



Department of Administrative Services  
Presentation to the State Audit Committee  
*SAS-70 Audit Update*

*December 1, 2009*



- I. Breakthroughs
- II. 2009 SAS-70 Audit Overview
- III. OAKS Disaster Recovery Approach
- IV. Supplemental Material

# Breakthroughs



*Significant improvement was achieved in the results of the OAKS SAS-70 audit from FY2008 to FY2009.*

## Improvement in OAKS SAS-70 Audit Results from 2008 to 2009

Audit Items	FY2008		FY2009
Unmet Control Objectives	<b>15</b>		<b>4</b>
Audit Comments	<b>38</b>		<b>24</b> 7 of the 24 relate to the 4 Unmet Control Objectives above and could have a potential impact.

As part of our risk management strategy DAS is focusing on remediation efforts for the four unmet control objectives.

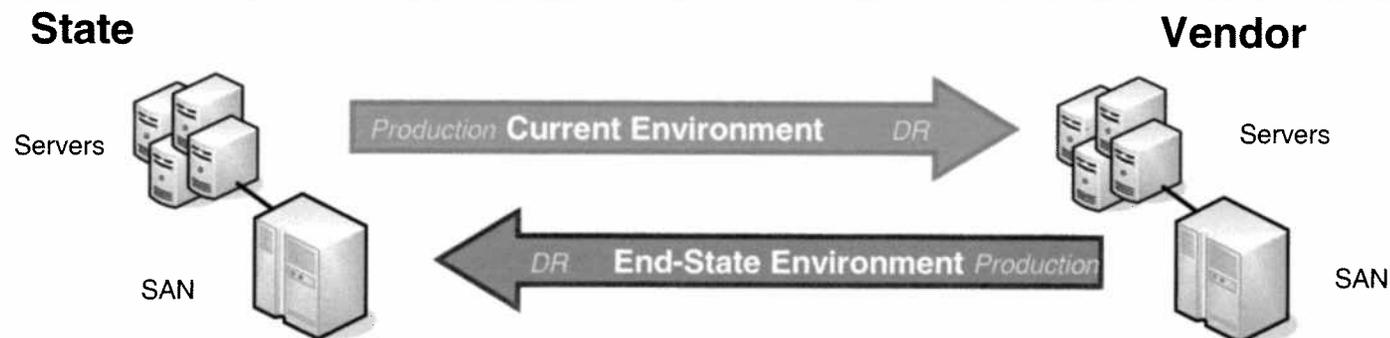
# 2009 SAS-70 Audit Details and Audit Comments Crosswalk



Progress continues in the OAKS program area. In FY09, only seven of the comments issued resulted in unmet control objectives.

Control Objective	Audit Comments and Status
<p><b>1. Change Management</b> – Requirements for test documentation need to be stated in procedure documents.</p> <p>Repeat finding from FY08.</p>	<p><b>#4</b> – Program change comment documentation and unclear training requirements.  <b>Status</b> – Change control processes are being refined and adjusted. These processes are being managed by the Managed Services vendor. Training requirements are specified by the State. Compliance monitoring processes are being implemented by OAKS Service Assurance.</p>
<p><b>2. Security Management</b> – Employee sign-offs and network access approval.</p> <p>Both are repeat findings from 2008.</p>	<p><b>#5</b> – Missing policy signoffs. This has been remediated.  <b>#6</b> – OAKS network user access approval.  <b>Status</b> – The Service Assurance group has implemented periodic audits of all environments and is currently doing a full audit of all environments to prepare for a new on-boarding/off-boarding process. Part of this process will include management confirmation of employee access needs with appropriate disposition of any discrepancies found. We expect to implement the new process by January 2010.</p>
<p><b>3. Application Controls (FIN)</b> – Chartfield changes and update access to standing data.</p> <p>Both #19 and #20 are repeat findings from 2008, and #17 is new in FY09.</p>	<p><b>#17</b> – Vendor change documentation and authorization (OBM). This has been remediated.  <b>Status</b> – The vendor update process moved to OSS on 9/1/09. As of this date, all vendor change documentation is scanned and retained electronically based on legal requirements. OBM believes that the current methodology for maintaining vendor EFT information is adequate, but will continue to explore technology based solutions to strengthen existing controls.  <b>#19</b> – Unauthorized update access to standing data (OBM). This has been remediated.  <b>Status</b> – The four unauthorized users identified in the comment have been removed. In connection with the move of this function to OSS, OBM is developing a process to validate users with access to the vendor file on a periodic basis.  <b>#20</b> – Chartfield changes not documented or formally approved (OBM).  <b>Status</b> – The chartfields referenced in this comment refer to Fund, ALI and ISTV Xref which are established by Legislative and Controlling Board actions and are documented as part of the public record. OBM is evaluating the extent to which we maintain duplicate documentation, solely for auditor review.</p>
<p><b>4. Physical Security (Warrant Writing)</b> – Physical security of the warrant writing facility including key storage and physical access.</p> <p>Physical security is a repeat finding from 2008.</p>	<p><b>#22</b> – Physical security of warrant writing facility (GSD). This has been remediated.  <b>Status</b> – Keys are now stored in the vault. Security now updates the Integrity Drive location when someone leaves and a review of badge access has been performed and access removed where appropriate.</p>

# OAKS Disaster Recovery Approach



## ***Current Environment***

- Production operations located at the State
- Disaster Recovery located at the Vendor
- Tier II facility
- RPO (Recovery Point Objective) of 24 hours
- RTO (Recovery Time Objective) of 96 hours
- DR tested in September 2009

## ***End-State Environment*** → February ***(As Proposed by Managed Services Vendor)***

- Production operations located at the Vendor
- Disaster Recovery at the State
- Tier III facility
- RPO (Recovery Point Objective) of 24 hours
- RTO (Recovery Time Objective) of 48 hours
- DR test slated for late January 2010

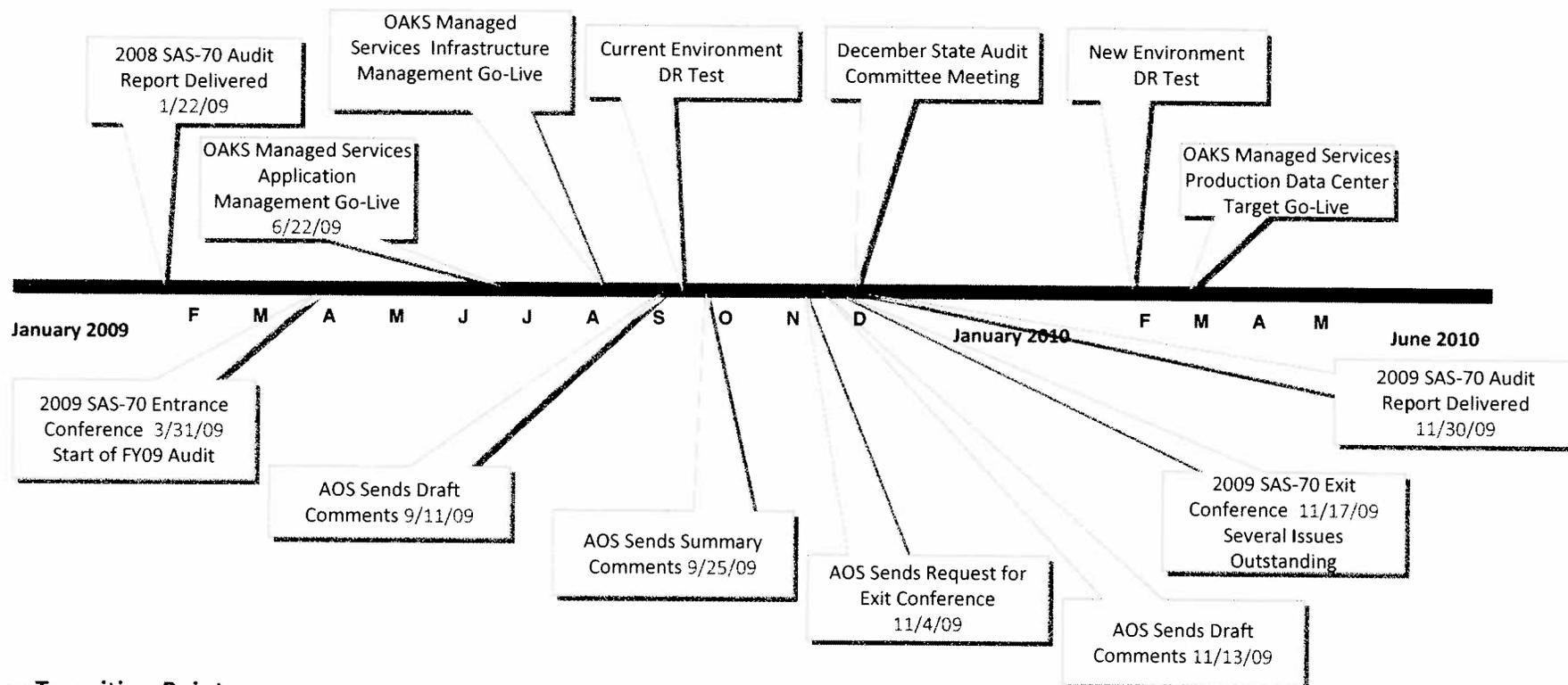


- I. Overview Timeline
- II. Status of Open Items from 2008 SAS-70 Audit

# Overview Timeline



**The following is a brief overview of the timeline associated with the 2008 and 2009 SAS-70 OAKS Audits and the OAKS transition to Managed Services.**



## **Key Transition Points:**

- OAKS Managed Services has taken control of application management (6/22/09) and infrastructure management (8/3/09) and successfully executed a current environment disaster recovery test (9/16/09).
- OAKS Managed Services migration to new data center is planned for late February 2010.
- In conjunction with moving OAKS to this data center, hardware upgrades (reliability and performance) and disaster recovery capabilities will be implemented and tested prior to the cutover to the new data center.

# Status of Open Items from 2008 SAS-70 Audit



*Progress has continued since the September 2009 State Audit Committee Meeting. Status updates on items reported as open in September are as follows:*

Area	Status
<p><b>1. General OAKS Security</b> – Update comment log documentation for all changes to applications to reflect the current processes and procedures of their computer applications. Create a comprehensive evaluation of the current documentation for each application to help ensure that all program changes have been made.</p>	<p>On target for remediation in December 2009.</p>
<p><b>2. Manual Combo Code Entry</b> - Update the OAKS application to prohibit agency users from having the ability to manually enter Combo Codes outside their assigned agency.</p>	<p>On target for remediation in Q1 2010. Business needs require that this functionality remain in the application. Additional system and procedural controls are being implemented.</p>
<p><b>3. OAKS Data Masking</b> - OAKS to sanitize all production data used in the testing environment to prevent the compromise of sensitive employee information.</p>	<p>On target for remediation in December 2009.</p>
<p><b>4. Disaster Recovery</b> – OAKS to complete the formalized state-developed disaster recovery plan.</p>	<p>On target for remediation in conjunction with move to new data center.</p>