OS system Sarbanes Oxley and CIBIT compliant?	Even if you have outsourced your systems, you are still the owner of your data and are therefore liable under Sarbanes-Oxley. <b>eventACTION</b> and <b>ussACTION</b> can help protect your data and your systems.
Sarbanes Oxley Section 404 <i>(Any process or system that could influence the integrity of transaction processing or data must be examined, and controls must be in place to ensure overall process and system integrity)</i>	Can you track alterations in the z/OS systems area?	There are many tools that track a small proportion of these changes, but only <b>eventACTION</b> and <b>ussACTION</b> can provide a secure audit trail.
	Can you prevent unauthorised or uncontrolled changes from being made in the systems area?	There are many ITIL based change management products, unfortunately none of these, unlike <b>eventACTION</b> / <b>ussACTION</b> , can prevent unauthorised changes from being made.
	Can you satisfy your auditors that all changes have been recorded?	Only <b>eventACTION</b> ’s and <b>ussACTION</b> ’s unique tracking and management capabilities allow your organisation to be certain that all changes were tracked and that no unauthorised changes bypassed your Change Management System/Controls.
	Can you assure Third Party Software providers that their products only run on authorised systems?	With <b>eventACTION</b> ’s PXC (Product Execution Control) facilities you can prevent products from being used on non-licensed LPARs or Systems.
Sarbanes Oxley Section 103 <i>(Auditors must describe any weakness in the company’s internal controls) and (Auditors must provide reasonable assurance regarding prevention or timely detection)</i>	People or process oriented solutions (Best Practices) are not secure. The risks may have been identified but cannot be controlled.	These “Best Practice” processes cannot track changes and cannot prevent changes from being made. These controls are unique to <b>eventACTION</b> and <b>ussACTION</b> .
	Many of the weaknesses have been identified by ITIL Processes, but many also lie undiscovered. The risks represented by these undetected loopholes can be enormous and very costly.	<b>eventACTION</b> and <b>ussACTION</b> can not only correct the identified weaknesses, but can also expose and correct further unidentified problems. For example, an Application Development Tool controls the development process from source to the production programs. All appears to be correct however changes can be made and implemented outside the control of these products, with no traces in either the ITIL or Change Management Systems. With <b>eventACTION</b> and <b>ussACTION</b> these unauthorised changes can be prevented.

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How eventACTION and/or ussACTION can improve compliance
COBIT – Security Administration  DS5 Ensure Systems Security	Current IT Security Controls only manage the access at a “Dataset” level and cannot prevent changes as long as the user has the requisite access level.	<b>eventACTION</b> and <b>ussACTION</b> not only extends the security level to the member level, but can also, through the use of the Change Management controls, prevent or allow each and every change to the datasets under their control.
COBIT – Application Change Control Management  A12 – Acquire and Implement application software A13 – Acquire and Implement technology infrastructure A16 – Manage Changes	Currently the majority of organisations are using ITIL based controls or Change Management products that are either “Paper Based” or react after the event. In other words they provide a certain level of documentation, but do not actively control/prevent changes from being made and are definitely not “Audit Secure”.	<b>eventACTION</b> and <b>ussACTION</b> through their “event” tracking and their “management controls” provide an “active” solution for Application Control Management. Once resources have been defined to <b>eventACTION</b> / <b>ussACTION</b> and the management options activated, no changes can be made without the required level of authorisation or documentation. This is absolutely unique in the z/OS world.
COBIT – Data Management and Disaster Recovery  DS4 – Ensure Continuous Service	If changes to the systems cannot be actively controlled, tracked and/or prevented, then these changes will periodically lead to the loss of application availability or even outages to the complete system.	<b>eventACTION</b> ’s and <b>ussACTION</b> ’s Tracking and Backup capabilities make it simple to determine what has changed in a selected area over a selected period using the SCAN and “Datasets Changed” functions. Thus the cause of a problem can be quickly located and the original status immediately restored from <b>eventACTION</b> ’s or <b>ussACTION</b> ’s backups that are taken each time a member/file is changed. In addition to this the active Change Manager controls prevent illegal changes from being made that inadvertently lead to outages. Thus the availability of the systems and applications are improved.
COBIT – Data Management and Disaster Recovery  DS11 – Manage Data	At any point in time a dataset can be damaged or deleted. Currently these can only be recovered to the point when the last backup was taken and all subsequent changes are lost.	<b>eventACTION</b> and <b>ussACTION</b> have the ability, via their tracking functions, to take backups of members/files every time they are changed. This allows the user to re-create lost or damaged datasets/directories back to the point of loss by restoring all changed members. The result is that there is no data loss and the systems and applications can continue without interruption.
COBIT – Operations and Problem Management  DS1 – Define and Manage Service Levels  DS10 – Manage Problems and Incidents	These two go hand-in-hand. In order to manage and comply with service levels, problems and incidents must be resolved quickly. Using current methods localising the source of a problem can sometimes take hours or even days. This has a huge impact on availability and on corporate image.	<b>eventACTION</b> ’s and <b>ussACTION</b> ’s SCAN and “Datasets Changed” functions allows the user to localise the cause of a problem in seconds. These problems can usually be fixed by restoring one or more members/files from <b>eventACTION</b> ’s/ <b>ussACTION</b> ’s backups. The result is that the applications or systems are up and running again in a very short time, helping you to meet your service level agreements. <b>Note:</b> these backups may not be available from any other source.

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How eventACTION and/or ussACTION can improve compliance
COBIT – Operations and Problem Management  DS13 –Manage Operations M1 – Monitor the Processes	In managing the operation and monitoring the processes the operations staff need to know exactly what is being changed in the system and which commands are being issued. As most Change Management systems don't actually control the changes being made, there is often no documentation or indication that a change has been made. A change that could have adverse effects.	The comprehensive Change Management and Tracking functions of <b>eventACTION</b> and <b>ussACTION</b> can prevent any unauthorised or illegal changes from being made, thus giving the operations staff the confidence that they can easily identify any changes that have been made. In addition to this <b>eventACTION</b> 's Command Manager features allow all system commands to be tracked and controlled, giving the operations the ability to find which commands were issued just before a problem occurred or to see which devices or applications were modified at any point in time.
COBIT – Asset Management  DS9 – Manage the Configuration	There are many other asset management tools, but none of these can prevent a product from running on an unlicensed CPU/LPAR	The PXC (Product Execution Control) feature of <b>eventACTION</b> gives the user the ability to monitor, warn or prevent the use of a product on unlicensed systems. Audits by third party software companies will prove license compliance. This reduces the risk of additional license charges for using software on unlicensed systems or LPARs.

These are just some of the exposures in your z/OS systems which need to be addressed in order for you to be Sarbanes Oxley compliant. As you can imagine, to list all of the weaknesses and solutions would require a much longer document.

<b>SOX</b>	Sarbanes Oxley Act – Imposes new restrictions and penalties on auditors and IT-Processes. These requirements can only be met in z/OS by Systems-Based-Controls and cannot be achieved using “Best Practices”.
<b>COBIT</b>	IT Control Objectives for Sarbanes Oxley – A set of objectives for auditors and IT Systems. These objectives can only be met by system products that actively protect, control and track the system’s resources.
<b>ITIL</b>	IT Infrastructure Library – A set of IT Service Management “Best Practices” – These can guide the organisation but cannot actively control or prevent changes.

## ***eventACTION* / *ussACTION* Overview**

**eventACTION** is a z/OS product designed specifically to track and control events in the MVS environment. **ussACTION** does the same for the USS (Unix System Services) environment. In many ways these products are unique as they have the ability to prevent changes that have not been authorised from being implemented in the system.

The main components within **eventACTION** and **ussACTION** are:

<b>eventACTION</b> Change Tracker	Tracks all changes and records Statistics and/or Backups
<b>eventACTION</b> Change Manager	Controls/manages and prevents unauthorised changes
<b>eventACTION</b> Reference Tracker	Tracks all references to Members and Datasets
<b>eventACTION</b> Command Manager	Tracks and controls all system commands
<b>eventACTION</b> Communication Manager	Supports change distribution and cross system communication
<b>eventACTION</b> Product Execution Control	Ensures that products only run on licensed systems
<b>eventACTION</b> Compare Utility	A powerful and unique Side-by-Side compare
<b>ussACTION</b> Change Tracker	Tracks all changes and records Statistics and/or Backups
<b>ussACTION</b> Change Manager	Controls/manages and prevents unauthorised changes
<b>ussACTION</b> Reference Tracker	Tracks all references at the directory and file level
<b>ussACTION</b> Compare Utility	A powerful and unique Side-by-Side compare

Both **eventACTION** and **ussACTION** have a host of additional functions to help an organisation to secure, control, audit and operate its z/OS systems resulting in greater control, improved availability, tangible financial benefits and an enhanced corporate image.

## **Action Software International**

Address:	Action Software International	Telephone:	905.470.7113
	20 Valleywood Drive, Suite 107	Facsimile:	905.470.6507
	Markham, Ontario	E-Mail:	<a href="mailto:sales@actionsoftware.com">sales@actionsoftware.com</a>
	Canada, L3R 6G1	Web-Site:	<a href="http://www.actionsoftware.com">www.actionsoftware.com</a>