Department of Administrative Services Presentation to the State Audit Committee

SAS-70 Audit Update

March 9, 2010

Agenda

I. Meeting Control Objectives

II. 2009 SAS-70 Audit Overview

III. Unscheduled Disaster Recovery Testing

IV. Summary of Progress

The OAKS goal is to meet all control objectives.

Our goal is to design and implement controls that will provide reasonable assurance that risks are identified, measured, and managed so that relevant control objectives will be achieved.

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

Audit Items	FY2008		FY2009	Current State
Unmet Control Objectives	**15**	→	**4**	**1***

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

*OAKS Network access approval is the only item remaining to be remediated. This is part of a larger effort to implement a comprehensive user provisioning process and is targeted for completion Q4 FY2010.

2009 SAS-70 Audit Overview

Progress continues in the OAKS program area. In FY09, only seven of the comments issued resulted in unmet control objectives. Remediation has been completed or is in progress for the following items.

Control Objective	Audit Comments and Status
1. Change Management – Requirements for test documentation need to be stated in procedure documents. **Repeat finding from FY08.**	**#4** – Program change comment documentation and unclear training requirements. **Status – Remediated** •The Managed Services Vendor (MSV) has responsibility for the process. •Recently added application changes to the process. •As of March 1, 2010 the change management documentation has been updated to include a decision point for training requirements. In addition the forms have been modified to include check-off that a training decision has been made. **Continuous Improvement – Monthly monitoring of process documentation** • The Security Operations group will begin monthly monitoring of the change process by auditing a sample of the changes. The audit will look for required documentation and appropriate approvals. Results will be provided to the MSV and the Change Advisory Board (CAB). This process has not gone through a monitoring cycle since the new changes have been implemented.
2. Security Management – Employee sign-offs and network access approval. **Both are repeat findings from FY08.**	**#5** – Missing policy signoffs. **Status – Remediated** **#6** – OAKS network user access approval. **Status – Remediation nearly complete**. •Auditing documentation of on-boarding and off-boarding has completed. Outdated access approval documentation has not been re-created if missing. The new process will document approval based upon current access. Strict controls of who can request have been enforced and two check points are in place to check for appropriate documentation and signatures. •Currently auditing all environments and cleaning up accounts. •Process refinement is planned for implementation Q4 FY2010. •Implementation of InfoPath form to catalog all access for a user is planned in concert with process refinement.

2009 SAS-70 Audit Overview

Progress continues in the OAKS program area. In FY09, only seven of the comments issued resulted in unmet control objectives. Remediation has been completed or is in progress for the following items.

Control Objective	Audit Comments and Status
3. Application Controls (FIN) – Chartfield changes and update access to standing data. **Both #19 and #20 are repeat findings from FY08, and #17 is new in FY09.**	**#17** – Vendor change documentation and authorization (OBM). **Status – Partially Remediated** **#19** – Unauthorized update access to standing data (OBM). **Status – Remediated** **#20** – Chartfield changes not documented or formally approved (OBM). **Status – Remediated**
4. Physical Security (Warrant Writing) – Physical security of the warrant writing facility including key storage and physical access. **Repeat finding from FY08.**	**#22** – Physical security of warrant writing facility (GSD). **Status – Remediated** • New combination lock has been installed and procedures implemented for both access to the combination and a process to change out the lock if an employee with the combination leaves the agency. • Additional audits of physical access have been implemented. These are now done on a monthly basis. • One point of contact for additions and removals has been established and has direct contact with the Security team who controls badge access.

Research Results

- Performing “unscheduled” or “unplanned” disaster recovery testing involves the premeditated disruption of the normal operation of a system to test the disaster recovery plan.
  - This type of testing is costly and will disrupt normal operations.
  - No enterprises perform this type of testing except in a highly controlled, duplicate test environment.
- National Institute of Standards and Technology’s (NIST) Special Publication 800-34 “Contingency Planning Guide for Information Technology Systems”
  - NIST does not recommend unscheduled or unplanned testing as key elements in its testing and contingency strategies.
- NASCIO response
  - Approximately 20 states responded to our request for information.
    - None are performing unplanned or unscheduled DR tests.
    - None were aware of any state or other enterprises that are performing unplanned or unscheduled DR tests.
    - All cited the high risk and cost as the primary reason for not performing this type of testing.
    - All recommended tabletop exercises as an alternative.
- Gartner research recommends:
  - Use a tabletop exercise as a basis for defining contingencies.
  - Use a live disaster recovery test performed at the recovery site (hot site or other alternate recovery site) to test the execution efficiency and effectiveness of the disaster recovery plan.

Conclusion

- Research suggests non-production tests such as tabletop exercises are best practice methods for determining disaster recovery contingencies while minimizing impact to the business.

- DAS conducted a full recovery OAKS DR test on 2/3/2010. We are in the process of analyzing the results.

- Because this is a new DR plan and a new environment, another test is being planned for the July/August timeframe.

- Our assessment will also contemplate what control designs need to be improved as part of our operational go-forward plan, which we will be prepared to share with the Committee at the next quarterly meeting.

The OAKS goal is to meet all control objectives.

Our goal is to design and implement controls that will provide reasonable assurance that risks are identified, measured, and managed so that relevant control objectives will be achieved.

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

Audit Items	FY2008		FY2009	Current State
Unmet Control Objectives	**15**	→	**4**	**1***

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

*OAKS Network access approval is the only item remaining to be remediated. This is part of a larger effort to implement a comprehensive user provisioning process and is targeted for completion Q4 FY2010.

Status of Open Items from 2008 SAS-70 Audit

Progress has continued since the December 2009 State Audit Committee Meeting. Status updates on items from the 2008 SAS-70 audit reported as open in December are as follows:

Area	Status
1. General OAKS Security – 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.	Remediated
2. Manual Combo Code Entry - Update the OAKS application to prohibit agency users from having the ability to manually enter Combo Codes outside their assigned agency.	Remediated
3. OAKS Data Masking - OAKS to sanitize all production data used in the testing environment to prevent the compromise of sensitive employee information.	Remediated
4. Disaster Recovery – OAKS to complete the formalized state-developed disaster recovery plan.	Remediated