

# Sarbanes Oxley 2<sup>nd</sup> Edition, COBIT 4.0 and ITIL Compliance *eventACTION & 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 2<sup>nd</sup> Edition (*Exposure Draft – i.e. not the final version*) and COBIT 4.0 requirements, which both go a lot further than the previous versions.

Both SOX 2<sup>nd</sup> Edition and COBIT 4.0 have made significant changes in the way IT Systems should be controlled and have also stated that these controls also apply to outsourced systems. In other words the organisation is **always** responsible for ensuring that both the systems and the data handling comply with Sarbanes Oxley 2<sup>nd</sup> Edition and COBIT 4.0. The outsourcer **must** be forced by the organisation to conform to these 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 the 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 be sufficiently controlled or prevented.
- **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 the applications and systems 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/LPARs.

## **Data Ownership and the Consequences**

It must be clearly understood that an organisation is always 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 organisation from complying with Sarbanes Oxley.

The use of SLA's (Service Level Agreements) only define the level of support required by the organisation and penalties are, more often than not, levied when the outsourcer fails to meet these service levels.

However, under the Sarbanes Oxley Act, the organisation is ultimately responsible for **all** aspects of its systems and data. Thus, should a loss of service or loss of data occur, the organisation will be held responsible and not the outsourcer. It is of course possible that the contractual agreements between the organisation and the outsourcer clearly define that any infringements under the Sarbanes Oxley Act will be carried by the outsourcer, though it is unlikely that an outsourcer would agree to such conditions.

It is clearly imperative that the organisation 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 use of paper driven rules and regulations that rely on the personnel adhering to the rules and being punished for omissions is a method accepted by some auditors. However, most interpretations of the Sarbanes Oxley Act and COBIT Guidelines clearly state that if the problems could have been avoided by software or other electronic controls, then the penalties due under these laws will still be levied.

**To summarise:** Paper driven rules and regulations may be acceptable to the auditors, but problems that could have been avoided by other means will result in penalties under the Sarbanes Oxley Act. A single infringement can cost up to \$1 Million, whereas the cost of installing and maintaining a software product that meets the Sarbanes Oxley requirements could cost considerably less than a single infringement.

Added to this, products such as *eventACTION* and *ussACTION* deliver many additional benefits that can reduce costs, improve efficiency, controls, availability and security.

Installing these products is not just an "Insurance Policy" but a valuable addition to help control and optimise your z/OS Systems.

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 an USS (Unix System Services) environment under z/OS.

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How <i>eventACTION</i> and/or <i>ussACTION</i> can improve compliance
Are you Sarbanes Oxley 2 <sup>nd</sup> Edition/ COBIT 4.0 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 <i>eventACTION</i> and <i>ussACTION</i>
Have you outsourced your Mainframe systems?	Is your outsourced z/OS System Sarbanes Oxley and COBIT compliant?	Even if you have outsourced your systems, you are still the owner of your data and are therefore liable under Sarbanes Oxley. <i>eventACTION</i> and <i>ussACTION</i> can help protect your data and your systems.
Sarbanes Oxley Section 404 (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)	Can you track alterations in the z/OS systems area?	There are many tools that track a small proportion of these changes, but only <i>eventACTION</i> and <i>ussACTION</i> 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 <i>eventACTION/ ussACTION</i> , can prevent unauthorised changes from being made.
	Can you satisfy your auditors that all changes have been recorded?	Only <i>eventACTION</i> ’s and <i>ussACTION</i> ’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?	No, unless you use <i>eventACTION</i> ’s PXC (Product Execution Control) facilities. This can prevent products from being used on non-licensed LPARs or Systems.
Sarbanes Oxley Section 103 (Auditors must describe any weakness in the company’s internal controls) and (Auditors must provide reasonable assurance regarding prevention or timely detection)	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 <i>eventACTION</i> and <i>ussACTION</i> .
	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.	<i>eventACTION</i> and <i>ussACTION</i> 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 <i>eventACTION</i> and <i>ussACTION</i> these unauthorised changes can be prevented.

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How <i>eventACTION</i> and/or <i>ussACTION</i> can improve compliance
COBIT – Plan and Organise  P09 – Assess and Manage IT Risks	The risks of outages of the whole z/OS System or even of single Applications are both underestimated and in many organisations ignored completely. Any outages can result in loss of business and loss of image, both of which can be extremely expensive.	<i>eventACTION</i> and <i>ussACTION</i> will expose, and can subsequently eliminate, many of the risks that could lead to system or application outages. This risk control is achieved through event monitoring and active controls to prevent uncontrolled or unauthorised changes from being made to the systems datasets.
COBIT – Acquire and Implement  AI1 – Identify Automated Solutions AI3.3 – Infrastructure Maintenance	Many organisations are still using “paper driven” Change Management solutions. These are, despite all assurances and controls, not 100% reliable and cannot effectively prevent unauthorised changes from being made.	<i>eventACTION</i> and <i>ussACTION</i> offer an automated solution with active controls that cannot be circumvented. In other words if a dataset has been defined as requiring a Change Request and Authorisation (on single or multiple levels), then changes cannot be made until the requirements have been satisfied. This is a true and accurate control of resources. AI3.3 states “... Ensure that changes are controlled in line with the organisation’s change management procedure.”
COBIT – Acquire and Implement  Application Change Control Management  A12 – Acquire and Implement application software A13 – Acquire and Implement technology infrastructure	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 “Audit Secure”.	<i>eventACTION</i> and <i>ussACTION</i> through their “event” tracking and their “management controls” provide an “active” solution for Application Control Management. Once resources have been defined to <i>eventACTION/ussACTION</i> and the management options activated, no changes, including changes to the permission and ownership bits, can be made without the required level of authorisation or documentation. This is absolutely unique in the z/OS world.



Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How <i>eventACTION</i> and/or <i>ussACTION</i> can improve compliance
COBIT – Deliver and Support Security Administration  DS5 – Ensure Systems Security  DS5.5 – Security Testing, Surveillance and Monitoring DS5,9 – Malicious Software Prevention, Detection and Correction	Current IT Controls only manage the access at a “Dataset” level and cannot prevent changes as long as the user has the requisite access level.  Quote “A logging and monitoring function enables the early detection of unusual or abnormal activities....”	<p><i>eventACTION</i> and <i>ussACTION</i> 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.</p> <p><i>eventACTION</i> and <i>ussACTION</i> enable the organisation to detect abnormal activities that might result in the detrimental manipulation of the system.</p>
COBIT – Deliver and Support  Operations and Problem Management  DS1 – Define and Manage Service Levels DS8 – Manage Service Desk and Incidents DS10 – Manage Problems	These three go hand-in-hand. In order to manage and comply with service levels, problems and incidents must be managed and 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. A quote from DS10.2 “Identify and initiate sustainable solutions addressing the root cause, raising change requests ....”	<p><i>eventACTION</i>’s and <i>ussACTION</i>’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 <i>eventACTION</i>’s/ <i>ussACTION</i>’s backups. <b>Note:</b> these backups are probably not available from any other source. 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.</p> <p>In many cases, as seen from DS10.2, the root cause of problems can and often is due to uncontrolled changes.</p>
COBIT – Deliver and Support  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.	<p><i>eventACTION</i> and <i>ussACTION</i> 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.</p> <p><i>ussACTION</i> also tracks changes to the permission and ownership bits.</p>

Sarbanes Oxley Section or COBIT Control Objective	Exposures in z/OS (MVS and USS)	How <i>eventACTION</i> and/or <i>ussACTION</i> can improve compliance
COBIT – Deliver and Support Operations and Problem Management DS13 –Manage Operations COBIT – Monitor and Evaluate ME1 – Monitor and Evaluate IT Performance	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. Adverse changes and outages lead to both internal and external user dissatisfaction.	The comprehensive Change Management and Tracking functions of <i>eventACTION</i> and <i>ussACTION</i> 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 <i>eventACTION</i> 's Command Management 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. <i>eventACTION</i> and <i>ussACTION</i> 's tracking and control capabilities reduce the risk of problems, outages or manipulation, thus giving rise to improved internal and external user satisfaction.
COBIT – Deliver and Support 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 <i>eventACTION</i> gives the user the ability to monitor, warn or prevent the use of a product on unlicensed systems. Audits by TPS (Third Party Software) companies will prove license compliance. This reduces the risk of additional license charges for using software on unlicensed systems or LPARs.
COBIT – Monitor and Evaluate ME2 – Monitor and Evaluate Internal Control	Organisations must monitor, assess and improve the effectiveness of internal controls for information security and change controls	<i>eventACTION</i> and <i>ussACTION</i> provide a fully comprehensive audit trails and change controls that can prevent unauthorised changes from being made. All changes are tracked and reported so that changes outside the scope of the change controls can also be quickly and easily identified and reported on.
COBIT – Monitor and Evaluate ME3 – Ensure Regulatory Compliance	Currently very few organisations can claim to be fully compliant with Sarbanes Oxley 2 and/or COBIT 4.0	<i>eventACTION</i> and <i>ussACTION</i> provide the most optimal solution for both MVS and USS in regards to the system's areas. Unlike other products <i>eventACTION</i> and <i>ussACTION</i> provide real-time controls and full audit trails of any changes that are made in the system's area.

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 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 systems products that actively protect and control 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 an z/OS Product designed specifically to track and control events in the MVS environment. *ussACTION* is a supplementary product that does the same for the USS (Unix System Services) environment, but requires *eventACTION* as a prerequisite. 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 functions within *eventACTION* and *ussACTION* are:

<i>eventACTION</i> Change Tracker	Tracks all changes and records Statistics and/or Backups
<i>eventACTION</i> Change Manager	Controls/manages and prevents unauthorised changes
<i>eventACTION</i> Reference Tracker	Tracks all references to Members and Datasets, allowing for a comprehensive clean-up of internal datasets
<i>eventACTION</i> Command Manager	Tracks and controls all system commands
<i>eventACTION</i> Communication Manager	Supports change distribution and cross system communication
<i>eventACTION</i> Product Execution Control	Ensures that products only run on licensed systems
<i>eventACTION</i> Compare Utility	A powerful and unique Side-by-Side compare
<i>ussACTION</i> Change Tracker	Tracks all changes and records Statistics and/or Backups
<i>ussACTION</i> Change Manager	Controls/manages and prevents unauthorised changes
<i>ussACTION</i> Reference Tracker	Tracks all references to Members and Datasets, allowing for a comprehensive clean-up of internal datasets
<i>ussACTION</i> 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 GmbH**

Address:	Action Software GmbH Alte Steinhauserstr. 1 CH-6330 Cham Switzerland	Telephone:	+41 41 748 6266
		Facsimile:	+41 41 748 6267
		E-Mail:	<a href="mailto:Marketing@ActionSoftware.ch">Marketing@ActionSoftware.ch</a>
		Web-Site	<a href="http://www.actionsoftware.ch">www.actionsoftware.ch</a>