Sarbanes Oxley Act
Statement of Ability

An AdRem Software White Paper

©2009 AdRem Software, Inc.

This document is written by AdRem Software and represents the views and opinions of AdRem Software regarding its content, as of the date the document was issued. The information contained in this document is subject to change without notice.

ADREM SOFTWARE MAKES NO WARRANTS, EITHER EXPRESS OR IMPLIED, IN THIS DOCUMENT. AdRem Software encourages the reader to evaluate all products personally.

AdRem Software and AdRem NetCrunch are trademarks or registered trademarks of AdRem Software in the United States and other countries.

All other product and brand names are trademarks or registered trademarks of their respective owners.

AdRem Software, Inc.
410 Park Avenue, 15th Floor
New York, NY 10022
USA

Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
Email: sales@adremsoft.com
Web site: http://www.adremsoft.com

Sarbanes Oxley Act Statement of Ability

Many organizations are looking to adhere to Sarbanes Oxley (SOX) as a means of achieving corporate governance. As a result, there is a growing pressure on software vendors, such as AdRem, to publish compliance statements.

However, AdRem Software would like to state the following: Audit companies see the Sarbanes Oxley Act as a means of regulating the amount and quality of publicly available information published by organizations in order to avoid scandals such as Enron; the availability of this information does place a burden on IT services, systems and software but there is no SOX compliance or certification for vendors to adhere to; SOX is all about corporate governance, IT is an underpinning requirement so the auditors expect organizations to embrace the COBIT (Control Objectives for Information Technology) framework.

COBIT

COBIT is a substantial best practice framework covering 34 IT Control Objectives:

Part One - Planning & Organization

Define a strategic IT plan
Define the Information architecture
Determine the technological direction
Define the IT organization and relationships
Manage the IT Investment
Communicate management aims and direction
Manage human resources
Ensure compliance with external requirements
Assess risks
Manage projects
Manage quality

Part Two - Acquisition & Implementation

Identify automated solutions
Acquire and maintain application software
Acquire and maintain technology infrastructure
Develop and maintain procedures
Install and accredit systems
Manage changes

Part Three - Delivery & Support

Define and manage service levels
Manage third party services
Manage performance and capacity
Ensure continuous service
Ensure systems security
Identify and allocate costs
Educate and train users
Assist and advise customers
Manage the configuration
Manage problems and incidents
Manage data
Manage facilities
Manage operations

Part Four - Monitoring

Monitor the process
Assess internal control adequacy
Obtain independent assurance
Provide for independent audit

Again, there is no compliance certification for COBIT as it is the sum of many parts, from CIOs simply publishing their strategic IT plans, to infrastructure builds, managing configurations and monitoring process. COBIT is a framework of activities that can be best enabled using best-of-breed solutions.

The ability of AdRem's products to integrate with other best of breed tools, including IT infrastructure management solutions and IT help desk systems enables organizations to run a connected portfolio of products that guarantee the availability of the systems delivering information to satisfy auditors and corporate governance requirements.

How AdRem's solutions address COBIT objectives

AdRem's products work best on parts 2 and 3 and to a lesser extent part 4 as detailed below:

Part Two - Acquisition & Implementation

Install and accredit systems

AdRem's network management products are best installed right at the beginning of a project as they can be used to ensure networked devices are installed and commissioned without incident and problems. After which they will ensure availability and alert to capacity issues.

Manage changes

Monitoring the effect of changes is important and AdRem's product can report on device durability in order to help forecast potential change requirements. They can also alert on problems that occur during and after changes have been expedited. Impact reporting can also be set up to highlight other connected concerns.

Part Three - Delivery & Support

Define and manage service levels

Where known priorities exist structured monitoring and alerting can be set against devices and AdRem's products will ensure Service Level Agreements (SLAs) and Operating Level Agreements (OLAs) are not breached. Integration with IT service management solutions will ensure greater transparency of device SLAs and OLAs to those providing services.

Manage 3rd party services

AdRem's alerting capabilities means problem escalation to third party service providers can be instantaneous as a device starts to fail.

Manage performance and capacity

AdRem's products can be used to set performance thresholds against network devices to ensure uptime and management reports can flag issues with devices unable to cope with demand.

Ensure continuous service

Availability is key to providing continuous service; the types of alerts set within AdRem's solutions will ensure first response to issues and allow management to accurately set preventative maintenance activities.

Manage the configuration

A configuration is a group of connected devices and AdRem would use SNMP to discover these devices and range them by using IP ranges. This presents analysts with a view of the network upon which failing devices are displayed and actions to manage the whole configuration and to communicate status to affected users can be expedited.

Manage problems and incidents

By integrating AdRem's products with IT Service Management solutions, the ability to differentiate between incidents and problems occurring on the network can be made through detailed fault profiling. This will ensure resourcing and escalation is priority driven.

Part Four - Monitoring

Monitor the process

Where processes are automated and run by networked applications and devices, again, the AdRem's products can ensure that alerting and monitoring is set against business rules governing these processes.

Best practice practitioners are accepting COBIT as a means of bridging governance issues facing IT and the business. Many recommend ITIL as the process framework to realize the stages represented by COBIT, although it still is not recognized within the BS15000 IT Service Management Standard.