

Management Response to the  
State of Ohio SAS70 OIT OAKS FIN HCM Warrant Writing and EFT  
Issued by: Ohio Department of Administrative Services (DAS)  
And the  
Ohio Office of Budget and Management (OBM)

### OAKS Application Automated Security Program

Priority	Auditor of State Recommendation	Management Response
1	ML#12: We recommend authorized account application forms be submitted and maintained for all OAKS access requests; management should complete a full review of user access to ensure all access to the application is documented and approved and extraneous rights removed.	Completed. As part of the development and implementation of the HCM Application Automated Security Program, OAKS security coordinators completed a review of row-level HCM access for their employees that ensured appropriate restrictions, correction of assigned roles, and identification of separated employees. The security program implemented on 10/22/2008 replaced the paper form application and approval process with an automated submission and approval process that is maintained by OAKS personnel. The security program automatically removes employee's HCM roles upon termination, promotion, demotion, or reassignment within an agency. <b>Agency: DAS</b> <b>Management status: Completed 10-22-2008</b>
1	ML#13: We recommend OAKS establish and follow formal termination procedures.	Completed. OAKS collaborated with HRD Policy in order to establish a formal user access termination process which was incorporated in the HCM Application Security program. HCM Application Security Program was implemented 10/22/2008 and automatically removes roles from HCM when an employee is terminated from the agency. <b>Agency: DAS</b> <b>Management status: Completed 10-22-2008</b>
1	ML#27: We recommend that management update the OAKS application to prohibit agency users from having any access to data or transactions outside of their assigned agency.	Completed. As part of the development and implementation of the HCM Application Security Program, OAKS security coordinators completed a review of row-level HCM access for their employees that ensured appropriate restrictions from viewing data or transactions outside of their assigned responsibilities. OAKS security coordinators corrected assigned roles, and identified separated employees. The security program was implemented on 10/22/3008. The development of a similar FIN access security program is in progress. <b>Agency: Shared</b> <b>Management status: In process with planned completion of April 2009</b>

## OAKS Application Automated Security Program (Continued)

Priority	Auditor of State Recommendation	Management Response
1	ML#28: We recommend that management limit the number of authorized personnel having access to all state agency payroll data to ensure that access is commensurate with users' current assigned job duties. We also recommend the department periodically review access levels for OAKS users in accordance with Security Procedures Document.	<p>Completed. HCM Application Security Program was implemented 10-22-2008.</p> <p>As part of the implementation, <b>security coordinators</b> reviewed row level access to ensure employees in HCM are appropriately restricted. Security Coordinators from each agency are to review employee access annually.</p> <p><b>Agency: DAS</b>  <b>Management status: Completed 10-22-2008</b></p>
1	ML#11: We recommend authorized account application forms be submitted and maintained for all OAKS FIN access requests. Management should complete a full review of user access and extraneous rights removed.	<p>Automated system has been developed that automatically removes FIN roles when an employee is terminated from the agency. For future access, FIN is moving toward the use of an online access request form.</p> <p><b>Agency: Shared</b>  <b>Management status: In process with planned completion date of October 2009</b></p>
2	ML#33: We recommend OAKS FIN management perform periodic review of update access to sensitive data tables to ensure that only authorized individuals have access.	<p>Unauthorized users were removed in August 2008 and revalidated in February 2009. Security coordinators from each agency are to review employee access annually.</p> <p>DAS reflects a role level review by the agency Security Coordinators as open until April 2009.</p> <p><b>Agency: Shared</b>  <b>Management status: In process with planned completion date of April 2009</b></p>

## Additional OAKS Application Security Access Recommendations

Priority	Auditor of State Recommendation	Management Response
2	<p>ML#4: We recommend OAKS complete the following functions for all OAKS test environments on a periodic basis:</p> <ul style="list-style-type: none"> <li>• Periodically review and verify system and application-level profiles and access authorities are appropriate for the assigned job and maintain documentation as an audit trail.</li> <li>• Ensure that when users are terminated or transferred to new departments, their access is updated appropriately on a timely basis and related documentation is maintained as an audit trail.</li> </ul>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009. The OAKS team will continue to work with the Managed Service Vendor (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>
1	<p>ML#6: We recommend management complete a full review of user access to the PeopleSoft Production permission lists to help ensure all access to department resources is documented and approved.</p>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009. The OAKS team will continue to work with the (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>
1	<p>ML#7: We recommend management complete a full review of user access to ensure all access to the application is documented as approved and any extraneous access rights should be removed.</p>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009. The OAKS team will continue to work with the (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>
1	<p>ML#9: We recommend OAKS comply with their Security Procedures Document by ensuring that computer violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis.</p>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009. The OAKS team will continue to work with the (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>

## Additional OAKS Application Security Access Recommendations (Continued)

Priority	Auditor of State Recommendation	Management Response
1	<p>ML#17: We recommend OAKS limit the number of accounts with administrative privileges in the application to the security team to help prevent the number of unauthorized personnel having access to add and modify roles. We also recommend OAKS periodically review users with elevated privileges to detect and prevent inappropriate access levels.</p>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009.</p> <p>The OAKS team will continue to work with the (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>
1	<p>ML#18: We recommend OAKS ensure that only individual accounts are used to provide for individual accountability. We recommend management complete a full review of user access to production, EPM, CRM data bases to ensure that all access to these resources is documented and approved and that any extraneous rights should be removed.</p>	<p>The OAKS Application Security team and the OAKS Infrastructure team is in the process of reviewing and remediating these security concerns with a projected completion date of April 1, 2009.</p> <p>The OAKS team will continue to work with the (MSV) during the transition phase to ensure these controls continue after the vendor assumes responsibility for these.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>
2	<p>ML#23: We recommend the Department consider implementing additional monitoring and tracking controls for the batch administrator ID to help ensure effective audit trail is in place.</p>	<p>The OAKS Security Office (OSO) is in the process of developing a monitoring structure that will enable the batch administrator to perform a quarterly access review as well as a review of various security reports on a daily basis.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with planned completion date of April 2009.</b></p>

## OAKS Back Office Remediation

Priority	Auditor of State Recommendation	Management Response
1	ML#15: We recommend the UNIX system password parameters be in compliance with the OAKS Security Procedures Document. In addition, UNIX accounts should be set to automatically lock after a set number of unsuccessful attempts to adequately reduce the chance of unauthorized access to programs data. Finally, user accounts must be disabled after a period of defined terminal inactivity.	Completed. Tasks included enabling of UNIX password policies and resetting of passwords. Logoff established after a set period of terminal inactivity will not be implemented unless the server was external facing, since many tasks and jobs require no auto logoff. <b>Agency: DAS</b> <b>Management status: Completed 12-31-2008</b>
1	ML#16: We recommend management complete a full review of user UNIX access to ensure all access to the department resource is documented and approved and any extraneous rights are removed.	Completed. OAKS staff assisted DAS / Service Delivery Division (SDD) and provided a list of current user-ids. SDD reviewed the list of current user-ids and removed those user-ids no longer needed. <b>Agency: DAS</b> <b>Management status: Completed 12-31-2008</b>
2	ML#19: We recommend OAKS ensure that all SU logs are maintained for at least one audit cycle.	Completed. UNIX backup policy is to back up the entire server and keep for 365 days. This was completed after TSM conversion completion. <b>Agency: DAS</b> <b>Management status: Completed 12-31-2008</b>
1	ML#25: We recommend the department maintain a tape tracking database or spreadsheet to help ensure the physical location of all backup tapes is known at all times.	Completed. A rotation schedule was created to be able to track back up of tapes. Once backups are converted to OSS backup service, TSM, there will be no need for a rotation schedule. <b>Agency: DAS</b> <b>Management status: Completed 12-31-2008</b>

## OAKS Restructuring to Incorporate Managed Services

Priority	Auditor of State Recommendation	Management Response
2	ML#1: We recommend that OAKS complete the change request forms in their entirety before work commences on completing the changes/ Appropriate approvals should be obtained and documented at all stages of the program change cycle to ensure updated applications are operating as intended.	<p>A process for approving change requests on before work commences on completing the changes existed at the time of the audit. Since the audit, no change requests are processed without 100% of the required information and approvals.</p> <p>The OAKS Security Office will work with the MSV to develop a periodic review process to ensure compliance is met.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with a planned completion date of September 2009</b></p>
2	ML#3: We recommend OAKS follow the established program change documentation standards to reasonably ensure that all key documentation of testing performed for all program changes is maintained.	<p>Established program change documentation standards existed at the time of the audit. Since the audit, all key documentation in support of performed testing is maintained without exception.</p> <p>The OAKS Security Office will work with the MSV to develop a periodic review process to ensure that compliance is met.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with a planned completion date of September 2009.</b></p>
2	ML#5: We recommend OAKS ensure all program changes are properly tested, reviewed, and approved by management and documented approval is obtained before the changes are transferred into the live environment.	<p>A process for approving program changes to the “live” environment existed at the time of the audit. Since the audit, no program change requests are processed unless 100% of the program change testing results is reviewed and approved The OAKS Security Office will work with the MSV to develop a periodic review process to ensure compliance is met.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with a planned completion date of September 2009.</b></p>
1	ML#8: We recommend OAKS update comment log documentation for all changes to applications to reflect the current processes and procedures of their computer applications. In addition, a comprehensive evaluation of the current documentation for each application should be conducted to help ensure that all program changes have been made.	<p>Managed Services Vendor will address this issue with OAKS. During the transition phase to managed services, policies and procedures will be addressed. Undocumented policies and procedures will be formalized. Outdated policies and procedures will be updated to reflect the current and future operations.</p> <p><b>Agency: DAS</b>  <b>Management status: In process with a planned completion date of September 2009.</b></p>

## OAKS Restructuring to Incorporate Managed Services (Continued)

Priority	Auditor of State Recommendation	Management Response
2	ML#24: We recommend the Department develop, formalize, and approve standards and procedures for the entire batch processing change request.	<p><b>MSV has completed its review and development of batch processing procedures. They are being reviewed by OAKS Chief Information Security Officer.</b></p> <p><b>Agency: DAS</b></p> <p><b>Management status: In process with a planned completion date of September 2009</b></p>
2	ML#30: We recommend OAKS staff ensure controls are put into place to ensure the earnings dates on all manual checks correspond to the actual dates worked by employees.	<p>The MSV in collaboration with the State will address these recommendations with substantial changes in HCM coding. Payroll staff have been trained on what dates to use when preparing off-cycle checks. The Payroll supervisor runs a query each pay to identify and correct overpayments before they occur.</p> <p><b>Agency: DAS</b></p> <p><b>Management status: In process; to be determined</b></p>
2	ML#31: We recommend that management update the OAKS application to prohibit agency users from having the ability to manually enter combo codes outside their assigned agency.	<p>The MSV in collaboration with the State will address these recommendations with substantial changes in HCM coding.</p> <p><b>Agency: DAS</b></p> <p><b>Management status: In process; to be determined</b></p>
1	ML#2: We recommend OAKS sanitize all production data used in the testing environment to prevent the compromise of sensitive employee information.	<p>An assessment of the Oracle database has been performed by Accenture outlining which tables and their corresponding fields contain sensitive information. Per the contract with the MSV, non-production and non-QA environments will be sanitized. A process will be created that will perform data masking whenever non-production and non-QA environments are refreshed with production data.</p> <p><b>Agency: DAS</b></p> <p><b>Management status: In process with a planned completion date of September 2009</b></p>

## General OAKS Security

Priority	Auditor of State Recommendation	Management Response
2	<p>ML#10: We recommend OAKS ensure that all employees with access to electronic agency resources are required to sign an acknowledgement stating they understand and agree to adhere to OAKS workplace and IT Policies and Procedures.</p>	<p>A process exists to require employees acknowledge receipt and understanding of policies and procedures.</p> <p>A thorough review of employee acknowledgements has been performed.</p> <p>As part of the on-boarding procedure, the new OAKS IT Resource Form provides guidance requiring the signing of acknowledgements prior to the user gaining network access.</p> <p><b>Agency: DAS</b> <b>Management status: Completed 06-01-2008</b></p>
2	<p>ML#14: We recommend the Department utilize the IT access request forms to document and authorize the most current logical access assigned. In addition, the OAKS management should review all current users' forms to ensure access levels are documented and authorized. Finally, access reviews should be periodically completed to validate access is necessary for the users' job function.</p>	<p>Addressed during the audit.</p> <p>A thorough network access review has been completed. Quarterly access reviews will be performed by the OAKS Security Office.</p> <p>Finally, an updated OAKS IT Request Form was developed to provide guidance for both on-boarding and off-boarding procedures. No network access is granted before the DAS LAN Administrator receives and reviews this form.</p> <p><b>Agency: DAS</b> <b>Management status: Completed 06-01-2008</b></p>
1	<p>ML#26: We recommend the Department complete the formalized state-developed disaster recovery plan.</p>	<p>OAKS Management realizes that disaster recovery is a critical aspect to the success of the OAKS application and the State. OAKS will work with DAS/OIT, OBM and the managed service vendor to develop, implement and test a capable disaster recovery solution.</p> <p><b>Agency: DAS</b> <b>Management status: In process; to be determined</b></p>

## General OAKS Security (Continued)

Priority	Auditor of State Recommendation	Management Response
2	ML#20: We recommend OAKS take the necessary steps to ensure the physical card access list to the OAKS PMO is reviewed on a periodic basis to validate the need for user access.	<p>Addressed during the audit. A full review of the physical access to the building and the OAKS server room has been performed including a reduction in the number of individuals who have access to the server room. These accesses will be reviewed quarterly. The badge assignment documentation has been significantly upgraded and easily identifies employees who have access to the server room. Physical security services have been procured. Visitor access procedures have changed requiring sign-in and sign-outs. Building maintenance was notified of issues with the server room and the library. Work was performed on the ventilation system of the server room and the dead mold was cleaned. The library door still needs to be re-hung. However, the door will lock sufficiently with the proper care. Physical security checks the library door to ensure it is locked when they make their nightly visits to the PMO.</p> <p><b>Agency: DAS</b>  <b>Management status: Completed 06-01-2008</b></p>

## Requisition / Purchase Orders Created and Approved by Same User

Priority	Auditor of State Recommendation	Management Response
1	ML#32: We recommend OAKS_FIN Management ensure that changes are developed and implemented to restrict a user from creating an approving their own purchase requisition / order.	On January 23, 2009 the corrected workflow was put into production. Application Security Team to develop role assignment matrix to identify roles that cannot be combined. Consequently, requestors can no longer approve their own purchase requisition / order <b>Agency: DAS</b> <b>Management status: Completed 01-23-2009</b>

## Management of Physical Access

Priority	Auditor of State Recommendation	Management Response
2	<p>ML#21: We recommend ISD continue to review the physical access privileges for all users with 2nd floor computer room access. Work with the agencies to further restrict privileges to only those whose job functions warrant access. Additionally, steps should be taken to ensure the door between the ODJFS and main computer room is protected by physical access controls such as a card reader.</p>	<p>Mitigating actions have been taken to reduce the security risk: 1) OSS Server cabinets are locked, (2) WSS and UNS OAKS Cabinets that can be locked, have been locked, (3) One cabinet ( Cabinet 7) has no door. Door is being purchased for that cabinet as soon as possible. State Auditor noted that a single door was not locked during the time of their walkthrough. This door cannot be locked because it is a FIRE DOOR. This issue will not be acted on.</p> <p><b>Agency: DAS</b>  <b>Management status: Completed</b></p>
2	<p>ML#22: We recommend the SOCC security department track all requests for confirmation of the quarterly review of access. Batch Account password parameter settings should be modified to force password changes at least every 90 days.</p>	<p>Since the Audit, all security card access reports are completed electronically and agencies respond by sending back the reports with the changes indicated. Reports are now maintained for a minimum of one year.</p> <p><b>Agency: DAS</b>  <b>Management status: Completed</b></p>

## Duplicate HCM Payments Issued to Employees

Priority	Auditor of State Recommendation	Management Response
1	<p>ML#29: We recommend OAKS and the user entities take the necessary steps to recover amounts overpaid to employees. Devise and implement internal control procedures that provide reasonable assurance that payments are paid only once. We also recommend OAKS and user entities develop and implement policies and procedures to ensure duplicate / overpayments do not occur in the future and to help ensure data in HCM is accurate.</p>	<p>HRD Policy has developed a letter to send to employees owing monies to DAS. The Office of the Attorney General is reviewing the proposed letters to employees.</p> <p><b>Agency: DAS</b></p> <p><b>Management status: In process with a planned completion date of February 2009 / March 2009.</b></p>

## Warrant Writing Security

Priority	Auditor of State Recommendation	Management Response
2	ML#36: We recommend the Print staff begin recording the number of overflow checks on the OAKS Check Log so the Fulfillment Center staff will be able to reconcile their fulfillment logs to the check logs. Also the Fulfillment Center staff should be maintaining all documentation related to the processing of the OAKS warrants for at least one year to provide an audit trail.	<p>The fulfillment center log identifies how many pieces of mail resulted from the inserting process (used for postage) and is balanced with the total number of documents provided by state printing by fulfillment center personnel. The check log identifies the number of warrants, stubs and voids. The voids are returned to state printing by fulfillment personnel. The two logs are now reconciled. Logs maintained permanently.</p> <p><b>Agency: DAS</b> <b>Management status: Completed July 2008</b></p>
2	ML#37: We recommend the Department develop standardized procedures for tracking check stock inventory.	<p>Prior to the audit, state printing would confirm the number of warrant rolls received and the actual number of warrants used in printing. After the audit, state printing maintain a perpetual inventory record of all warrants noting receipt date, date printed and dated moved. The small stock of old inventory shredded. Physical bi-weekly warrant inspectors continued. Documentation of inspectors began January 2009.</p> <p><b>Agency: DAS</b> <b>Management status: Completed January 2009</b></p>
2	ML#35: We recommend the Department review the physical access privileges for all users of the Warrant Writing facility.	<p>DAS reviewed and updated the list of authorized users to the Warrant Writing facility. Warehouse gates kept locked All warrants kept in locked warrant cage. Void room restricted to personnel with individual keys. LAN Room - servers relocated to secured service racks. LAN room is closed and locked.</p> <p><b>Agency: DAS</b> <b>Management status: Completed January 2009</b></p>

## OBM Specific

Priority	Auditor of State Recommendation	Management Response
1	ML#34: We recommend OBM management develop and implement an approval process whereby the OBM management can validate the request for a chartfield value.	<p>OBM will maintain a list of the CFOs and designee for all agencies. The Chartfield Request forms will be changed requiring the CFO or designatee's signature. OBM will verify the signature before entering/changing the value in OAKS. Desk Procedures have been written to eliminate the risk of chartfield values being entered without the proper authorization and State Accounting Supervisor has implemented specific filing instructions.</p> <p><b>Agency: OBM</b>  <b>Management status: In process</b></p>
2	ML#38: We recommend OBM management ensure all reconciliations of EFTs are performed on a daily basis.	<p>This has been corrected. These files are currently being verified each pay cycle to ensure all documentation is in the file. Also this procedure was enhanced in November 2008 with the implementation of a comprehensive treasury management report.</p> <p><b>Agency: OBM</b>  <b>Management status:</b>  <b>Completed November 2008</b></p>