OAKS HUMAN CAPITAL MANAGEMENT (HCM) & FINANCIALS (FIN) WARRANT WRITING AND EFT

ISA, FRANKLIN COUNTY

SAS - 70

JULY 1, 2009 THROUGH JUNE 30, 2010

Mary Taylor, CPA
Auditor of State

TABLE OF CONTENTS

This Page Intentionally Left Blank

Mary Taylor, CPA
Auditor of State

INDEPENDENT ACCOUNTANTS' REPORT

To the Department of Administrative Services, (DAS) and the Office of Budget and Management, (OBM):

We have examined the accompanying description of controls of the state of Ohio applicable to the processing of transactions for users of the Ohio Administrative Knowledge System (OAKS) Financials (FIN) and the OAKS Human Capital Management (HCM-payroll). We also examined the accompanying description of the Warrant Writing and Electronic Fund Transfer (EFT) controls applicable to the processing of warrants and EFTs for OAKS. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the state of Ohio's controls that may be relevant to a user agency's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user agencies applied the internal controls contemplated in the design of the state of Ohio's controls; and (3) such controls had been placed in operation as of June 30, 2010. The control objectives were specified by DAS for OAKS FIN, HCM, and Warrant Writing, and OBM for EFT. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of the DAS, and OBM controls that had been placed in operation as of June 30, 2010. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of DAS and OBM's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the preceding paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from July 1, 2009 to June 30, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user agencies and to their auditors to be taken into consideration along with information about the internal control at user agencies, when making assessments of control risk for user agencies.

The description of controls states that access to update OAKS PeopleSoft access security rights is restricted to valid users and that access to OAKS system administrator privileges and privileged commands is restricted and logged. It also states that access to the production OAKS databases is restricted to valid users. Our tests of operating effectiveness noted that access to update OAKS access security rights was not restricted to only those individuals whose job responsibilities require it, logs of privileged UNIX commands were not consistently maintained, and access to the production OAKS databases was not restricted to only valid users. These issues resulted in the nonachievement of the control objective, "Use of master passwords, powerful utilities, and system manager facilities should be adequately controlled."

The description also indicates that access to update the vendor database is appropriately restricted. It indicates that only authorized personnel can make changes to the OAKS chartfields. It also indicates OBM documents and approves all changes and modifications to the fund, account, ALI, and ISTV Xref chartfields. Our tests of operating effectiveness noted that users had access to update the vendor database that was not required for performance of their job responsibilities. In addition, not all chartfield changes were supported by documentation and not all users with access to make these chartfield changes had job duties to warrant the access. These deficiencies in aggregate resulted in the non achievement of the following control objective, "Changes to standing data are authorized and accurately input."

In our opinion, except for the matters described in the preceding paragraphs, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from July 1, 2009 to June 30, 2010.

The relative effectiveness and significance of specific controls at DAS and OBM and their effect on assessments of control risk at user agencies are dependent on their interaction with the controls and other factors present at individual user agencies. We have performed no procedures to evaluate the effectiveness of controls at individual user agencies.

The description of controls at DAS and OBM is as of June 30, 2010, and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2009 to June 30, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at DAS and OBM is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the DAS and OBM and their user agencies, and the independent auditors of those user agencies.

Mary Taylor

Mary Taylor, CPA
Auditor of State

October 6, 2010

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

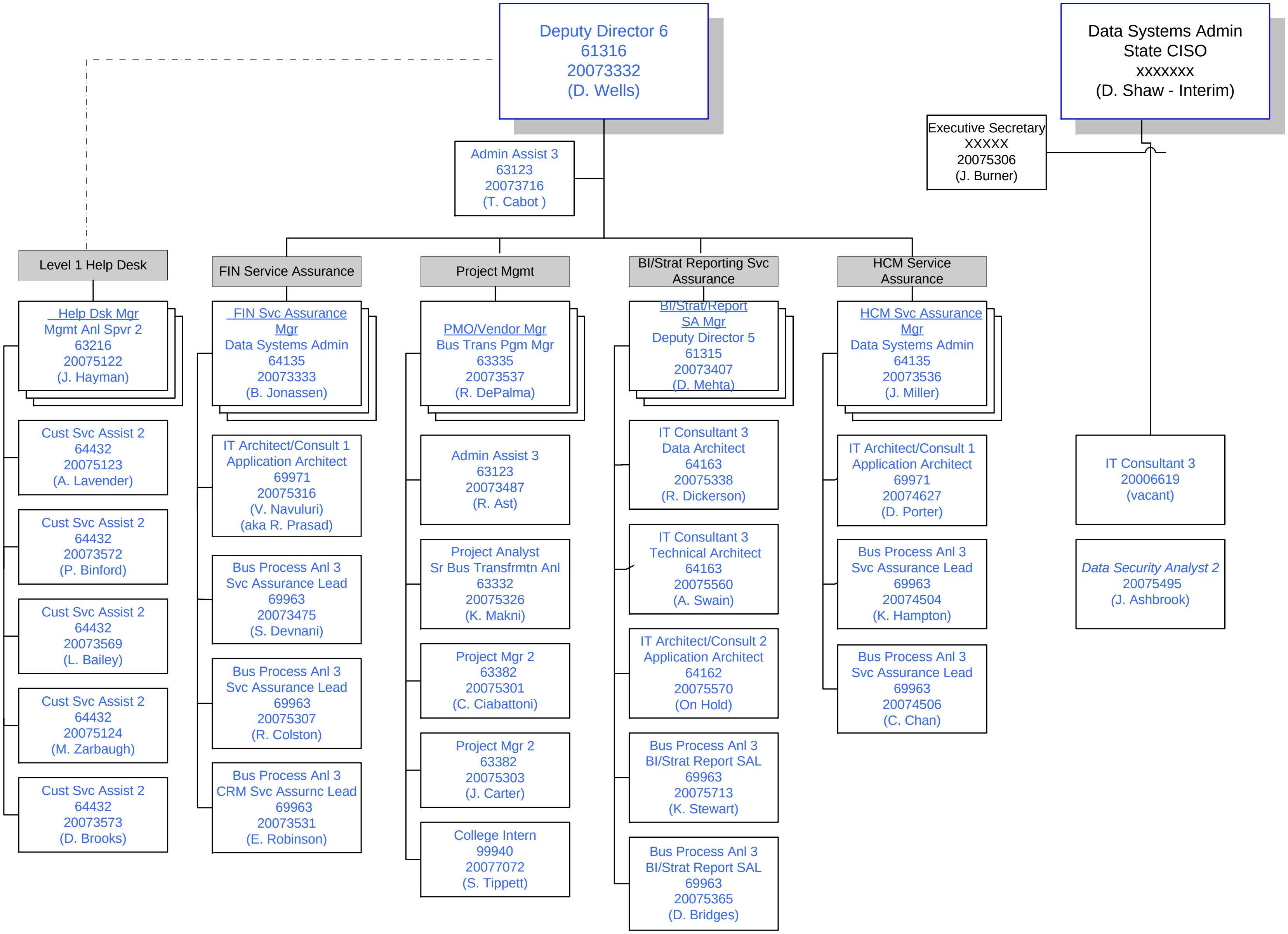
The OAKS control objectives and related controls are included in Section III of this report, “Information Provided by the Service Auditor,” to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the OAKS description of controls.

OVERVIEW OF OPERATIONS

The Ohio Administrative Knowledge System (OAKS) is an online enterprise resource planning application that integrates the following major business functions for Ohio: capital improvements, financials, fixed assets, human resources, and procurement. The Department of Administrative Services (DAS), the Office of Budget and Management (OBM), the Office of Information Technology’s (OIT) Infrastructure Services Division (ISD), and the Accenture Managed Service Vendor are all partners in the administration and operation of OAKS. The following OAKS project management office (PMO) has been created and is responsible for oversight and management of the OAKS application.

NOTE: OAKS is commonly referenced in two different fashions. OAKS is the HR and financial application software that replaced the state’s legacy HR and accounting systems. For purposes of this report, OAKS will not pertain to an entity, but to the software. This report will refer to OAKS management or staff that administers, secures, maintains, and operates the OAKS software as DAS/OIT.

OAKS Project Management Office



Deputy Director 6
61316
20073332
(D. Wells)

Data Systems Admin
State CISO
XXXXXXX
(D. Shaw - Interim)

Executive Secretary
XXXXX
20075306
(J. Burner)

Admin Assist 3
63123
20073716
(T. Cabot)

Level 1 Help Desk

Help Dsk Mgr
Mgmt Anl Spvr 2
63216
20075122
(J. Hayman)

Cust Svc Assist 2
64432
20075123
(A. Lavender)

Cust Svc Assist 2
64432
20073572
(P. Binford)

Cust Svc Assist 2
64432
20073569
(L. Bailey)

Cust Svc Assist 2
64432
20075124
(M. Zarbaugh)

Cust Svc Assist 2
64432
20073573
(D. Brooks)

FIN Service Assurance

FIN Svc Assurance Mgr
Data Systems Admin
64135
20073333
(B. Jonassen)

IT Architect/Consult 1
Application Architect
69971
20075316
(V. Navuluri)
(aka R. Prasad)

Bus Process Anl 3
Svc Assurance Lead
69963
20073475
(S. Devnani)

Bus Process Anl 3
Svc Assurance Lead
69963
20075307
(R. Colston)

Bus Process Anl 3
CRM Svc Assurnc Lead
69963
20073531
(E. Robinson)

Project Mgmt

PMO/Vendor Mgr
Bus Trans Pgm Mgr
63335
20073537
(R. DePalma)

Admin Assist 3
63123
20073487
(R. Ast)

Project Analyst
Sr Bus Transfrmtn Anl
63332
20075326
(K. Makni)

Project Mgr 2
63382
20075301
(C. Ciabattoni)

Project Mgr 2
63382
20075303
(J. Carter)

College Intern
99940
20077072
(S. Tippett)

BI/Strat Reporting Svc Assurance

BI/Strat/Report SA Mgr
Deputy Director 5
61315
20073407
(D. Mehta)

IT Consultant 3
Data Architect
64163
20075338
(R. Dickerson)

IT Consultant 3
Technical Architect
64163
20075560
(A. Swain)

IT Architect/Consult 2
Application Architect
64162
20075570
(On Hold)

Bus Process Anl 3
BI/Strat Report SAL
69963
20075713
(K. Stewart)

Bus Process Anl 3
BI/Strat Report SAL
69963
20075365
(D. Bridges)

HCM Service Assurance

HCM Svc Assurance Mgr
Data Systems Admin
64135
20073536
(J. Miller)

IT Architect/Consult 1
Application Architect
69971
20074627
(D. Porter)

Bus Process Anl 3
Svc Assurance Lead
69963
20074504
(K. Hampton)

Bus Process Anl 3
Svc Assurance Lead
69963
20074506
(C. Chan)

IT Consultant 3
20006619
(vacant)

Data Security Analyst 2
20075495
(J. Ashbrook)

More than 140 agencies, boards, commissions, colleges, and universities throughout Ohio use OAKS to perform functions such as payroll, human resources, reporting, budgeting, accounting, procurement, and asset management. OAKS can be accessed using a standard web browser.

In May 2005, the Accenture LLC consulting firm was awarded the contract to serve as the OAKS integrator. The integrator's role was to help lead the development of the OAKS project until July 2009 when all designed enterprise modules of the OAKS project were successfully developed, tested, and migrated into production. During the first quarter of fiscal year 2008, the OAKS project started the transition to a steady state operation forming a new division within the Department of Administrative Services. An OAKS management team was formed and assumed responsibility for the development, security, and operation of the OAKS development, test, and production environments. The OAKS DAS/OIT team worked in conjunction with Accenture and state employees from various agencies in the ongoing development and maintenance efforts.

The OAKS programs and data resided in development, test, and production environments during the various stages of the OAKS system development. The North American Delivery Center (NADC) was used by Accenture as the OAKS development and test environments until September 2008. During fiscal year 2009, the State of Ohio Computer Center (SOCC) in Columbus housed the production servers that use the PeopleSoft enterprise resource planning (ERP) programs to process all the OAKS HR and financial data. The SOCC also housed the quality assurance servers for testing of all OAKS program changes and the servers that contain the OAKS data warehouse environment. The data warehouse is a “mirror image” repository of; the production environment data designed to facilitate state reporting and analyses. Because it is separate from the production environment, it provides retrieval of OAKS data without slowing down daily production processing.

The SOCC also houses the data processing facilities for many of the agencies, boards, commissions, colleges, and universities. The SOCC was designed to provide a state-of-the-art computer facility to provide maximum protection for the state's computer resources necessary to process the government's transactions. The building has been designed to solve the major electrical, design, and security problems germane to the operation of large data centers. The building has state-of-the art security, back-up power, and climate control systems and is dedicated to the data processing for state agency customers only.

The SOCC is operated by OIT/ISD. ISD employs a staff of over 100, primarily system programmers, network professionals, and computer operators. In an average month, the ISD staff handles 4,000 calls to the help desks, installs network lines and terminals, maintains an inventory of more than 200,000 magnetic tapes and cartridges, and distributes over 950 miles of printed output.

The Office of Information Technology provides governance and management of information technology functions of state agencies under the authority of the Governor. The Office of Information Technology is led by the State Chief Information Officer (CIO).

To address the challenges of continued service delivery in support of OAKS and to help create an OAKS organization that can effectively support current and future business needs, the State contracted with a vendor to perform an assessment of the strengths, weaknesses and managed services opportunities available for OAKS. Subsequent to the assessment, the state issued an RFP, awarded a contract, and began the transition process to a managed service provider.

The state contracted with Accenture to serve as the managed services provider responsible for the OAKS infrastructure, data center operations, application development, application testing and application administration.

State employees retain management of the OAKS functions where significant knowledge and understanding of state-related operations is required. This includes strategy, governance, business interfaces and other customer-facing support functions.

OAKS began operating under a managed services model on June 22, 2009. The Managed Services group, operated and managed by Accenture, took over key functionality related to application security administration, day-to-day application management, and new development. Some of these key functions include:

- Performing all OAKS application coding changes.
- Performing required unit and system testing before migration into production.
- Migrating changes into production.
- Documenting the program changes.
- Deleting, adding, or changing user access rights, per approved agency requests.
- Resetting passwords.

In September 2009, the Managed Services group took over the physical and logical security, operation, and administration of the OAKS production servers.

As part of this change to a managed services model, the physical locations of the OAKS environments also changed. In February 2010, the OAKS production servers were transferred to the NADC, the SOCC began hosting the OAKS QA environments as well as the State's new disaster recovery environment, and the development environment was housed at the State Office Tower.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, AND MONITORING

Control Environment

During the audit period, the data processing of the OAKS data submitted by the state entities and processed by the OAKS ERP software was administered, secured, and operated by a combination of State Service Assurance personnel, OSS, and the Managed Service vendor. These state entities included approximately 150 state agencies, boards, and commissions. Major state agencies included the Department of Job and Family Services, the Lottery Commission, the Department of Administrative Services, the Department of Health, Department of Education, Office of Budget and Management, Department of Mental Health, Department of Health, Department of Public Safety, Department of Transportation, Department of Youth Services, Rehabilitation and Corrections, and Mental Retardation and Developmental Disabilities.

OAKS production hardware, system software and ERP programs and data were housed at the SOCC until February of 2010 at which time they were moved to the NADC CBTS center in Cincinnati, Ohio. While at the SOCC, ISD was the group responsible for providing Internet, electrical, and telecommunications services. In August 2009, the managed services vendor took over responsibility for managing the OAKS infrastructure as well as providing all administration, security and operational support for OAKS processing.

The state agencies, boards, and commissions enter their HR and financial data from their respective local area networks (LANs) into OAKS. These LANs are all attached to the ISD network, known as ohio.gov. This WAN is linked to the wide-area data and video communications network (WAN). OIT’s Unified Network Services division administers and controls this network, providing metropolitan and local area network services to state agency customers. OAKS users are responsible for authorization and initiation of all of their transactions. OAKS management encourages the deployment of agency-level security administrators to assist in the security administration and control of the agency’s users of the OAKS computer resources.

An OAKS Governance Charter has been created to help guide the overall Governance of the managed services contract and operations of OAKS in support of the State’s mission. The charter defines the governance vision, mission, and critical success factors.

The vision statement of the OAKS Governance Charter is: “To be seen by our customer as a high performing solution that provides superior customer service in leading the State’s Enterprise Resource Planning services.” The mission of the OAKS Governance Charter is: “To improve the effectiveness, efficiency, and integration of state government business functions through an Enterprise Resource Planning system while supporting business initiatives and requirements.”

The OAKS Governance charter describes the OAKS Executive Board, Steering Committee, and Change Control Board. These board seats are filled with state project leads who are responsible for the oversight of the Accenture contracted staff. The contract between the State and Accenture specifically lists the responsibilities of the contractor and the responsibilities of the State, including transition services, technology updates and refresh, steady state run services, infrastructure management services, program management services, and termination services. Security is embedded in each section of the responsibilities.

The OAKS Executive Board is comprised of directors from DAS, OBM, and the Ohio Department of Job and Family Services (ODJFS), a representative from the Ohio Department of Insurance (INS), the state CIO and the OAKS Executive Program Manager. The Board’s first meeting was October 8, 2009. The board meets quarterly and is responsible for business oversight, approval for “large” projects, and issue and risk management escalation.

The OAKS Steering Committee is comprised of representatives from OAKS, OBM Budget, State Accounting, DAS/HR, Asset Management, OAKS PMO Lead, Shared Services Lead, Treasurer of State's Office, and the Attorney General's Office. The initial meeting was in April 2009. The committee meets monthly and is responsible for the overall strategic IT portfolio/program oversight, issue and risk management, and approval for "large" discretionary change requests. The Steering Committee reports to the OAKS Executive Board.

The OAKS Change Control Board, formed in April 2009, is comprised of representatives from OAKS; Business Process Owners, including: State Accounting, Budgeting, Procurement, HRD, and Shared Services Operations Lead; Service Assurance Leads, including: Finance, HR, and the Lead Architect. The board meets bi-weekly and is considered a central point of entry and "logging" for all system changes. The board is responsible for approval of "small" discretionary change requests. The board also is responsible for analysis of "large" discretionary requests, and making recommendations to Steering Committee for approval of the large requests.

OAKS developed a draft Information Security Strategic Plan with a mission, vision, guiding principles, governance, organizational structure, and roles and responsibilities. OAKS also developed an Enterprise Application Roadmap document for FY2009-FY2014. The roadmap contains plans for HRD, Finance, Enterprise, Technology, and other business applications, with the following criteria: Business Objectives, Sponsoring Agency, Sponsor Name, Service Assurance Lead / Other Lead, Funded Dollar Amount, Business Case Completed, Start Date, and End Date. Although DAS, OBM, and OIT have developed long-range IT plans that include some OAKS planning; a strategic IT plan that addresses all requirements in accordance with State of Ohio Policy ITP-D.4 was not prepared for fiscal year 2010.

Additional oversight is provided through the State Audit Committee. The State Audit Committee was formed in September 2008 through the authority of Sub. H.B. 166 and meets quarterly. The State Audit Committee charter states that "the Committee exists to assist the Governor and Director of the Office of Budget and Management ("OBM") in fulfilling their oversight responsibilities in the areas of financial reporting, internal controls and risk assessment, audit processes, and compliance with laws, rules, and regulations." The State Audit Committee has five members - one public member appointed by the Governor; two public members appointed by the Speaker of the Ohio House of Representatives, and two public members appointed by the President of the Ohio Senate.

OBM formed the Office of Internal Audit (OIA) during 2008 under the authority of section 126.45 of the Ohio Revised Code. The OIA reports to their Chief Audit Executive (CAE), who reports administratively to the OBM Director and in an advisory capacity to the State Audit Committee.

The OIA was established with the purpose of providing state agency management and the State Audit Committee with a systematic, disciplined approach to evaluate agency information, internal controls and governance processes. The OIA is responsible for monitoring 21 state agencies and departments.

The OIA submits an annual risk-based audit plan to the State Audit Committee for review and comment, periodically provides information on the status and results of the audit plan, and coordinates with other internal and external control and monitoring functions.

DAS and OBM follow the DAS human resource policies, directives and executive orders from the Governor's office and the OIT IT policies. Background checks are required for new employees. When a new employee or contractor begins working at DAS/OIT, they receive and acknowledge the OAKS/DAS Work Rules and Policies. Contractors are also required to sign a non-disclosure agreement.

Roles and responsibilities are defined through organization charts and written job descriptions. The DAS/OIT organizational structure allows for direct reporting of staff to a team lead for the various areas and the team leads report to the deputy director. DAS/OIT follows the DAS performance evaluation policy and completes evaluations on an annual basis. Although a formalized continuing education policy or training policy was not in place DAS/OIT employees attend training as needed. OAKS Service Assurance employees attended ethics training during the period as required by the Governor’s office.

The DAS/OIT has been lead by the current Executive Program Manager since March 3, 2008. Staffing at DAS/OIT has been relatively stable during FY 2010.

Staffing with the managed services vendor has been fluid throughout the fiscal year. Much of this can be attributed to transitioning the production environment to the new data center in Cincinnati Ohio. The OAKS PMO maintains a listing of all staff (employees and contractors) brought onto the project with their on-boarding and off-boarding dates.

Risk Assessment

The position of the state's CIO provides statewide oversight and leadership for all activities related to information technology including strategic IT planning, data processing, telecommunications, and systems development. The CIO is responsible for optimizing the uses of IT resources, and assuring the state's investment achieves planned programmatic objectives.

The Office of IT Policy reviews long-range IT plans for all state agencies, as required by DAS. These plans outline future IT initiatives and forecasts for upcoming fiscal years. These long-range plans address and are not limited to the following:

- Changes in operating environment.
- New personnel.
- New or revamped information systems.
- Rapid growth.
- New technologies.
- New lines, services, or activities.

Upon reviewing the findings of an external review performed in July of 2007, the state hired a chief information security officer (CISO) to oversee security practices of the OAKS program and data. In October 2009, the State CISO employed a Deputy CISO to oversee those operations and the OAKS security operations team transitioned to reporting through this structure. The State CISO resigned in January 2010 and the deputy CISO was subsequently appointed interim CISO.

Monitoring

During the audit period, State Service Assurance personnel and the Accenture managed service vendor were responsible for the administration and monitoring of the OAKS application. As of the beginning of fiscal year 2010, Accenture was in charge of the development, testing, implementation, administration, security, and operation of the OAKS software project. Monitoring of the project during the fiscal year 2010 was also conducted by OBM's Office of Internal Audit (OIA) and the DAS Office of Finance – Compliance and Financial Reporting Unit.

The OAKS ERP software is monitored by the Managed Services Vendor as a normal part of their activities. The various monitored events include:

- Antivirus detections
- OAKS firewall access violations
- Computer security violations
- Physical/environmental security events of the PMO network room
- System availability
- Database performance, administration, and security incident events
- Production batch schedule problems

INFORMATION AND COMMUNICATION

The OAKS website provides information and links to procedure manuals, job aids and forms, and other information helpful to users. Information about the system status and other current topics are communicated on the website through alerts. These alerts announce various system modifications, enhancements and outages, new job aid postings, OAKS system availability, and other helpful information suggested by members of the OAKS program management office (PMO). In addition to being posted on the OAKS website, these items are emailed to the agency liaisons and agency leadership, as appropriate. All OAKS alerts, dating back to December 2006, are archived and available on the Web for OAKS users to review.

OAKS management provided web-based training during the audit period to all OAKS users. Training was available for FIN, HCM, general ledger, accounts payable, accounts receivable, billing, budget, asset management, payroll, time and labor, purchasing, data warehouse,

Additional aspects of the information and communication component of internal control as they affect the services provided to state entities are also discussed within the General EDP and Financial Application control sections.

GENERAL EDP CONTROLS IN THE PEOPLESOFT/UNIX ENVIRONMENT FOR OAKS

The following general controls apply only to the OAKS application. They have been outlined here to provide a more complete understanding of the EDP control environment related to the maintenance, security, administration, and operation of the OAKS application.

Changes to Existing Applications and Systems

OAKS uses a structured process to monitor and authorize changes to the OAKS production environment. Beginning in March of 2010 all changes (Applications and Infrastructure) go through the change management process as detailed in the Change Management Process Document. Prior to that, changes for applications followed a process where SA leads worked with the functional areas to gain approvals for proposed changes while the infrastructure changes followed the current change management process.

DAS/OIT has a documented formal program change request process in place for the FIN and HCM applications to ensure changes are properly processed and to help ensure proper segregation of duties.

The Production Support team meets periodically to discuss all aspects of the FIN and HCM production application changes. The HCM SA team, HRD and MS team meets every day on processing weeks and once a week on non-processing weeks. The FIN team meets once a week.

Program enhancements are initiated through SMS (Accenture Service Management Suite) tickets and modifications are initiated through the CRM cases created by Service Assurance team members. The HCM Development Team completed/closed 150 CRM break/fix and enhancement cases during FY10. The FIN Development Team completed/closed 194 CRM break/fix and enhancement cases during FY10.

Application:	Number of Programs / Objects	Number of Programs / Objects Changed in FY10	*Number of Major Program Changes in FY10
FIN	337,152	624	36
HCM	220,037	328	100

NOTE: Objects refer to codes and scripts that support the PeopleSoft application. The number of HCM programs/objects that changed included fields, records, pages, components, menus, application engine programs, and PeopleCode programs. The number of FIN program changes included records, pages, components, menus, application engine programs, and PeopleCode programs. The number of major program changes includes those changes for which a formal change request (SMS) was completed and targeted for the production environment. An SMS is completed for all enhancements, and for break fixes which require changes to HCM code.

DAS/OIT requires an SMS ticket/ CRM case initiated by the requestor through PeopleSoft Accenture Service Management Suite or CRM application for all standard FIN and HCM enhancement and modification changes. The SMS tickets and CRM cases are prioritized and assigned to Managed Services Vendor (MSV) for completion. Anyone with access to the Accenture Service Management Suite or the CRM application is able to submit a change for consideration. The OAKS FIN and HCM Service Assurance teams and functional teams will then determine whether the change should be approved for implementation. OAKS modifications and enhancements must be approved by the appropriate OAKS Service Assurance teams before the program change begins. If the request is determined feasible for completion, the modifications and/or enhancements are prioritized and assigned to the MSV for completion.

OAKS utilizes vendor software along with a SharePoint tracking log to monitor and track all FIN and HCM code changes. Approvals are attached to the SharePoint tracking log to indicate approval to move changes forward to production. ITG is used to submit production migration requests which are approved by the respective MS Lead.

Vendor-Provided Changes

PeopleSoft Maintenance Packs, PeopleSoft Tax Updates, and OAKS Releases are vendor support changes to OAKS that do not follow the standard program change request process. Some characteristics are as follows:

Maintenance Packs:

- Required to be installed by the client.
- Delivered by PeopleSoft with fixes and minor enhancements between service packs of a major or minor application release for the core PeopleSoft code.
- A CRM case is *not* required to be completed because they are required to be installed.
- Not required to be prioritized, assigned, or authorized because they are required to be installed.
- MSV reviews the current workload of the development teams and schedules a date for the Maintenance Packs to be installed. Work relating to these Maintenance Packs is assigned based on an assessment of individuals' workloads.

Tax Updates:

- Required to be installed by the client.
- Deliver legislative changes for PeopleSoft Enterprise HRMS North America Payroll. The resulting changes are delivered only for supported major and minor releases, for as long as the major or minor release is supported.
- A CRM case is *not* required to be completed because they are required to be installed.
- Not required to be prioritized, assigned, or authorized because they are required to be installed.
- MSV reviews the current workload of the development teams and schedules a date for the tax updates to be installed. Work relating to these tax updates is assigned based on an assessment of individuals' workloads.

OAKS Releases:

- Required to be installed by the client.
- Major enhancements to the existing OAKS system, which include added functionality to the existing OAKS modules.
- Change Requests (CR) and general documentation is completed and maintained for OAKS Releases because they are agreed upon major enhancements to the OAKS system.

System Software Changes

OAKS has developed guidelines for the implementation of system software. The guidelines include procedures for tracking, obtaining, and applying patches and upgrades (network and UNIX, etc.), fix bundles, etc., as well as patches and minor upgrades to operating systems and other system software deployed by OAKS.

Testing of Program Changes

Formal written guidelines exist to define test procedures, strategies, and requirements for maintaining documentation of OAKS program changes. Program changes are tested by IT staff to help ensure that they will function as intended in the live environment. OAKS restricts access to the test environments to authorized personnel. In addition, the software used to maintain the OAKS program code has an automated lockout feature that prohibits multiple programmers from making simultaneous changes to the same program. DAS/OIT refreshes the testing environment every two weeks from a production backup. Confidential Personal Information (CPI) as defined by Ohio Revised Code has been masked within the development environment.

The approval of the requestor, Service Assurance, is required on all OAKS testing before acceptance of the program change. The approval is provided via e-mail and is documented in the Production Control Log (PCL) on SharePoint. The sign-off is maintained electronically within the Mercury ITG request software and also in the PCL on SharePoint.

Testing documentation is maintained for all OAKS program changes. Unit testing for each change is performed by the respective FIN and HCM application development teams. Software changes undergo various types of testing, depending on the nature of the change request. The State Functional teams complete user acceptance testing (UAT). Once the UAT is completed the respective State Functional Team signs off on the change via e-mail to document approval.

Migration to Production

OAKS utilizes vendor software to monitor and track all FIN and HCM code changes to the production environments. Code changes are migrated via a request type within ITG called, “Prod OMR”, which stands for Production Object Migration Request. The Prod OMR form is stored in a database and currently has no archive / purge restrictions in place (i.e. retained indefinitely). The ITG administrator role was set up and granted to key management to allow the assigning of access to staff and to maintain program change documentation and procedures.

Access to the OAKS production servers is restricted through UNIX security. Programmers and developers are restricted from having access to the production environments to help ensure programs are migrated by individuals independent of the development group. The FIN/HCM development lead and Service Assurance approval is required before a program is transferred into production. The FIN lead and MS designees have the authority to approve and submit FIN object migration requests. If the FIN leads are not available, one of the sub-team leads will submit FIN object migration requests in their absence.

The HCM lead and MS designees have the authority to approve and submit HCM object migration requests. If the HCM leads are not available, one of the sub-team leads will submit HCM object migration requests in their absence.

Once Quality Assurance (QA) testing is completed by the functional team, approval is sent by the tester and the approval is attached in the Production Control Log (PCL). Service Assurance will also provide their signoff based on the QA testing results and that leads to a PCL entry that is created. For FIN, one of the FIN development leads will approve the program change to be moved into production. Similarly for HCM, one of the HCM development team leads will approve the program change to be moved into production. The program(s)/file(s) are then moved to the “staged” environment.

Once a request to migrate a tested and approved program into production is submitted, it appears on the Mercury Dashboard Front Page for review by the request originator. The request originator will review to ensure the request is properly completed with all necessary information, update the request as needed, and resubmit the request within Mercury ITG.

When the ITG change analyst has all the needed information, they approve the request and submit it to a PS Admin to move the program into the requested production environment. A PS Admin will migrate the program(s)/file(s) to the proper production environment, note the migration in the related program change request in Mercury ITG, and mark the task completed. The migration request is then inspected to ensure the program(s) were migrated into the correct production environment.

Post Migration

Once the program change is migrated to production, the ITG Change Analyst closes the change request and an e-mail is sent to the change requestor with notification that the program has been moved into production. An individual from the functional/development teams ensures the change was migrated properly and working in production.

When changes are implemented into production, prior versions of each Structured Query Reporter, (SQR) and Structured Query Command, (SQC) object are available to be restored using Mercury ITG in the event of an emergency. These objects support the PeopleSoft application and are key to the restoration and functioning of the OAKS application in the event of an emergency. When changes are made to any type of online object or to COBOL code, a separate version is not maintained. The old code is commented out and left in the program and the new code is added.

Documentation standards are available to the OAKS development teams to follow to enhance and maintain PeopleSoft objects. The comments section of the PeopleSoft application code is updated to reflect a detailed description of the program change(s) made. FIN and HCM Production Support developers also insert comments in the header portion of the relevant program with technical documentation for each coding change. Program changes are documented within the program code and/or developer’s packets. Developer’s packets are maintained by SMS number and document the affected programs, changes to source code, and testing scenarios/results. Systems documentation is also updated to reflect program or system changes along with a cross-reference to supporting program change documentation.

Notification of program changes, documentation, and training, are provided to affected users.

IT Security

Security and IT Policy

Security management for the OAKS system is handled by the Office of Information Security and Privacy (ISP), under the Direction of the State Chief Information Security Officer. In October of 2009, the ISP hired a Deputy State CISO to manage the OAKS security operations team. The Managed Services Vendor completed and provided a gap analysis document to the state to show where the NADC and overall OAKS environment may not be aligned with the NIST (National Institute of Standards and Technology) 800-53 framework. While there is still work to be done in this area, there have been advances made with compliance to the NIST framework.

DAS/OIT has an application security policies and procedures document to outline user responsibilities for OAKS application security and access.

IT security policies and procedures are in place to guide the security and administration of the OAKS infrastructure application. OAKS systems are expected to be compliant with OIT/DAS policies as a minimum standard. At times, the vendor may require a more stringent control than is currently required by the state.

All employees and contractors assigned to OAKS are required to sign an acknowledgement of state IT policies related to data security as part of the initial condition of employment or assignment.

To help restrict unauthorized OAKS FIN and HCM usage, a security notice/banner screen is displayed prior to logging into the FIN and HCM modules that states: “OAKS is a State of Ohio computer system, which may be accessed and used only for official state business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.”

FIN and HCM Access Requests

From July 1, 2009 to approximately May 5, 2010 State agencies, boards, and commissions document, authorized and submitted all FIN access using a Security Request Form. DAS/OAKS worked with each agency to establish security designees at each entity. The role of these security individuals was to request access for their agency employees requiring access to FIN. Once the Security Request Form was documented and authorized, the form was submitted to the OAKS FIN Security e-mailbox. DAS/OAKS security personnel then grant the requested user access and confirm back to the agency the access that was actually granted. Beginning approximately May 6, 2010, the FIN PeopleSoft application was customized to allow for the appropriate Security "Designees" to request and approve all access for individuals within the agency. The Online Security Request process replaces the soft copy “paper-based” forms and helps to streamline the process of granting FIN access. All FIN Online Requests are fulfilled in real-time; however, if a request is entered that requires a higher level of approval; a workflow approval process is available to follow.

The HCM PeopleSoft application has been customized to allow for the appropriate Security "Designees" to request and approve all access for individuals within the agency. This prevents manual intervention by the PeopleSoft Security Administrators to grant the security. In HCM, an overnight batch program processes any requests that were made that day. If a request is entered that requires a higher level of approval; a workflow approval process is available to follow.

Terminations

When an OAKS user is terminated, the security automation program will identify the terminated user and remove the user’s access from the application.

HCM

All non-self-service roles are removed from the user’s account by SQL statements run via the Security Automation Program. The appropriate self-service roles remain on their profiles, so that they may still review paychecks as needed for tax purposes, etc.

FIN

All roles are removed from the user’s account and the user’s account is locked by SQL statements run via the Security Automation Program. The only exception to this rule is for workflow related roles, which may remain on a user’s profile until the appropriate workflow items are transferred by the Workflow support team. Once the workflow has been transferred the Requirements and Configuration Management (RACM) team manually removes the rest of the roles from their User Profile.

OAKS MS Contractor / OAKS Related Project Contractor Roll-Offs

ALL SYSTEM ACCESS

If the OAKS contractor has access to any of the OAKS systems, then the manager/PMO of the contractor is responsible for entering a CRM request to have the employee removed from all of the systems indicated above. Once the CRM request has been made the Accenture service desk is responsible for creating ITSM tickets and assigning them to the correct team(s) to have the contractor access removed from the other systems.

Agency Contractor Roll-Offs

PEOPLESOFT ACCESS

HCM

The Agency Security Liaison is responsible for requesting removal of their access using the online security request form.

FIN

The Agency Security Liaison is responsible for requesting removal of their access using the online security request form.

ALL OTHER SYSTEM ACCESS

On the rare occasion these agency contractors have access to any of the OAKS systems aside from PeopleSoft, then the manager/PMO of the contractor is responsible for entering a CRM request to have the employee removed from all of the systems indicated above. Once the CRM request has been made the Accenture service desk is responsible for creating ITSM tickets and assigning them to the correct team to have the employee removed from the other systems.

Periodic Review of Access

One of the key aspects of managing security is implementing monitoring that shows security controls are being followed. Several monitoring activities are in place to deal with this. OAKS personnel audit the change control process on a monthly basis. ‘Back-office’ or direct access was being reviewed quarterly until late in calendar year 2009. This is when the state and the MSV began the process of doing a complete system audit to inventory all users and their respective access rights. The first step in this process was to ensure that any user accounts for people no longer on the project were put into a specific category to disable access and ensure that they are easily identifiable when it comes time to remove them from the system. By the end of FY 2010 the security operations group plans to have the audit completed and user inventories distributed for management approval. Quarterly audits will begin again once the current audit has finished. The various audits under the monitoring program are discussed in more detail below.

Semi-Annual Security Review:

FIN and HCM PeopleSoft accounts are reviewed periodically to determine appropriateness of access and to eliminate unnecessary accounts. The OAKS Security Team is scheduled to request lists that contain all users in the agencies with access to the HCM and FIN applications and the exact access they have. This includes Business Unit (BU) access, role assignments, and workflow information. The lists are given to the OAKS Service Assurance teams for distribution to the agency security designees who must then review this information and submit any changes that are necessary to clean up security within their agency. The OAKS Service Assurance teams are responsible for tracking the status of each agency and ensuring the task has been completed. OBM has reserved the right to revoke FIN application access for a full agency if they do not complete any security tasks that have been assigned to them.

OAKS LAN Network (G-drive) Review:

At least quarterly the OAKS Security Team requests a list of all the current OAKS network user accounts from the DAS network administrator and reviews the accounts to determine whether the user accounts belong to individuals who are still associated with OAKS and submits the necessary changes via OIT Helpdesk ticket requests.

OAKS Database Access Review:

At least quarterly, the OAKS Security Team requests a list of all the user accounts in the OAKS databases from the Managed Services Provider and reviews the accounts to determine whether the user accounts belong to individuals who are still associated with OAKS. The OAKS Security team reviews the lists for accounts that were not properly processed for Off-Boarding and submits the changes to the Managed Services Provider.

OAKS Windows Server Access Review:

At least quarterly the OAKS Security Team requests a list of all the user accounts in the OAKS Windows servers from the Managed Services Provider and reviews the accounts to determine whether the user accounts belong to individuals who are still associated with OAKS. The OAKS Security team reviews the lists for accounts that were not properly processed for Off-Boarding and submits the changes to the Managed Services Provider.

OAKS UNIX Server Access Review:

At least quarterly, the OAKS Security Team requests a list of all the user accounts in the OAKS UNIX servers from the Managed Services Provider and reviews the accounts to determine whether the user accounts belong to individuals who are still associated with OAKS. The OAKS Security team reviews the lists for accounts that were not properly processed for Off-Boarding and submits the changes to the Managed Services Provider.

OAKS VPN Access Review:

At least quarterly, the OAKS Security Team requests a list of all the OAKS token user accounts from OIT/UNS and reviews the accounts to determine whether the user accounts belong to individuals who are still authorized for the OAKS VPN access. The OAKS Security team reviews the lists and submits any changes to OIT/UNS.

Incident / Security Violation / Access Log Reports

Application access information (i.e. user id, IP address of the user, last user ID update date/time, last login date and time, failed log in attempts) is maintained for the OAKS PeopleSoft system. The last user ID update date/time, last login date/time, and failed login attempts to the PeopleSoft application are available to be reviewed by the OAKS security team to help troubleshoot application user issues. IP Addresses can be reviewed as needed with the assistance of the PS Admin team.

Accenture follows guidelines set forth in the National Institute of Standards and Technology Special Publication 800-61 Revision 1 Computer Security Incident Handling Guide.

In addition, all employees receive training upon hire that inform the employees to contact the Accenture Security Operations Center (ASOC) in the realization of a Security incident or breach.

Overall OAKS Processing Environment

Access to OAKS was designed to allow a user to log into OAKS from the Internet. Agency, board, and commission users log into the PeopleSoft application through an OAKS website via an OAKS user ID and password. The servers that house the PeopleSoft ERP software are currently located at the CBTS and run on the UNIX operating system. The OAKS HR and financial transaction data entered by the state entities and processed by these PeopleSoft application programs (HCM, FIN, Billing, Budgeting, Inventory, etc.) are housed in a cluster of Oracle databases that also run on UNIX servers. The UNIX servers are administered and controlled by the Managed Service Vendor (Accenture). These servers sit on a network behind the firewalls administered and secured by Accenture at the North American Delivery Center offices in Cincinnati, Ohio. This OAKS LAN is one of many agency LANs that sit on the ohio.gov wide area network (WAN) protected by a firewall environment that is the first level of protection from the Internet. The WAN firewall is administered and secured by the ISD Network Security Group at the SOCC. Related security violations are reviewed by the ISD Unified Network Services (UNS) Group housed at the SOCC. The following sections of this narrative discuss the key components of this environment.

TCP/IP Access

Procedures are in place for requesting encrypted TCP/IP access to ISD secured devices. Access request forms must be completed by agencies and approved by ISD personnel. Each agency is required to designate a security administrator who will be responsible for ensuring that their employees and/or contractors are authorized and have access to the resources that they require to perform their job duties. Agency security administrators are responsible for adding, deleting or modifying employee and/or contractor access. System changes to access privileges are performed by the ISD security personnel upon request of the agency's designated security administrators. ISD security administrators track employee and/or contractor unauthorized access attempts of another agency's datasets.

Firewalls

OAKS is secured with a traditional depth-in-defense array of network security controls. At the external layer, OAKS’ DMZ is present. Inside the DMZ, network/firewall security is provided via Intrusion Detection Systems (IDS) and firewalls within each of the three distinct OAKS environments (NADC, SOCC & SOT).

OAKS’ boundary protection involves monitoring and control of communications at the external boundary of the information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels etc.).

OAKS uses a firewall to aid in the protection of the entity's assets, including the OAKS production environment. Network Security Administration, including both IDS and Firewall monitoring & administrative actions are performed at the by OAKS' Production Support Staff at the NADC. Unauthorized network traffic for the OAKS production environment is monitored by network personnel to identify key intrusion events in a timely manner.

All information transmitted online utilizes HTTPS connection. Secure Shell VPN connectivity is also made securely available to team members.

Any modifications to existing firewall rules must follow the standard change review & approval process prior to being executed by NADC resources.

Firewall rules are by default set to restrict the maximum amount of unwanted traffic while not impacting legitimate system use. Traffic is restricted based on IP address, destination address, and/or port address.

Designated accepted connections along with all dropped and rejected connection attempts are logged on the firewall log and regular/ongoing monitoring reviews are performed. NADC logs designated accepted connections along with all dropped and rejected connection attempts.

Logical access to the firewall rules is restricted to appropriate personnel. Administration of firewalls and modifications to the firewall rules for the firewalls protecting the OAKS production environment are documented by Accenture. Modifications to the firewall rules for the firewalls protecting the network are fully described, documented, reviewed and approved by the OAKS Change Advisory Board (CAB), as described in the Change Management Narrative.

All administrative activity related to Network security is tracked via ticket so that artifacts are available as summary reports from the OAKS ticketing system or individual work tickets, including approvals where applicable.

OAKS Intrusion Detection System (IDS) Capability

Security Monitoring and Detection is performed through a combination of both automated security tools and human checks. Security tools used for monitoring security include intrusion detection systems (IDS) and log scanners. There are defined procedures on how to respond to those events that have been identified as potential threats.

OAKS runs CISCO IDS modules to track all traffic in the three distinct environments:

- Production (NADC).
- DR (SOCC).
- Development (SOT).

All IDS Monitoring and administration is performed by NADC network specialists. OAKS understands the importance of proper tuning for the IDS (so that the ratio of false positives and false negatives is appropriate). The IDS system auto-generates alert tickets and also pages-out Network Security Response Team Members as needed. The ticketing system with which the OAKS IDS is linked is the same ticketing system used to track all OAKS-related work. Therefore, records and artifacts of all such activity are retained.

Once the auto-generated tickets/pages are generated, OAKS' standard Incident Management processes are followed to handle the incident to resolution. IDS rules can be updated (via the normal change process) to account for Security Alerts (e.g. US-CERT warning to block or monitor particular IPs or ranges of IPs, which are known to be malicious).

In addition to the real-time notifications, IDS Logs are reviewed (for any other suspicious activity) at a minimum of every eight hours, and typically more frequently.

Windows Network Security

The OAKS's Windows network security regime provides a secure processing backbone environment for OAKS via multi-layer firewalls, a DMZ, and intrusion detection software. Network segments are restricted by using virtual LANS (VLANs). Windows operating system logins are restricted to administrators and application services. Remote logins to the Windows network are restricted to secured VPN.

Access to the OAKS network is restricted to authorized state employees and contractors working at OAKS. Windows access control security software is installed on the OAKS LAN to help ensure a secure environment for all OAKS transactions. OAKS uses the Windows login ID and password as the first layer of security to the production and development servers. Access to the OAKS network is restricted to authorized state employees and contractors working at OAKS. Users can be part of the Domain Users group or the Domain Admin group. Requests for Windows access are submitted on a request form that is then e-mailed to the OAKS Technical Security team (OTS). This form specifies which Windows servers are being requested and what level of access is required, as well as the appropriate Windows administrator group the user should be added to via the Windows group policy.

System sign-on parameters have been established for the OAKS Windows Network. The Windows Group Policy is used to adjust default security permissions that are assigned to new accounts. The default Windows passwords are applied to all users at the domain level, and include:

- Minimum password length of 7 characters.
- Password complexity requirements (must contain at least one digit, one alpha character, and one special character).
- Password must be unique for a period of time (differ from the previous 5 passwords).
- Passwords have a maximum and minimum age (valid for no more than 75 days, and no less than 1 day).
- Account lockout is in effect after five invalid logon attempts.
- Locked out accounts reset after 30 minutes, and the lockout counter also resets after 30 minutes.

The OAKS Windows servers are accessed and managed using Active Directory, which is used to create and control the Windows accounts. Active Directory is a key network service that provides information on the Windows objects, organizes the objects, controls logical access, and sets security. All the OAKS Windows administrators have administrator access privileges on the Windows severs.

UNIX Operating System Security

Access to the OAKS UNIX production servers is restricted through UNIX security. Access to these OAKS UNIX servers is controlled by logical access controls via an access account that requires a user ID and password login. File and directory permissions are used to control access to specific files and folders from within a server, once connected.

In addition to file and directory access, adding users to uniquely-functioning UNIX groups enables only authorized users to have access to particular files and directories for those particular groups. Access procedures are managed by the Managed Services Vendor and must be approved by OAKS Security Service Assurance.

Users requesting access to an OAKS production server must complete an OAKS UserID Request Form.

System password controls have been established for the UNIX system on the production servers that process the OAKS programs and data. All UNIX user accounts require passwords. The following password parameters have been implemented:

- User accounts are locked after five authentication failures.
- The last successful and unsuccessful login attempts are displayed at login.
- Minimum password length of 7 characters.
- Password must be unique for a period of time (differ from the previous 5 passwords).
- The ALLOW_NULL_PASSWORD parameter is set to zero (prevents logging in without a password).
- The minimum number of upper-case characters required in a password is one.
- The minimum number of lower-case characters required in a password is one.
- The minimum number of digits required in a password is one.
- The minimum number of special characters required in a password is one.
- Passwords have a maximum age of 91 days.
- Passwords have a minimum age of 7 days.
- Users are warned seven days before their password expires.

Root account (superuser) access is required to manage the OAKS UNIX servers and is limited to OAKS NADC resources who require this access to perform their job functions.

To prevent unauthorized computer access, security controls at the operating system level must also be used to restrict access to computer resources. The following controls must be in place:

- Access control should be in place to appropriately restrict access to non-public computers. Only authorized users have access to the computer. The user must be identified, verified and authorized at the time of access.
- Server system commands and utilities must be protected, and access must be granted to authorized users only. The following operating system objects must be protected from unauthorized access:
    - Registry entries or system settings.
    - System files.
    - Application data or files.
    - Password files.
    - System log files or audit files.

OAKS PeopleSoft Application Security

The OAKS application incorporates PeopleTools application security software that uses roles, permission lists, field level security, page permissions, and row-level security to prevent unauthorized access to transactions. PeopleSoft components define user profiles (user IDs), permission lists, roles, field level security, page permissions, row level security, and security trees.

A User Profile is a set of data describing a particular user of the PeopleSoft system. This data includes everything from the low-level data that

PeopleTools requires, such as Language Code, to application-specific data such as the SetID a user is authorized to access. OAKS creates operator ids (user ids), which are required for a profile. There are currently two types of User Profiles within the HCM system, which include:

- State Employees
  - A new employee with the State of Ohio will receive a system generated User id which is also considered their EMPLID. This will be completed by the designated Agency when their payroll information is created.
- State Contractors
  - If a user is not currently an employee of the State of Ohio but is contracted to work within the states HCM environment they will be created as a Person of Interest (POI) in HCM and EMPLID will be created.

The user id field length is only 30 alphanumeric characters long. If by chance a user's user id exceeds the limit it will be truncated to fit the required field length. An OAKS_HCM user will use the HCM user profile in combination with a password to login or access the HCM application. Passwords for each module must be changed separately (i.e. they are not synchronized).

A role is assigned to a User Profile, and should represent a job functionally. A role can contain any number of Permission Lists. Some employees will fill several roles. These employees will be granted both roles and will inherit both sets of Permission Lists. By inserting this level of granularity into the security structure, the maintenance should decrease since the assignment can happen dynamically.

A role and its description(s) for each module came from a combined effort between the OAKS functional team, DAS HRD, and select agency liaisons.

A Permission List is the core of PeopleSoft online access. Permission lists work together to provide a range of access for an employee. The Permission List schema is very modular so it can be scalable. It is possible to have a single permission list for every role, but setting up two similar roles would be easier if the Permission Lists were more modular in nature. This means that Permission Lists should contain a functional/logical set of access rights. Some of these modules might be Personal Data access, sign-on times, or Job Data access. These groups can be further broken down into the type of access that a user might have. For example, the Job Data group could have an inquiry only group, a data entry group, and a correction mode group. The State of Ohio client determined how permission lists are organized. Some permission lists are assigned directly to a user profile while others are assigned to roles, which are in turn assigned to a user profile. In most cases, a profile will contain both types of permission lists with the majority of them inherited through the roles assigned to it.

Field Level security secures certain fields on a page. Field level security is created by using PeopleCode and is applied to a certain field for fields on a page within the PeopleSoft Application. All field level security code is attached to a specific ROLE or PERMISSION LIST and any user with a ROLE or PERMISSION LIST has access to update that particular field. The field level construct is as follows: OHFL_POSITION_STATUS = (OH = Ohio, FL = Field Level role, "Position Status" = a description of the main purpose of this role). In other words, any user that has a ROLE that contains the PERMISSION LIST called OHFL_POSITION_STATUS would be able to update the position status on the position page.

The general options of a Permission List include several settings. The ability to start an Application Server, permission to e-mail passwords, and time out minutes are each defined at this level.

Page Permissions define what menu bars, components, pages, and actions a user has. Types of actions include Add, Update and Display. Access to PeopleSoft applications and pages is granted through the page permissions. Page permissions should give the users the access they need to complete their job functions, but no more. Therefore, it is extremely important to organize the page permissions within permission lists so that they are easily assigned and revoked with minimal manual intervention. This was a joint effort between the agencies, change management, and the security team.

Some users need access to run batch and online processes, and organizing these processes by department or task will help to more efficiently assign them to users. Process Groups organize the different online and batch processes into logical families. These groups are assigned to Permission Lists to give individuals access to run appropriate processes. For example, by grouping the HR processes the Security Administrator can require that only certain individuals have the ability to run HR reports by giving only them access to the group. Running reports and updating the security tree are examples of processes to which OAKS individuals may need access.

Permission lists also control sign-on times for users. Any number of ranges can be assigned to permission lists to cover any applicable work shifts. OAKS agency users have 24-hour log-in access.

The ability to run certain processes is limited by access to various pages and process groups. In addition, this will control many aspects of how the Process Monitor tool will act. For example, the ability for others to see output from a process or update a process status is controlled with this type of security.

PeopleSoft determines which data permissions and default values to grant a user by looking at the users' Primary Permission List and Row Security Permission List. In the HCM module, the primary permission lists will control the default values for Business Unit, SetID, Company, Country, Regulatory Region, and Currency. The primary permission list also determines which queries a user has access to and how they run them. This permission list can also determine what objects can be accessed using the Application Designer tool.

Row-Level security refers to what data each user can see through the pages and components they have been granted access to. While a manager needs access to the information for each subordinate employee, HR Representatives in one department may not need access to the information for employees in another department. Row-level security enables an HR Administrator to only see the data for the employees they are working with. HCM row-level security is based on the department security tree and assigns permissions based on what nodes of the tree a user has been granted access to. The department security tree enables the SA to grant (or deny) access to an employee's data by granting access to the entity to which they report. Access to data is based on the hierarchy that one creates. If one grants access to a department, one also grants access to each department that reports to that department.

The security tree describes a hierarchy of departments according to organizational structure. Trees are built with levels and nodes, where levels represent the levels of the hierarchy and nodes, representing departments, are added at different levels to indicate their place in the hierarchy. For example, the first level of the tree might be the company level. The second level might be the regional level. A node that is added at the first level is a company-level node and represents the company department. A node that is added at the second level is a regional-level node and represents a regional department, such as an office. The first node in the organization is the root node. This is the highest node in the hierarchy. Other nodes (departments) report up to the root node. The data permission list is used to define user access at this level. The permission list will include the departments to which the user has access to and if needed it will also specify any child departments that the user will not have access to.

The naming construct for row-level security can vary based on the accesses required for an individual. However all row-level security permission lists begin with OHRL_.

Below are examples of these naming conventions used within OAKS HCM:

- OHRL_DNR100000_NO_TL.
- OHRL_10099223_NO_TL.
- OHRL_DAS01.

Access to update OAKS access security rights is restricted to only those individuals whose job responsibilities require it.

Requests to change security objects other than user profiles are sometimes required. For example, a change may be needed to a role or permission list. Changes to security objects, such as roles and permission lists, may impact multiple users in the production environment and, therefore, this access is restricted to the OAKS Security Team.

The OAKS Security Team members are assigned the following roles:

- OH_SECURITY_ADMINISTRATOR.
- Security Administrator.
- Portal Administrator.

The combination of these roles will provide full access to the security functions within the FIN and HCM OAKS PeopleSoft Applications.

OAKS Helpdesk users will be allowed minimal security access to the HCM PeopleSoft Application. These users will be able to Lock/Unlock and reset passwords on user accounts. These users will not have the ability to Create/Change/Update Roles, Permission Lists, or User Profiles. All of the Helpdesk Users will have the following role assigned to them: OH_OAKS_HELPDESK.

PeopleSoft User Preferences

PeopleSoft Security can sometimes require that the appropriate User Preference settings be put in place to grant the user certain access in the PeopleSoft environments. User Preferences are most prevalent in the FIN application. The preferences do not grant access to pages in the application, but rather control exactly what a user can do on pages that are accessible to them throughout the application. For the most part User Preference settings are automatically assigned by various security automation process that have been put into place. In rare cases these may be manually assigned as well.

PeopleSoft Application Password Criteria and Inactivity

Application sign-on parameters have been established for the OAKS FIN and HCM modules. The following are the default minimum password requirements for the OAKS application:

- Minimum password length.
- Password complexity requirements.
- Password must be unique for a period of time and must differ from previous passwords.
- Passwords have a maximum age.
- Account lockout is in effect after invalid logon attempts.

Users initially log into the system using a password that is randomly generated by the system at the time when the user ID is created. Upon logging in, users are required to change their password. The new password must still adhere to the PeopleSoft password guidelines.

The OAKS system automatically logs users off the system after a period (18 minutes) of terminal inactivity. A window appears warning the user that their session is about to be timed out as a security precaution.

Both the OAKS HCM and FIN applications can be accessed from any computer with internet access.

OAKS Databases

Access to the OAKS databases that house production data is restricted to authorized users. Requests for back-END OR DIRECT access is submitted on a request form specifying what access is being requested and what level of access is required. Approvals from the Service Assurance team are documented on these forms. These requests are reviewed by the Access Control Security Analyst for appropriate approvals and completeness of content. If there are questions or concerns, the SA Lead approving the access is contacted to assist with remediation of the concerns.

Once approved by the security team, the CRM ticket is assigned to the MSV team to implement. When completed, the ticket is updated to indicate that the requested access has been granted.

Physical Security

The OAKS PeopleSoft servers were housed in three environments during FY10:

1. Development servers are located in Columbus, OH at the State Office Tower (SOT). Before February 22, 2010 the SOT also hosted the State’s DR Environments.
2. Before February 22, 2010 The State of Ohio Computing Center (SOCC) hosted both the Production and Quality Assurance (QA) environments. On and after this date the SOCC hosted the QA environments, but also began to host the State’s new DR environment. The DR environment’s spare capacity is also leveraged to host testing servers for special projects.
3. Beginning on February 22, 2010 NADC (CBTS) began hosting the State of Ohio’s Production environments.

Security for the Cincinnati Data Center:

The production servers were housed at the Accenture North America Delivery Center for infrastructure outsourcing in Cincinnati, Ohio (CIN-NADC) beginning on February 22, 2010. The CIN-NADC data center is a secure facility providing essential services required to operate computer systems (e.g. conditioned and backup power, a temperature and humidity controlled environment, fire protection, redundant network connectivity, lockable cabinets and cage space, and building access security). The CIN-NADC also provides daily operations, monitoring, maintenance, upgrades, performance tuning, and data backup of hosted servers and applications.

The building had three main entrances; one entrance for data center personnel, one entrance for visitors, and a loading dock for equipment and supply delivery. Data center personnel entered and exited the building through an entrance that is secured by a swipe card reader. Visitors entered into a vestibule area and had to contact the security guard station via a direct telephone line to the security guard station to gain access to the lobby of the facility to be granted their visitor badges and to meet their data center escort. There is a set of doors between the visitor vestibule area and the lobby that had to be electronically unlocked by the security guard so visitors could gain access to the facility. All visitors and data center clients were required to be escorted to and from the requested work location within the facility by a data center employee. Anti-pass back swipe card readers protected the loading dock and cargo elevators and all cargo/supply deliveries were required to be escorted by a data center employee.

Visitor access to the NADC data center is monitored and restricted. The data center security personnel must be notified of all planned visits by non-data center individuals by authorized data center or data center client personnel prior to the time the visitor arrives at the facility. Once the visitors identify themselves and the security guard verifies the visitors are on the visitor list for the given day, they unlock the door electronically so the visitors can enter the building (Note: The security guard at the security desk in the lobby can see the visitors in the vestibule area). The security guard requires all visitors and clients to provide a state issued photo ID before proceeding any further into the facility. The security guard compares the photo ID to the visitor list and if the names agree, the visitors will be granted a visitor badge. The visitor badge does not have swipe card access and cannot open any doors that were protected by a swipe card reader. Data center clients, such as authorized Accenture personnel, are authorized to be granted a swipe card (permanent visitor badge) that will open doors protected by a swipe card reader. If an authorized client requests a “permanent visitor badge” they must surrender their photo ID to the security guard until they return the permanent visitor badge. All visitors and clients were required to be escorted to and from the requested work location by a data center employee.

The computer room and data processing facilities and equipment at the data center are protected by environmental and physical access controls. Access cards or visitor cards are required for all employees and individuals to the building at all times. Environmental controls identified include:

- Raised floors.
- Water sensors under the floor.
- Fire Extinguishant-25 (FE-25).
- Smoke detectors in the ceiling and floors.
- Fire extinguishers.
- Emergency power-off switches.
- UPS system and backup generators.
- Video surveillance system.

A notification system monitors the temperature and humidity throughout the processing facilities.

Anti-pass back swipe card readers protect all entrances and exits to the data center floors. The data center floor the OAKS production hardware is housed on has three entry/exit points. The main entrance to the data center floor the OAKS production hardware is housed on is only accessible via the elevators. This door is protected by anti-pass back swipe card readers. There is also two emergency exit stairwells that are protected by anti-pass back swipe cards readers with direct access to the floor the OAKS production hardware is housed on at the facility. The cargo elevator can also stop on the floor the OAKS production hardware is housed on, but the cargo elevator leads to a storage/staging area on the floor. There is a door between the storage/staging area and the data center that is protected by anti-pass back swipe card readers.
Floor operators staff the data center 24 hours a day/seven days a week. Floor operators have access to all cameras on all data center floors in order to monitor the data center. OAKS hardware is physically mounted in hardware cages and all hardware cages are enclosed with fencing from the floor to approximately one foot from the ceiling. The fencing doors are protected by swipe card readers. Only Accenture authorized personnel with a permanent visitor badge and data center personnel have access to the OAKS hardware in the data center.

The generators, switchgear, and UPS systems are stored in separate rooms with a firewall between the data center and the generator and UPS rooms. The data center performs weekly inspections (and maintenance, if necessary) on the generators (i.e. run the generators), switchgear, and

UPS systems. CBTS performs weekly inspections on the A/C units and bi-monthly maintenance is performed on the A/C units as well. Additionally, the data center performs an annual lights out test.

Security of the SOCC:

Prior to February 22, 2010, the production and QA FIN, HCM, and CRM servers used by OAKS were located at the SOCC. To lessen the risk of unauthorized physical access to the key computer hardware located at the SOCC, background checks are required before access is granted to non-visitor personnel at the SOCC. Potential candidates for employment follow a standard hiring practice and are screened by the DAS/OIT Division of Human Resources. Prior to employment, potential new employees must undergo a background check by the Ohio State University (OSU) police utilizing WebCheck software, which accesses the Bureau of Criminal Identification and Investigation. In addition to the OSU background checks, Security, OSP/DPS, and DAS-MARCS potential new employees also undergo a full background investigation by the Ohio State Patrol (OSP).

The SOCC conducts quarterly confirmations of user agency personnel with access to the SOCC. On a quarterly basis, state agencies are asked to confirm authorization for access to the SOCC, which includes the computer room on the second floor. The SOCC site security coordinator sends building cardholder list reports to all state agency customers indicating cardholder names, card numbers, card status (active/inactive), expiration date, department, sign-in privileges, and job title. Each department will also receive a Cardholder Detail Report containing detail information for each employee with an access card. This Detail Report contains information on access level details that indicate to what rooms the individual has access. Each agency is required to review this packet of security information, make any necessary changes, approve the defined access, and return it to the SOCC site security coordinator. The SOCC site security coordinator then makes all applicable changes in access.

Access to the grounds of the SOCC is restricted. All employees, visitors, mail, and packages entering the building are screened. SOCC building access is restricted and monitored 24 hours a day, seven days a week. Visitor access to the SOCC is monitored and restricted. The “State of Ohio Computer Center Visitor Notification Form” is completed and approved in advance or at the time the visitor arrives at the SOCC by an authorized SOCC employee who has sign in privileges. The form includes relevant information guiding and documenting visitor access.

The computer room and data processing facilities and equipment at the SOCC are protected by environmental and physical access controls. Access cards are required for all employees to the building at all times. Use of the elevators is restricted. Environmental controls identified to safeguard the computer facilities include:

- Raised floors.
- Water sensors under the floor near A/C units.
- Pre-action sprinkler heads at the ceiling level.
- Smoke detectors in the ceiling and floors.
- Fire extinguishers.
- Emergency power-off switches.
- Fire hoses.
- UPS system and backup generators***.***

A maintenance alarm system monitors the temperature and humidity throughout the building. All of these environmental controls are monitored 24 hours a day, seven days a week by a security and maintenance alarm system.

The CPUs housed at the SOCC and emergency lighting are backed up by an uninterruptible power supply (UPS). This battery backup system can provide power for a maximum of 20 minutes. In the event battery backup is insufficient, six diesel generators provide generating capacity based on current loads. If needed, the generators activate within eight seconds after interim battery backup is provided. Monthly load tests are performed to help ensure the OIT/ISD's generators, switchgear, and UPS systems are available for providing constant power for data processing.

Access to the computer room at the SOCC is restricted to authorized personnel. In order to access the computer room, an individual must have a valid security card programmed for access to the room. Approximately 260 onsite and offsite personnel have physical access to the computer room. This includes DAS/OIT personnel and state agency customers with hardware housed at the SOCC.

IT Operations

System Performance

OAKS management meets weekly to discuss any production issues with the OAKS applications. A Customer Relationship Management (CRM) ticket and a corresponding IT Service Management (ITSM) ticket is created to help monitor the status of identified system issues. Representatives from the HCM development team, HCM functional team, and HRD attend the meetings. Representatives from the FIN development team, OBM, and GSD also attend the meetings. All issues marked with urgent priority are completed first. The remaining issues (marked high, medium, and low priority) are completed as time permits throughout the business day.

Detailed OAKS Root Cause Analysis (RCA) reports are created to document, maintain, and track any OAKS Severity 1 system issue, including any application outage, security issue, or major batch scheduling problem that may cause a major business impact of downtime. The reports document a description of the issue, the overall impact, the timeline of events, a root cause analysis, how and when the incident was noticed, the exposure of recurrence, and the production changes required due to the incident.

OAKS system availability/downtime is monitored and documented on the OAKS Service Level Availability spreadsheets. The service level availability spreadsheet is manually generated by the DBAs after reviewing the scheduled and unscheduled outages for production and non-production application each month.

Technical Operations meetings are held weekly. These meetings have four main objectives. First, all major issues over the last week are reviewed and discussed to ensure that proper root-cause analysis has been completed and that the support organization can continually improve. Second, the status (complete, deferred, in progress, etc.) of all planned maintenance during the past seven days is discussed. Third, all planned maintenance activities are discussed. The key highlights of cases opened with product vendors supporting OAKS are also discussed.

The general system maintenance (i.e. dealing with incidents, production issues, etc.) for OAKS is conducted on Sundays. However, maintenance activities are occasionally performed on weeknights if not completing the activity could have a negative impact on the OAKS business operations.

PeopleSoft SYSAUDIT reports are generated on a quarterly basis to identify system integrity issues for the OAKS FIN and HCM modules and are available for review by the OAKS infrastructure team. The SYSAUDIT report is a PeopleSoft-generated audit report that provides details on the system integrity of the PeopleTools components. The report identifies any discrepancies in the system integrity and provides the recommended corrective action. The OAKS Application teams analyze their respective sections of the report and take corrective action as needed. The report is re-run to help ensure the errors were resolved.

Databases

OAKS uses Oracle databases to store its financial data. Database administrators use a number of tools to manage and help ensure optimum performance of the OAKS databases. Management of the databases is accomplished using the following tools:

- Oracle Enterprise Manager (OEM) – OEM is a set of system management tools provided by Oracle for managing the Oracle databases. OEM provides tools to monitor Oracle environments and tasks. All the OAKS database administrators (DBAs) have privilege to access the databases using OEM.
- SQLPlus – SQLPlus is a command line SQL and PL/SQL language interface and reporting tool used by OAKS DBAs to interact with the Oracle databases.
- ISQLPlus – ISQLPlus enables OAKS developers and users to use a web browser to control and query the Oracle database and perform the same tasks that can be done through the command line version of SQLPlus.
- VMSTAT - Reports information about virtual memory statistics regarding kernel thread, virtual memory, disk, trap, and CPU activity.
- Glance Plus or Top – Used to check the health of nodes including checking for CPU and memory spikes.
- UNIX CRSSTAT - This command shows the status of each registered resource in the cluster.

The Infrastructure Team has been in the process of developing a centralized directory for all their routine database scripts. The centralized directory of scripts maintained by the OAKS Infrastructure Team includes database monitoring scripts, database statistical scripts, and application scripts. The centralization of the database scripts is an ongoing project that requires changes to the script language as well as code fixes to accommodate the centralized password functionality that is integrated into each database script. The Infrastructure Team also plans on maintaining database scripts in the centralized directory for exporting data, Oracle's Recovery Manager (RMAN), and generating logs for the databases.

The Morning Prod Environment Health Checklist is completed daily to document the operational status of the OAKS databases and to verify the OAKS databases are operating as designed. The checklist is completed by the morning shift DBA each morning Monday through Friday and, once completed, sent via e-mail to the OAKS production DBA group and the infrastructure team leads. The checklists are stored on the intranet for reference.

Database incident reports are created to document, maintain, and track identified OAKS database issues. The reports document a description of the issue, the overall impact, the timeline of events, a root cause analysis, how and when the incident was noticed, the exposure of recurrence, and the production changes required due to the incident.

Database space check reports are automatically generated for the OAKS DBAs to review potential OAKS database issues. Corrective actions are then taken if needed. The reports provide a file system status of the environment, information on the automatic storage management (ASM) diskgroup space, information on tablespace utilization, notification to the DBAs of any segments nearing the Maxextents, verification of the flashback configuration, and information on the flashback space.

Database alert messages are automatically generated to notify the OAKS DBAs of OAKS database performance thresholds that are about to be and/or have been exceeded. A DBA will investigate the alert messages and take corrective action as needed.

Database security audits (ACLs) are performed at the beginning of every month. The ACLs are generated by SQLs that are run by the OAKS DBAs and submitted to the State's security team. The database access ACL contains the status of every account in the database and the roles granted to the accounts. The system privilege ACL contains all of the system privileges granted to users and roles.

Accenture has developed formal policies and procedures relating to security and general administration of the Oracle databases, which includes managing database statistics, backups, tuning, replication, adjusting table space, and installation of patches and minor upgrades.

PeopleSoft Administration

The OAKS PS administrator completes the Daily Morning Prod Environment PS Admin Health Checklist daily to document the status of the OAKS applications and critical components to verify the OAKS applications and components are operating as designed. The checklist is completed each morning Monday through Friday by the assigned PS Admin and sent via e-mail to the OAKS PS Admins, the infrastructure team and the management team. The checklists are stored on the SharePoint intranet site for future reference. The Daily Morning Prod Environment PS Admin Health Checklist procedures are completed to confirm the following:

- Application modules and process schedulers (HCPRD, FNPRD, EPPRD, CRPRD, ELPRD) are operating as expected.
- Cognos, Ascential Datastage, Tumbleweed, Mercury ITG, and UC4 are operating as expected.
- PeopleSoft Application Messaging infrastructure is operating as expected.
- Applications overall performance is operating as expected.

Application Server logs are available each day to the administrators, if needed, to help them investigate and resolve these errors. The Tuxedo logs, which document communication errors between web and application servers and the application servers and database servers, are available each day to administrators, if needed, to help investigate and resolve these errors. The Process Scheduler logs are available each day if needed to help investigate and resolve scheduling errors.

The PeopleSoft components of the technical architecture consist generally of two BEA products (Vendor: Oracle). BEA Web Logic serves as the web server tier for all OAKS applications. BEA WebLogic is a Java 2 Enterprise Edition application server. BEA Tuxedo serves as the application server tier. BEA Tuxedo provides the framework, or middleware, for building scalable multi-tier client/server applications in heterogeneous (dissimilar), distributed environments that extend from the Web to the Enterprise. The PeopleSoft Administration team maintains these components of the technical architecture.

Batch Processing

The OAKS Batch Operation Team is responsible for the data processing operations and related functions for FIN and HCM. EPM batch is monitored by OIT. OAKS batch processes are documented, scheduled, and maintained with automated batch processing software and are manually documented using various forms and worksheets.

The UC4 Job Inventory contains the list of automated jobs that operate the OAKS application. This helps to ensure batch processes are scheduled properly. The Production Resolution Matrices outline the batch job error/failure procedures and include information regarding the affected function(s), the affected area of OAKS, the affected job name(s), if it was a critical job, the issue title, issue description, the issue resolution steps, and if an on-call individual should be contacted. The automated batch jobs are manually documented via the Production Batch Schedule Worksheet by the OAKS Production Schedulers. The production batch schedule worksheet supports batch processes that must be run at specific times (e.g. daily, weekly, monthly, yearly), and contains information on the jobs, the related OAKS module, the PeopleSoft program name, the type of program, the run control IDs, the run control parameters, the execution sequence, and any related comments. OAKS Batch schedulers complete the Production Batch Worksheet on a daily basis. The forms are retained for a period of 12 months. When batches are completed, the status is communicated to the OAKS Operations Team. Any errors are corrected and the batch is resubmitted.

The batch account is the PeopleSoft account that has the ability to process run controls. This ID is used by the UC4 Job Inventory software. UC4 schedules all the automated batch jobs that operate the OAKS application. Access to the OAKS batch ID (used to administer batch processing) is restricted to authorized state employees and contractors working on the OAKS project. Thirteen state employees and one contractor know the password and share the batch account to administer the PeopleSoft run controls.

Backups

The backups of the OAKS production environment occur at the NADC. Backups of the OAKS quality assurance (QA) environment and development (DEV) environment take place at the SOCC in Columbus, Ohio and the State Office Tower in Columbus, Ohio respectively.

PrimaryBackups

Data replication and synchronization involves the process of keeping data integrity “current” in both the production (NADC) and DR (SOCC) environments. In the OAKS environment, HP Continuous Access (CA) and Oracle Data Guard facilitate the Windows servers HP Enterprise Virtual Array (EVA) (storage device) synchronization and Oracle database replication.

HP Continuous Access provides asynchronous replication between the NADC HP EVA and SOCC DR HP EVA for all Window servers. This synchronization process occurs almost instantaneously. Information is written to the NADC HP EVA and then that information is sent across the Time Warner WAN from NADC to SOCC and then written to the SOCC DR HP EVA.

Oracle Data Guard provides automated database replication between NADC production databases and SOCC DR databases. NADC Oracle database archive logs are created when data is written to a NADC Oracle database. As soon as the NADC Oracle database archive logs are created, they are sent across the Time Warner WAN from NADC to SOCC and then written to the SOCC DR HP EVA. The database archive logs are then applied to the SOCC DR databases to complete the synchronization between the NADC databases and the SOCC DR databases.

For NADC data stored on the HP-UX file systems (does not include data stored on Windows file systems and databases), the data is restored at the SOCC DR HPUX file system by tape. The HP-UX file system data does not contain critical application data but system and application log files which would be used only for auditing purposes.

<u>Database Backups</u>

For all locations and environments, Oracle RMAN software is utilized to backup and restore the databases. Part of the Oracle RMAN backup process is to create a physical file of the database backup on the HP Enterprise Virtual Array (EVA) storage device which can then be treated like any normal file on a file system.

At NADC for Production and at the SOCC for QA, the RMAN incremental backups occur on a daily basis and full backups occur on a weekly basis. On bi-weekly payroll weekends multiple full database backups occur in production. At the SOT for DEV, full RMAN database backups are taken every weekend.

At NADC for Prod, the RMAN database backup files are created on the EVA storage device. These RMAN backup files are then written to a separate storage device, Virtual Library System (VLS), by HP Data Protector. On a daily basis the database backup files are moved to the VLS. HP Data Protector will then move then database backup files from VLS to 256 bit encrypted tape (HP LTO4).

At SOCC for QA, the RMAN database backup files are created on the EVA storage device. Then HP Data Protector utilizing HP Serviceguard will write the RMAN database backup files directly to 256 bit encrypted tape (HP LTO4).

At SOT for development, the RMAN database backup files are created on the EVA storage device. For the SOT, OAKS utilizes OIT's primary backup system, TSM (IBM Tivoli Storage Management). TSM performs nightly incremental backups. TSM uses a progressive incremental forever-backup scheme, so there are no scheduled full backups. TSM replicates data between the SOT and the SOCC so no off site tapes are required. TSM is administered and supported by OIT. TSM server is administered and supported by OIT. TSM client is administered and supported by Accenture.

Secondary Backups

<u>File Systems</u>

For the NADC, the backup architecture for the file systems begins with HP Data Protector copying data from each mount point (UNIX) or each directory (Windows) directly to 256 bit encrypted tape (HP LTO4). For the SOCC, the backup architecture for the file systems begins with HP Data Protector copying data from each mount point (UNIX) or each directory (Windows) directly to 256 bit encrypted tape (HP LTO4). At NADC and SOCC, the incremental backups to tape occur on a daily basis, and the full backups occur on a weekly basis.

At the SOT, OAKS utilizes OIT's TSM. SOT file system backups begin with backing up data from each mount point (UNIX) or each directory (Windows). TSM uses a progressive incremental forever-backup scheme, so there are no scheduled full backups. The incremental backups occur on a daily basis.

<u>Tapes</u>

The NADC Production tapes of the files systems (including the RMAN database backups) are sent offsite to a Cintas document storage facility on a weekly basis for 12 week storage retention. The SOCC QA tapes are sent offsite to the Fireproof Records Center on a weekly basis for 12 week storage retention. For the SOT, TSM replicates data between the SOT and the SOCC so no off site tapes are required.

Monitoring

At NADC, monitoring of the backups exists for both the RMAN database and HP Data Protector file system tasks. If RMAN database backup is not successful, the batch monitoring team who monitor production batch will make a call out to the database team upon failure. Reporting exists within Data Protector to monitor the file system backups to the VLS and tape. Automated emails to the backup team occur to notify them of the completion of backups. If high or critical errors occur, text messages are auto generated and sent to the backup team.

For QA, RMAN database backup failures generate Oracle Enterprise Management alerts which are monitored by the Database Administrators on a daily basis. HP Data Protector will generate an alert if a file system backup fails. The Storage Administrators review HP Data Protector alerts on a daily basis.

For SOT, RMAN database backup failures generate Oracle Enterprise Management alerts which are monitored by the Database Administrators on a daily basis. TSM generates an alert if a file system backup fails. The TSM Administrators review alerts on a daily basis.

FINANCIAL APPLICATION CONTROLS FOR OAKS_FIN

OVERVIEW of OAKS_FIN

The Ohio Administrative Knowledge System (OAKS) is a statewide enterprise resource planning application that provides financial (FIN) functionality for all state agencies, boards, and commissions. OAKS FIN replaced the Central Accounting System (CAS) in July 2007.

The OAKS FIN modules implemented in July 2007 included Purchasing, General Ledger, Accounts Receivable, Accounts Payable, eProcurement, EPM (data warehouse copy of production data that is updated daily) for FIN modules, Expense, and the Central Accounting System (CAS) Data Warehouse. The Financials (FIN) Billing module was released in January 2008. Additional FIN modules released in July 2008, included Asset Management and Budget and Planning.

OAKS Financials contains seven modules:

1. **General Ledger**: Information processed in other modules is posted to the OAKS General Ledger (GL). Journal entries are also made to the General Ledger journals.

2. **Purchasing**: The Purchasing (PO) module is used for purchasing goods or services.

3. **Accounts Payable**: Accounts Payable (AP) module is used to enter vouchers (transactions that are used to initiate payment).

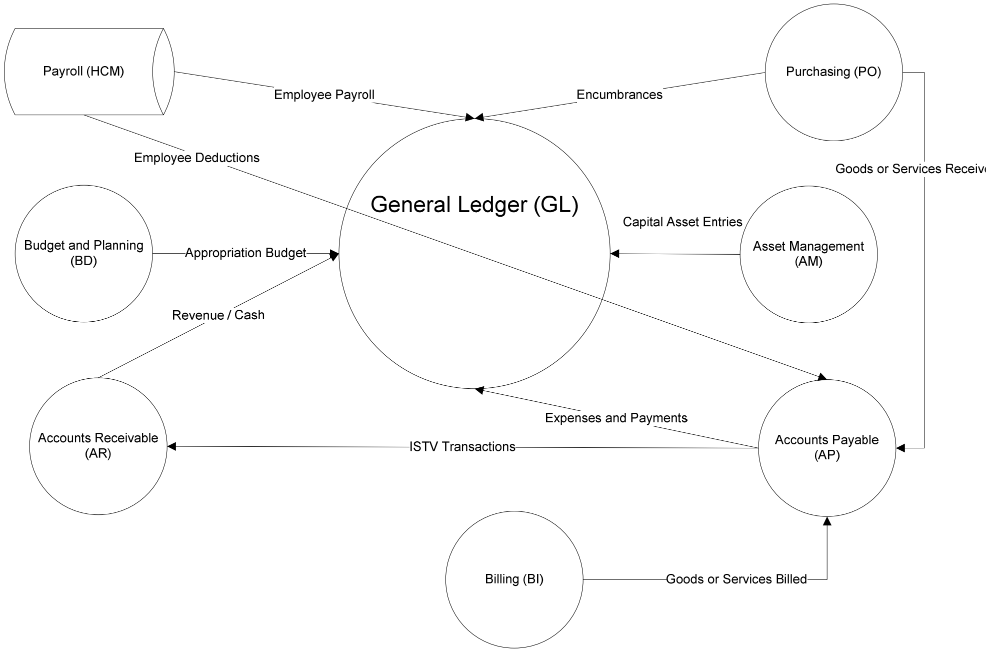
4. **Accounts Receivable:** The Accounts Receivable (AR) module is used to create pending items and record miscellaneous revenue and payments received from customers.

5. **Billing**: The Billing (BI) module allows for creation of bills and printing of invoices. The OAKS Billing module automatically sends invoices to AR as pending items. OAKS posts revenue created from AR directly to the GL.

6. **Asset Management:** The Asset Management (AM) module is used to track and maintain control of agency asset additions, retirements, and depreciation.

7. **Budget and Planning:** The Budget and Planning (BD) module is used by agency budget staff to create the biennial budget request. This module is used by the Office of Budget and Management (OBM) to analyze agency requests and produce the biennial executive budget recommendation.

OAKS Financials – Module Overview



These seven modules were all operating in the production environment. The following narrative will describe each of the above listed modules and then describe the reporting, monitoring and security common to all modules.

OAKS General Ledger/Chart of Accounts

The General Ledger, also known as the Actuals Ledger, is a section of OAKS FIN containing the state's official accounting record. It contains information similar to the detailed journals and transactional listings agencies have used in the past. The General Ledger is a central location where accounting transactions are recorded. OAKS automatically posts accounting information that has processed in other modules. Although all modules post accounting entries in the General Ledger, three modules in OAKS affect the revenue and expenditure balances in the General Ledger.

- Purchasing - Purchases goods and services, setting aside appropriation.
- Accounts Receivable - Creates journal entries when pending items are created or revenue is processed.
- Accounts Payable - Creates journal entries after vouchers and payments are posted.

The budgets, budget checking rules, ledgers, and chart of accounts are all set up in the General Ledger module. OAKS will create journal entries in the General Ledger from the revenue and expenditure transactions that occur in the purchasing, accounts receivable, and accounts payable modules.

All financial transactions in OAKS require agencies to enter accounting information. The accounting information that agencies enter comes from the Chart of Accounts (the list of financial accounts used by the State).

Chartfields

The OAKS General Ledger defines the financial structure of each organization by combining separate and distinct fields called chartfields. OAKS uses chartfields to classify the state's Chart of Accounts for financial reporting. Chartfields combined together to identify a transaction is called a chartfield distribution. Only authorized users can create or modify the chart of accounts (chartfields) in OAKS, which includes fund, program, ALI, department, and receipt number of the account codes.

OAKS uses the following chartfields:

- Fund*.
- Service Location.
- Appropriation Line Item (ALI)*.
- Reporting.
- Account*.
- Agency Use.
- Department*.
- Budget Reference.
- Program*.
- Receipt Number.
- Operating Unit.
- Grant/Project.
- ISTV Xref.
- Project.

*Required chartfields for most OAKS transactions include Fund, ALI, Program, Department, and Account.

Changes to chartfields may be requested by the individual agencies. OBM creates and/or modifies chartfields (department, program, grant/project, project, service location, reporting, agency use, and budget reference) based on Chartfield Change Request forms that are submitted by the agencies.

Change requests for chartfield updates are submitted to a specified e-mail address. When the GL team or OBM has completed the change or addition, they will notify the agency.

All change requests must be approved by an authorized agency representative. It is the responsibility of the individual agency to determine the appropriate level of approval. The agency CFOs submit a Chartfield Signature Authorization Form to OBM that identifies the employees who are authorized to sign the chartfield change request forms on behalf of the agency CFO. The GL team uses this list to verify that the chartfield change request came from an authorized agency representative.

The remaining chartfields (fund, account, ALI, and ISTV Xref) are owned and assigned by OBM. OBM will define and add the new chartfield; however, an agency can request that a new fund, account, or ALI be added based on a new purpose or legal authorization. The ISTV Xref chartfields are only changed when the state adds a new agency or changes an agency name. OBM State Accounting documents and approves all changes and modifications to the fund, account, ALI, and ISTV Xref chartfields.

Dates used in FIN

OAKS FIN has numerous dates within the system that have different meanings depending on the agency and type of transaction. The following are some of the more commonly used dates within FIN:

- **Accounting Date –** This date does not have a specific meaning that covers all transaction types. The date can vary from agency to agency because it can be manually entered. Typically, it is the date when a transaction was entered into the system.
- **Accounting Period –** Identifies a time period (1-12) to which transactions are posted to the General Ledger. The accounting period must be used in conjunction with the Fiscal Year in order to associate the transaction with the correct time period.
- **Journal Date –** The date the journal was created. This determines to which period the system posts the journals, unless it is an adjusting entry. This date is defaulted to the current day's date, but a journal can be back dated or future dated within an open period.
- **Budget Date –** This date determines the accounting period and fiscal year that the transaction will be reflected on the commitment control ledger.

Federal Stimulus Tracking in OAKS FIN

In order to track the American Recovery and Reinvestment Act (ARRA) federal stimulus funding that is received and spent in the state of Ohio, additional program chartfields were created within OAKS FIN. Federal stimulus program codes are requested by an OBM budget analyst, and created in the same manner as all other chartfields. A subset of program code values within the agencies' normal program code range was created for the ARRA funding. For example, agency ADA has ARRA program codes 2185 through 2199; agency ADJ has ARRA program codes 2291 through 2299.

There are four public queries in OAKS FIN that allow an agency to track their ARRA revenues and expenditures.

- The OBM_PROG_ATTRB_FED_STI_EXPENSE and OBM_PROG_ATTRB_FED_STI_REVENUE queries provide *detailed* ARRA expenditures and revenues, respectively.
- The DB_STIMEXP_PUB and the DB_STIMREV_PUB queries display ARRA *summarized* expenditures and revenues, respectively.

Journal Entries

Only authorized users can post journal entries directly to the general ledger.

Accounts Payable
OAKS creates accounting entries when vouchers and warrants are processed. When vouchers are created, the accounting entries debit expenses and credit liabilities. When warrants are processed, the accounting entries debit liabilities and credit cash.

OAKS runs a process to summarize Accounts Payable accounting entries into General Ledger journals.

Accounts Receivable
When an AR pending item is created in AR, the OAKS AR module automatically creates a journal entry that credits revenue and debits Accounts Receivable. Either a pending item is created or a payment reversal is processed.

When a revenue processor applies a payment for a pending item, the OAKS AR module automatically creates accounting entries that credit Accounts Receivable and debit cash.
Direct Journals create a journal entry that credits revenue and debits cash without creating a subsequent transaction within the processing module.

Purchasing
The OAKS Purchasing module does not create journal entries in the Actuals Ledger; it does, however, update the commitment control ledger by sending accounting entries for Purchasing.

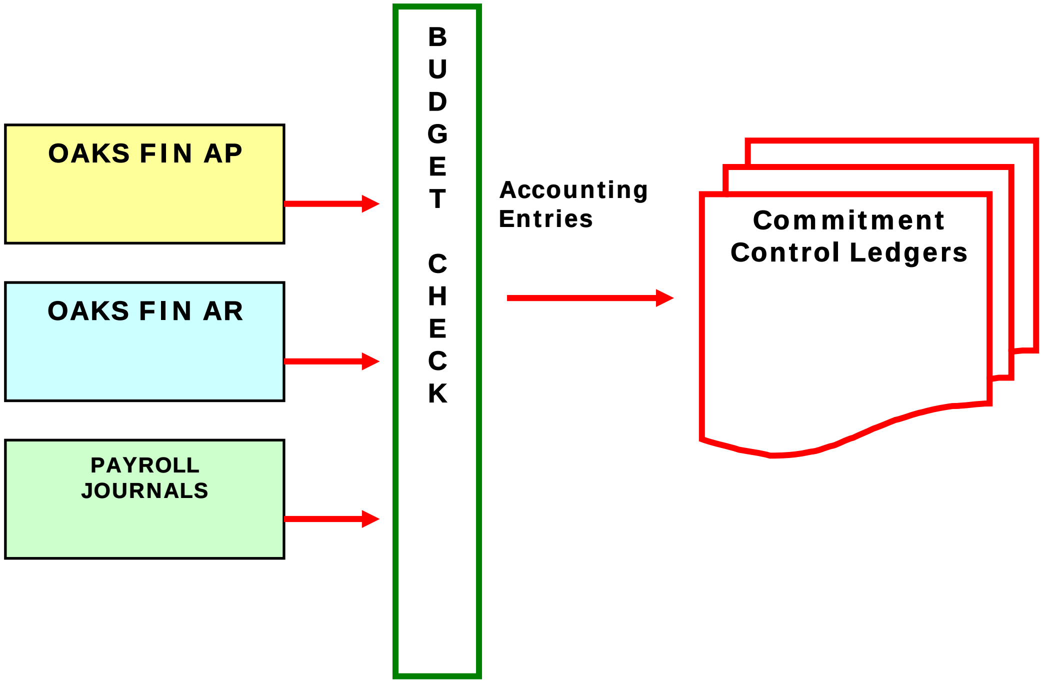
Asset Management
The Asset Management module does not create journal entries in the Actuals Ledger; it does, however, send asset management entries to the full accrual ledger for capital asset tracking.

There are no adjustments for the billing module. The billing module does not directly create GL entries; instead, entries are posted through Accounts Receivable.

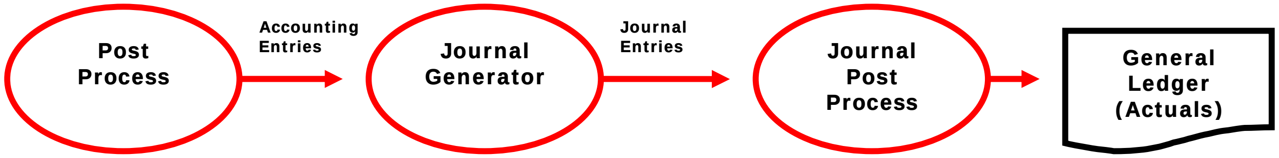
OAKS budget structure

OAKS uses commitment control ledger groups to track and control budgets. The highest levels of these ledger groups consist of cash, appropriation, and allotment. They represent central budgets that are controlled by OBM. At a minimum, there must be sufficient cash, appropriation, and allotment for transactions to process successfully in OAKS.

For example, someone in an agency creates a voucher to pay a vendor. OAKS checks the budget to ensure there is sufficient appropriation and cash to process the transaction. If sufficient budget is not available, the voucher fails the budget check process. Agencies must resolve the budget check error in order to issue payment for the voucher.



When agencies process encumbrances and expenditures in OAKS, they are budget checked against several budget ledger groups. These budget ledger groups are also referred to as commitment control ledger groups. OAKS controls agency transactions by stopping them from processing transactions when there is not enough resources in the budget.



The post process includes three types of transaction posting: Voucher Post, Payment Post, and AR Update.

There are four types of ledger groups that are available to agencies:

1. **Cash Control** – Is maintained centrally by OBM, ensures that cash is available prior to spending, and is increased when cash is received and decreased when it is spent. If sufficient cash does not exist, OAKS generates a budget check error for this ledger. Agencies must resolve this error to continue processing.
2. **Appropriation –** Is the legal spending limit authorized by the General Assembly, entered into OAKS by each agency using budget

journals and approved and posted by OBM, and is the highest level of expense budget in OAKS (the expense budget available to the widest range of accounts). If the appropriation has been exceeded or does not exist, OAKS generates a budget check error for this ledger. Agencies must resolve this error to continue processing.

3. **Allotment –** Is the breakdown of the appropriation line item (ALI) by expense accounts at the category level (for example, one category could be "Supplies & Maintenance"). It is entered into OAKS by each agency using budget journals and approved and posted by OBM. If the allotment does not exist or has been exceeded, OAKS generates a budget check error for this ledger. Agencies must resolve this error to continue processing.
4. **Agency-Level –** Is a tool used to manage an agency's budget. It is a more detailed breakdown of the allotment budget. This level is entered and maintained by the individual agencies.

The fund owner is the primary agency that monitors and spends from a particular fund.

Depending on agency choice of budget structure, transactions that exceed spending authority may cause an error to occur. When processing a transaction and the budget has been exceeded:

If the agency uses...	**Then the system will respond with...**
1. A control structure	1. Errors that prevent further processing
2. Tracking without budget structure	2. Warning messages that do not prevent further processing
3. Tracking with budget structure	3. A message that a budget must exist for the transaction

Payroll (HCM) Updates to the GL

Payroll transaction data comes directly from HCM to FIN (Financials) via a downloaded interface file. The interface file includes HCM journals that are budget checked in FIN, creating accounting entries to the Commitment Control Ledgers. The journals then post to the GL via the Journal Post Process.

HCM staff manually check the GL and AP files sent to FIN for accuracy and completeness. The process has been divided into three manual procedures to ensure the files sent to FIN match what is in HCM. The first check helps ensure that the GL file, which is created automatically via a batch process, matches the AP table in HCM. Staff performs several checks including the number of rows, sequence numbers, and totals. The procedures include steps to identify and correct errors. Once all the errors are corrected and the HCM staff is confident the file is correct and complete, the batch team is instructed to release the job that sends the file to FIN. At this point the second check is performed to verify the number of rows sent through the batch procedure matches the total record count from the file. The third check is performed to compare the voucher generation to AP. This check verifies all general deductions, benefit deductions, garnishments, and taxes were extracted and set to "S" for sent. Once this check has been performed, the batch team is instructed to continue processing the file in FIN.

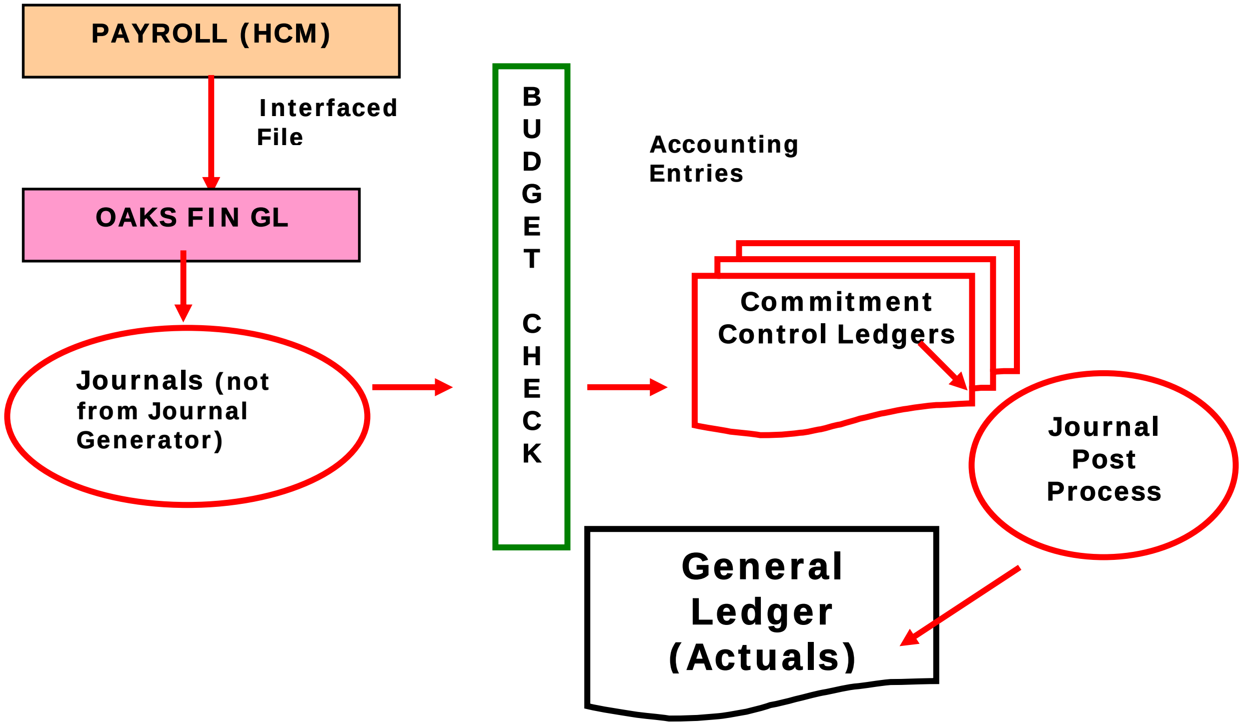
Once the HCM payroll files reach the FIN application, they are processed through a series of batch jobs automatically scheduled to run. The first batch that is performed in the FIN processing of the payroll files combines and totals detail rows of cash and liability chartfields by Fund, Account, and ISTV XREF and removes all other chartfields. Next, any objects that were coded according to the chartfields previously defined in CAS are converted to the new FIN Account chartfields. Then, if corrected journal entries are received from individual agencies, the original journal entry GL status is set to "I" so that it is ignored and not processed along with the new corrected journal entries. After these processes run, journal generator runs and creates one payroll journal entry per agency.

The payroll files are then run through a series of checks including edit checks and budget checks. FIN edit and budget check errors of payroll processing are available for review and correction by the individual agencies.

Payroll figures are posted to the GL as follows:

- Gross pay is an expense (5XXXXX),
- Employee and employer deductions as a payroll payable (200001),
- Net pay as cash (101000).

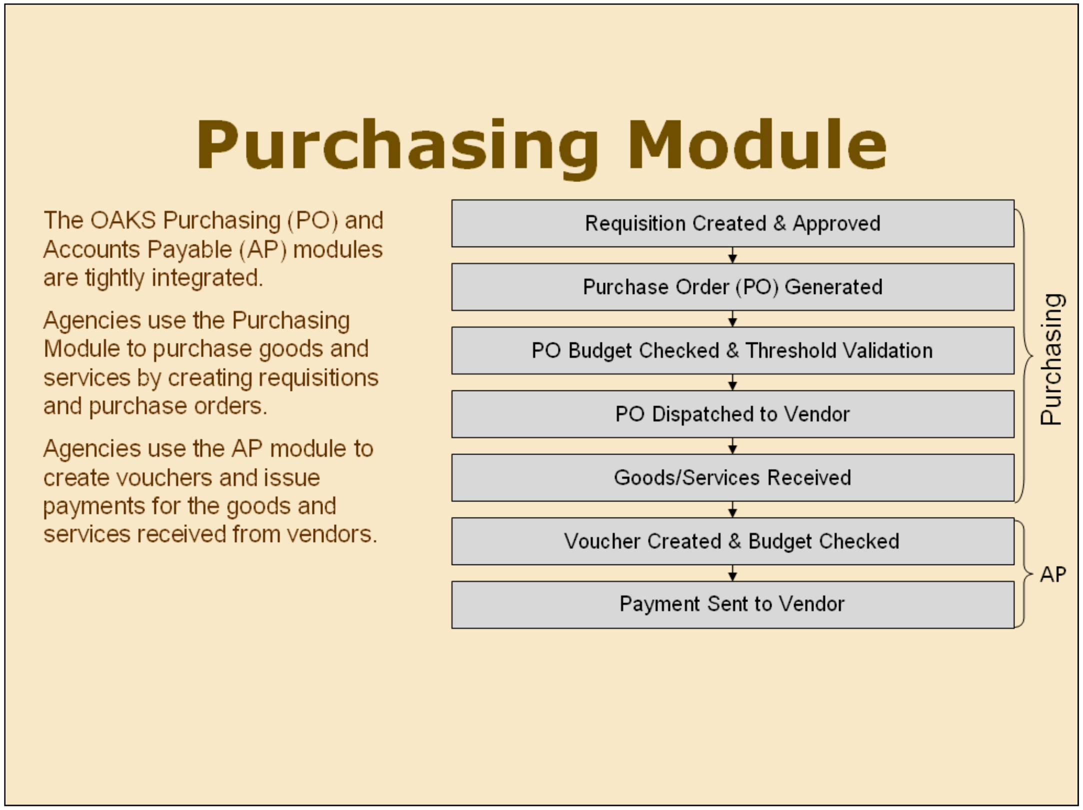
The FIN general ledger is accurately updated with HCM gross pay figures from payroll processing. Payroll data in FIN (GL) do not contain employee or agency-specific transactions, as they do in HCM, because the data is stored in a summarized format for each agency.



Purchasing

Agencies use the purchasing screens to enter requisitions and create and monitor purchase orders. Approved non-debit expenditures that exceed $500 require an approved purchase order. All special approval validation vouchers require an approved purchase order, regardless of the amount. Exceptions include items such as utility or subsidy payments. Additionally, special approval validation purchases charged to certain account codes and all purchased personal services require a PO. A requisition is a request to purchase goods or services. The purchasing module supports the requisition life cycle, which includes these steps:

1. Agencies create a requisition in OAKS.
2. The agency approver approves the requisition.
3. OAKS creates a purchase order (PO) from the approved requisition through a process called sourcing.
4. OAKS performs budget and Controlling Board threshold checks.
5. An agency requisitioner dispatches the PO, and OAKS automatically completes the dispatch process via e-mail (if the vendor does not have a valid e-mail address, it is printed and mailed to the vendor).
6. The agency receives the goods or services.



Purchasing Module

The OAKS Purchasing (PO) and Accounts Payable (AP) modules are tightly integrated.

Agencies use the Purchasing Module to purchase goods and services by creating requisitions and purchase orders.

Agencies use the AP module to create vouchers and issue payments for the goods and services received from vendors.

Requisition Created & Approved
Purchase Order (PO) Generated
PO Budget Checked & Threshold Validation
PO Dispatched to Vendor
Goods/Services Received
Voucher Created & Budget Checked
Payment Sent to Vendor
Purchasing
AP

Entering and Approving a Requisition

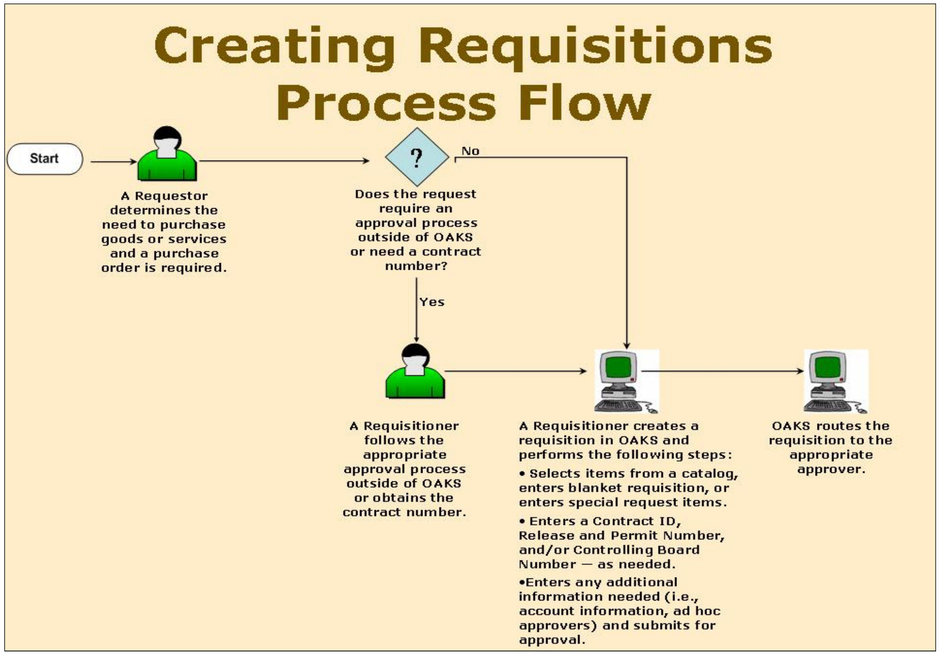
The first step to purchasing goods or services is for a requestor to initiate a request for the goods/services. Only agency users with the “Requisitioner” role have the ability to create requisitions within OAKS. A “Requisitioner” first selects the agency “requestor” (who may or may not be the “Requisitioner”) from a drop-down list of pre-defined requestor names. For example, when a clerical staff person prepares the requisition for his boss, he must have the requisitioner role to use the system. The clerical staff person will select a “requestor” which could be his boss, himself or some other individual on the drop down list.

The workflow approval path is determinate upon the chosen requestor (Requestor A dictates approval path 1; requestor B dictates approval path 2, etc) and three of the first four approval levels can be an individual or group. The Requisitioner then creates the requisition within OAKS. Required verification fields within OAKS requisition processing force the user to enter the following fields: requestor ID, category code, item description, units of measurement, quantity, price, ship to code, fund, account, ALI, department, and program code chartfields. Additionally, online edit checks prevent or detect incorrect entry of fund, account, ALI, department, program, grant/project, and project codes when creating a requisition. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved. As the account coding is being entered, the system is verifying the information against predetermined coding and will identify any incorrect entries in red. The OAKS application provides users with pre-populated data entry options in key fields to reduce input errors. Data input that does not match one of the entry options is rejected and the user receives an error.

Before a requisition can be processed into a PO, a level 4 approval is required. Beginning in January 2009, an edit was built into FIN to prevent a level 4 approver from approving their own requisition. The final level of approval (level 4) must be an individual and not a group. Although not required, agencies may elect to first have a level 1, level 2, level 3, or ad-hoc optional approver, if they desire. Only authorized users from each agency with the “Approver” role can approve requisitions within OAKS. Approval paths are determined by the agencies and set up in OAKS by OAKS staff through workflows. Only authorized OAKS staff can modify the approval paths, documented on the workflows, based on OAKS Agency Financials Security Application requests from the agencies. The agency’s decision regarding the number of approvals required is submitted to OAKS via the OAKS Agency Financials Security Application, and is maintained in the agency’s OAKS workflow.

Approvers are notified via e-mail that a requisition is ready for their approval. OAKS automatically creates a timestamp at each stage of the approval process that includes the user ID, the date and time of the approval, and any notes manually entered by the approver. If the approver changes the dollar amount of the requisition, the requisition must go back through the requisition process. A level 1, 2, or 3 approver can change the coding of the requisition and still mark the requisition as approved without retriggering the workflow process. The level 4 approver cannot change anything on the requisition without retriggering workflow and forcing the change to be resubmitted back through the original workflow/approval process. Once the first approver has approved the requisition, another notification e-mail is sent to the next level approver. For personal service purchases, a contract or agreement is scanned and attached to the requisition. Edits prevent transactions that exceed the Controlling Board’s threshold limit of $50,000.00. Agencies that have obtained a Controlling Board waiver for greater than $50,000 cannot process transactions that exceed the waiver amount.

After a requisition receives all necessary approvals, OAKS "sources" a requisition to a PO. When OAKS "sources" a requisition to a PO, it is automatically creating a PO based on information from the approved requisition. OAKS does not provide notification to inform a requisitioner that a requisition has not been successfully sourced to a PO. It is the requisitioner’s responsibility to monitor the progress of a requisition by checking its status in OAKS through the Sourcing Workbench page. The Sourcing Workbench page displays monitoring and disposition details on each requisition that goes through the sourcing process.



Creating Requisitions Process Flow

A Requestor determines the need to purchase goods or services and a purchase order is required.

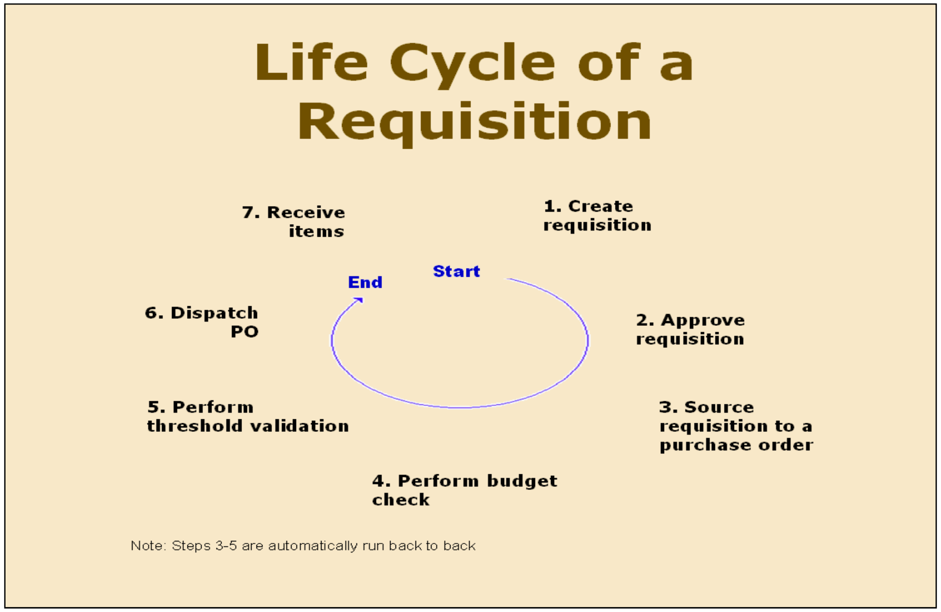
Does the request require an approval process outside of OAKS or need a contract number?

A Requisitioner follows the appropriate approval process outside of OAKS or obtains the contract number.

A Requisitioner creates a requisition in OAKS and performs the following steps:

- Selects items from a catalog, enters blanket requisition, or enters special request items.
- Enters a Contract ID, Release and Permit Number, and/or Controlling Board Number — as needed.
- Enters any additional information needed (i.e., account information, ad hoc approvers) and submits for approval.

OAKS routes the requisition to the appropriate approver.



Life Cycle of a Requisition

1. Create requisition
2. Approve requisition
3. Source requisition to a purchase order
4. Perform budget check
5. Perform threshold validation
6. Dispatch PO
7. Receive items

Note: Steps 3-5 are automatically run back to back

Vendor Information

Vendors were originally converted from the CAS application to OAKS. Vendors were then automatically assigned a unique sequential Vendor ID number (different from their tax ID number) by the OAKS system. The first 500 vendor ID numbers are reserved for petty cash vendors. State agency vendor numbers are also unique and are not sequentially assigned. Until September of 2009, vendor information was maintained by OBM. After September the OSS (Office of Shared Services) was responsible for maintaining vendor information.

For first three months of fiscal year 2010 for all vendor modifications and state employee creations, the documentation was only maintained for one month. Beginning in October 2009, OSS maintains all vendor addition and change documents indefinitely within the vendor record in OAKS.

Only authorized users can create or modify vendor information in OAKS. The Ohio Shared Services complete additions and modifications to the vendor file based on documented change or addition requests submitted by the vendors. All new or changed vendor information is entered and modified by shared services based on the respective vendor information form that the vendor submits. All vendor information forms are available to the public and can be downloaded from the OSS website at: http://ohiosharedservices.ohio.gov/Vendors.aspx. The following forms are available:

- Authorization Agreement for Direct Deposit of EFT Payments (OBM-1234)
- IRS Form W-9
- IRS Form W-8ECI
- Direct Deposit Form (OBM-5678) (MEDICAID - to be used by ODJFS Medicaid Providers only)
- State Employee Information Form (OBM-3458)
- Vendor Information Form (OBM-5657)
- 1099_Correction_Duplicate_Form (OBM-7501)

Vendor information forms can come into the OSS by mail, email, of fax. Mailed forms are scanned by the mail room into a folder on the shared drive that automatically empties into a database know as the Vendor Maintenance Tracker. Email and faxed forms are automatically moved from the inbox where they were received to this same folder, and loaded into the tracker. From the tracker, an agent at OSS changes that status of a group of claims from “Not started” to “In progress” and begins reviewing the forms received. The agent first searches for the tax ID and name in OAKS to ensure that an account for the vendor does not already exist, and ensures the vendor name, address, and tax ID match on all forms and that the forms are complete. The agent enters the vendor information into OAKS and a unique vendor ID is automatically assigned to vendor. They then set up the vendor for check payments. All forms are attached as a PDF to the OSS tab of the Vendor record in OAKS. Approximately 1,600 changes are made to the vendor table each month.

Of the eight OSS vendor maintenance agents, four senior agents hold the role of approver as well. For these senior agents,, simple vendor changes for address, pay terms, or contact information or additions including name, address, and tax ID only, are entered into OAKS with a status of “Approved.” All other additions or changes are entered as “Unapproved” and the changes must be reviewed by a different senior agent for accuracy. For all other agents, all additions or changes are entered as “Unapproved.” Once an approver has reviewed a vendor addition or change, the status is changed to “Approved.” Input documents for vendor additions and modifications are reviewed by the OSS approvers to validate that vendor information was completely and accurately entered. OSS maintains several spreadsheets to track the number of vendor additions/changes input by each agent, as well as the accuracy rate of each agent. The OSS does not have a formal process to verify that vendor changes are only requested by authorized vendor contacts.

Vendors are required to have a unique vendor ID and unique identifier (tax identification number) within OAKS to help prevent the entry of duplicate vendors. A "Check for Duplicates" option is available when adding a new vendor that identifies existing vendors with the same tax ID or same name. Required verification fields within OAKS force the user to enter the following fields when adding a new vendor: SetID (always = STATE), Vendor ID (assigned by OAKS), Vendor Short Name, Vendor Name, Status, Tax Identification number, Address, and Location. In addition, online edit checks prevent or detect incorrect entry of vendor ID type and tax ID when adding a vendor. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved. OAKS issues unique vendor ids for all new vendors.

A search option is available to allow agencies to select any vendors listed in OAKS, regardless of the agency. When the vendor is selected, OAKS pre-populates the vendor address and payment terms. Vendors in OAKS must have a status of "Approved" before a voucher and payment can be issued to the vendor.

Many vendors have multiple addresses assigned to their individual vendor ID number to accommodate various locations and business rules such as selected methods of payment. This requires careful selection by the user when selecting the vendor, because the user must ensure they have selected the correct address. Vendors in FIN are not assigned to a specific agency. Any agency may use a vendor once they have been added to the vendor database.

EFT Vendors

Vendors that are paid by EFT are required to complete and sign a direct deposit authorization form. The banking information is entered within the vendor record in OAKS.

OSS enters the vendor information, including vendor ID (or employee ID), bank account and routing number, and account type into the OAKS FIN Vendor Database. The forms are attached as a PDF to the vendor record through the OSS tab. EFT authorization and change forms must be accompanied by bank verification (a voided check or signed bank letter). The OSS now accepts fax or e-mail copies of these forms. The vendor name, address, and bank information on the EFT form and on the bank verification must match the name and address on file for the vendor, or the OSS will not add or change the EFT information and a letter will be sent to the vendor detailing the missing information.

For Medicaid-only providers who are paid from ODJFS, only EFT information is stored in OAKS. Once the OSS receives a Medicaid-only EFT form, an agent verifies the information on the EFT form against the provider information in the ODJFS Medicaid Management Information System (MMIS). The agent matches the Tax ID, provider name, and address to the request form and any banking information attached, and enters the name and banking information into OAKS. No other information is stored in OAKS and no vendor number is issued to these types of accounts. Forms are then attached to these types of accounts using the OSS tab.

When a vendor is set up in OAKS, the default payment type under the "Location" tab of the vendor information screens is set to "Check." If EFT information is received, the default payment type is changed to EFT (if the vendor has 1 address, if 2 or more addresses, the check location remains default). The bank name, routing number, account number, and account type are entered into the vendor payables options screen. OSS checks the "Pre-Notification Required" box on the EFT options section and selects "Payment Only" in the transaction handling section to automatically place a seven-day waiting period on paying the vendor via EFT. When the next pay cycle is run, the routing and account numbers are automatically validated with the bank and the vendor is paid by check. If the information is not valid, an error is received on the Key Total Treasurer (KTT) report; if the information is valid, the vendor will be paid by EFT the next time a payment is submitted or pre-note is complete.

OAKS has an edit in place to prohibit the submission of an EFT voucher for a vendor without EFT information in the FIN system. If an agency attempts to submit a voucher with a location type of EFT but there is no EFT information entered in the system, the payment will automatically default to a warrant during processing.

OSS performs periodic tasks to help ensure vendor information is being timely updated based on the forms received. A query is periodically run to identify vendors that have been in an unapproved status for more than a few days. An OSS agent follows up on these items to determine the reason for the delay.

Budget Check / Dispatch Process

1. Vendor transactions must pass a pre-defined set of budget rules to determine if the payment is allowable for processing. The budget checking process runs to ensure that chartfield strings on distribution lines are valid and to determine whether there is sufficient appropriation to cover the cost of items on a PO.

2. Should a PO fail a budget check, the agency will need to correct the error before continuing through the requisition life cycle.

3. Threshold validation verifies the requisition or purchase order does not exceed the maximum amount the state allows an agency to spend per vendor, per year, for non-contract purchases. OAKS performs an initial threshold validation when a requisition is created. After OAKS budget checks the PO, a final threshold validation is run on the PO. If a PO fails threshold validation, the agency must cancel the PO and edit the requisition.

    a. The upper threshold, above which all agencies cannot approve transactions, is $50,000.
    b. Controlling Board waivers can be obtained for transactions that exceed $50,000. When the controlling board waiver number is entered into the requisition, OAKS checks to ensure the transaction does not exceed the approved limit for the corresponding waiver number.

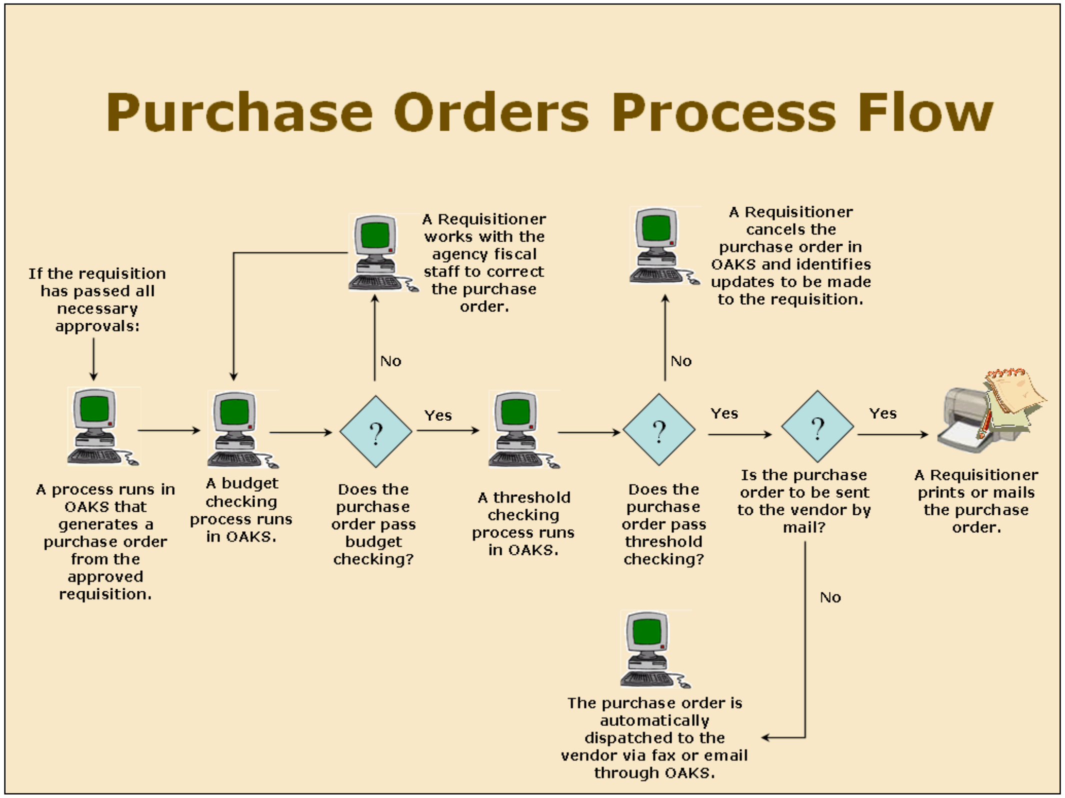
Only authorized OBM budget analysts can create or modify agency budget information in OAKS. Modifications must be accompanied by a change request form. A purchase order must pass “Budget Check” before it can be “dispatched” and used for payment processing. Budget Check validates that sufficient funds are available for the PO and, if successful, automatically encumbers the funds. The budget check sets the accounting date. Purchase orders that fail the budget check process are listed on an exceptions screen and are available for review by agency staff. Budget Check is automatically run five times throughout the day.

The Commitment Control page can be used to show budget exceptions by selected budget. Each day, the agency must check the Commitment Control screen to determine if any documents have failed. The agency must make appropriate changes to failed documents before the item can be purchased. The Reconciliation Workbench is available to agencies to search for POs that fail budget check or threshold validation.

Dispatching a PO makes it available for use by voucher creators. A voucher cannot be created from a purchase order unless the purchase order has been “Dispatched.” When a voucher is processed against a PO, the PO balance is automatically reduced by the voucher amount. Requisitions and vouchers must have a date within the current or future fiscal year. The PO will remain open in the system until manually closed; it does not automatically close if there are no funds left on the PO. The agency can print a report from OAKS of all open POs. Generally, blanket POs are entered as “Special Requests.” The purchase orders with uncorrected errors will remain on the exception list until the fiscal year end. Items with errors are not removed from the Commitment Control screen once corrected; they are maintained as an audit trail until fiscal year end. Once the PO has a valid Budget status (without budget errors), the agency can dispatch the PO and make the purchase.

OAKS reflects the amount remaining for the budget after the PO has been dispatched. If a subsequent adjustment needs to be made to the PO, notification must be sent to the agency finance director for the additional amount of appropriation needed so a journal entry can be prepared and submitted to OBM for approval. Only OBM budget analysts can post journal entry adjustments in OAKS.

The following chart depicts the general creation, approval, and dispatching process for a purchase order in OAKS:


Purchase Orders Process Flow
If the requisition has passed all necessary approvals:
A process runs in OAKS that generates a purchase order from the approved requisition.
A budget checking process runs in OAKS.
Does the purchase order pass budget checking?
No
A Requisitioner works with the agency fiscal staff to correct the purchase order.
Yes
A threshold checking process runs in OAKS.
Does the purchase order pass threshold checking?
No
A Requisitioner cancels the purchase order in OAKS and identifies updates to be made to the requisition.
Yes
Is the purchase order to be sent to the vendor by mail?
Yes
A Requisitioner prints or mails the purchase order.
No
The purchase order is automatically dispatched to the vendor via fax or email through OAKS.

Closing a PO

OAKS does not automatically close a PO once the balance reaches zero; therefore, the PO must be manually closed. In order to close a PO, a program must be run to remove the zero balance POs from all open PO reports or queries If all applicable vouchers have not passed budget check and processed for payment, the PO cannot be closed.

Accounts Payable

Vouchers are entered into OAKS to initiate payment to a vendor as either a PO voucher or non-PO voucher (otherwise known as a "Debit" voucher). A vendor is a person or company who provides goods or services to the State of Ohio.

The process to create a PO voucher is initiated by the creation of a requisition in OAKS. The requisition is subsequently generated by OAKS into a PO. Once the approved PO is dispatched to the vendor, the vendor sends an invoice to the state requesting payment. Once an invoice is received, a voucher is created and used to initiate payment to the vendor. Vouchers also initiate payments to other state agencies, an employee, a taxpayer, or a grant recipient. PO vouchers reference a PO and may also reference a receipt.

The Accounts Payable module supports the voucher life cycle, which includes the following steps:

1. Agencies create a voucher in OAKS.
2. OAKS matches the voucher to a PO and receipt. (PO Voucher only)
3. The agency approver approves the voucher.
4. OAKS performs a budget check.
5. OAKS performs a threshold check.
6. OAKS creates accounting entries for the voucher.
7. OAKS creates the payment and then creates additional accounting entries for the payment.

Creating a Voucher

The Agency Voucher Processor (Processor) is responsible for entering the invoice information into OAKS to create vouchers for payment. If the PO is not identified on the invoice, a search/worksheet function can be utilized and the purchase order information can be copied to the voucher. OAKS does not allow for the entry of a voucher with a duplicate voucher ID or business unit, invoice number, and dollar amount. An online error is received and will prohibit further processing. Required verification fields within OAKS voucher processing force the user to enter the following fields: voucher ID, invoice ID, invoice date, last receipt date, address code, pay terms, and account. Additionally, online edit checks prevent incorrect entry of fund, account, ALI, department, and program when creating a voucher. When entering ISTV vouchers, the cross reference field must also be populated.

A voucher number is automatically and sequentially assigned, if not manually entered by the user, once all required payment information has been entered. Voucher numbers are in sequential order by agency. The OAKS application provides users with pre-populated data entry options in the key fields of voucher entry processing to reduce input errors.

PO Vouchers are created by copying purchase order line item(s) into a voucher (i.e. quantity, price, distribution coding). The voucher total is automatically populated with the remaining balance of the PO; however, this amount can be manually adjusted to pay only a portion of the remaining balance.

PO vouchers are automatically processed through matching, in batch, every two hours in order to update the PO information. If a voucher is not matched to a PO successfully, it is listed on an exceptions screen and is available for review by agency staff. Vouchers are subsequently routed through Workflow for approval through a batch process that runs every fifteen minutes. Once a voucher is approved, it is processed through budget check which updates the budget to increase the expenditure and the encumbrance is thus decreased. The actual GL entries for a voucher are generated by Journal Generator. Agencies are able to view other agencies' payments and General Ledger.

Vouchers for non-debit expenditures less than $500 can be submitted without a corresponding PO. Agencies may create "Speed Charts" of codes with predetermined Fund, ALI, Department, Program, Grant/Project, etc. These "Speed Charts" allow agencies to more efficiently define distribution coding on a voucher.

Voucher Approval

Vouchers are required to be approved before a payment can be processed against it. Vouchers may require up to three levels of approval at the agency level. Only one approval is required by the system; however, agencies may elect to require more, before they are submitted for payment processing. Only authorized users from each agency with the "Approver" role can approve or deny vouchers within OAKS. This process is defined through a workflow. Vouchers awaiting approval will appear in the approver's "Worklist" within OAKS. If the approver does not agree with the accounting information on the voucher, the approver must deny the voucher to allow the voucher processor to make the necessary changes to the voucher, as the system does not allow a user to approve a voucher that they have either entered or updated. After the voucher has been approved by the agency, an additional approval may be required as determined by OBM based on the account code entered on the voucher, or if an ISTV Xref has been defined on the distribution line. If this is the case, a message will appear after the agency approves the voucher indicating that additional approval is needed. The voucher will be identified as having a "pending" status and will be routed to the next approver.

Only the employee ID of the voucher processor is displayed on the voucher; however, the identity of the approver user ID is available through a query. If the approver denies the transaction, they must enter an explanation/reason for the denial and save the document. The system will notify the creator via e-mail of the denial. The creator/processor must correct and resend the document or delete it. However, the system does not keep track of denied transactions; once corrected or deleted, the denial information is lost.

Payment Processing

Once all the voucher coding information is entered and approved, the processor will go to the payment screen and select the payment location code, payment method (CHK- warrant, EFT, ACH, GE - ISTV), and the handling code. This information is defaulted from the vendor entered on the voucher; however, the payment information can be changed as appropriate. There are two voucher styles available, RE or RA. RE (regular) means that all payments for any voucher to that particular vendor based on the payment will be accumulated into one payment ID (i.e. warrant number) and the payment is distributed to the vendor through Key Bank (contracted by the state as of November 2008) for EFT payments or mailed by state printing for warrant payments. RA (return to agency) means that all payments for any voucher to that particular vendor based on the payment method will be accumulated into one warrant and the agency will handle the warrant distribution. The system defaults to RE.

The payment process (Pay Cycle) occurs at 2:00 P.M. each day. Checks are cut based on the predetermined pay terms established by the vendor and indicated on the voucher. For example, if the pay term for a vendor is identified as "net 30", the payment will be held until 30 days from the invoice date defined on the voucher. Vouchers are not eligible to be processed through Pay Cycle until they have successfully passed budget checking. If a voucher with a current scheduled due date is not processed through budget check by 2:00 P.M., the payment will be processed for payment on the following business day.

Users can check the status of a voucher by running the "Voucher Activity Report" or the "Voucher Approval Status" query. The "Voucher Activity Report" will give the status of all vouchers for a particular range of dates. The report lists the voucher number, invoice number, PO number (if applicable), the OAKS created Vendor number, and the payment amount.

OAKS will not process purchase orders or vouchers in excess of the available budget. Transactions that have failed budget check can be viewed on the Budget Check Exceptions Screen. The PO and voucher process automatically update the corresponding commitment control budget. The voucher posting process creates the voucher accounting entries in which the cash account is decreased and accounts payable is increased. The actual GL entries for a payment are generated by Journal Generator. The payment post process creates the payment accounting entries after the payment has been created through Pay Cycle. The voucher post and payment processes are run in nightly batch processing.

Automatic Voiding of Stale Warrants

A job runs on the 8th business day of each month to automatically void unreconciled (non-redeemed) warrants that are over 90 days old. The job runs in FIN and looks for paid, unreconciled warrants that have been outstanding for greater than 90 days from the payment date plus the end of the month. The job does not void EFT payments. Tax refund warrants are voided after 2 years (730 days). When a payment is cancelled or voided in FIN, the commitment control expenses are automatically reduced and available appropriations are automatically restored by the amount of the original payment.

EFT payments are cancelled separately. Reasons for EFT payment cancellations include invalid account numbers, closed accounts, etc. Each day, the bank sends a file to OBM with the details of EFT payments that failed. OBM is also notified of Tax EFT payments that are rejected by the bank. The bank sends a daily interface file of rejected payments to OBM. A job runs daily and cancels tax EFTs payments listed on the bank file. The process voids the payment and it is automatically re-issued as a check.

Journal Generator

Journal Generator is an automated batch process that runs each night. Journal Generator primarily:

- Assigns a journal ID to the transaction.
- Assigns the fiscal year and accounting period (1-12).
- Summarizes accounting entries into journals.
- Creates journals in the Journal Transaction Report (for subsequent GL posting).

This program automatically generates the actual GL entries for vouchers that meet the following criteria:

- Entry status = “Postable”
- Match Status (if there is a PO) = “Matched”
- Approval Status = “Approved”
- Budget Status = “Valid”
- Post Status = “Posted”

Intrastate Transfer Vouchers (ISTVs)

Agency-to-agency billing is accomplished through the accounts payable function using an ISTV.

In the AR module, ISTVs can be prepared as a single transaction or in batches of up to 50 transactions. A group control total must be entered before entering the transactions. The transaction will not process if the total of all lines/transactions does not balance to the control total. Each line will represent an individual bill to another state agency and requires a unique number established by each agency based on their processing needs (shown as BILL and the invoice #). A customer ID, which identifies the payee, must be selected from a pre-populated drop-down box of all state agencies. The line must also contain the fund, account, ALI, department, program, and ISTV cross reference when it is an ISTV. The processor must also enter a reason code. Reason codes were established by the agency based on their processing needs. The processor must then hit the "Create Entries" button, which causes the journal entries to be prepared based on the reason code entered. If there is a problem with one payment within the batch, OAKS requires the entire batch to be resubmitted.

The buying agency must prepare a voucher in the Accounts Payable (AP) module to initiate payment for the bill. The process for entering ISTVs is similar to the process for entering regular vouchers. The agency chooses the selling agency as the vendor. When selecting the vendor for an ISTV, the user must select from a pre-populated drop down listing of all state agencies, which have been set up in OAKS as vendors. OAKS uses the agency Business Unit ID as the customer ID for each state agency. The format of the vendor ID for the selling agency is the agency acronym plus "01" (e.g. AOS01, DAS01, OBM01, etc.). These numbers can be manually entered or selected from a pre-populated menu in OAKS. ISTV vouchers must undergo the same batch processes as all other vouchers to process payment, such as matching (where applicable), approval, budget check, and threshold validation. The buying agency must select the ISTV option to have the payment made electronically. If they do not, a warrant is generated for the payment. The system does not default to ISTV payment for these transactions. To determine if there are any outstanding account receivables, an "Aging Summary by Business Unit" report can be run from OAKS.

Travel Expenses

Agencies use the travel expenses screens to process travel expenses or enter vouchers directly in accounts payable. These transactions require an additional level of approval from OBM.

Accounts Receivable

The OAKS Accounts Receivable (AR) module enables an agency to track and collect money owed to it by organizations and individuals for goods or services provided to them. Accounts Receivable (AR) provides assistance with the creation, maintenance, tracking, and collection of receivables from customers.

Agencies use a pending item to record monies owed from a customer. The Accounts Receivable module supports the pending item life cycle, which includes these steps:

1. Agencies enter a customer in OAKS.
2. Agencies enter a receivable.
3. Agencies enter the deposit into OAKS.
4. The AR examiner enters the information into OAKS to apply the payment and close the open item.
5. The Treasurer of State confirms the deposit.
6. Journal Generator sends Accounts Receivable (AR) accounting entries to the General Ledger.
7. Agencies manage each customer's account to keep open items that are past due to a minimum.

There are three AR processing options an agency can choose to use:

Option 1 – AR Open Item. This option utilizes OAKS *to create pending items and track receivables*. Each customer will have a unique customer number that must be used to process all transactions. This number was created by the agencies. Approximately 20 agencies have elected to use this option.

Option 2 – AR ISTV. This option is used *to process ISTV billings*. Each customer will have a unique customer number established by OBM for consistency across agencies. The selling agency will use this option to create the invoice in OAKS and track the payments received.

Option 3 – Cash Deposits. This option is used by those agencies that have their own systems *to create invoices and track receivables or for other types of collections*. Agencies use this option and Option 1 *to create a Payment Detail Report* (replaces the old revenue receipt document), which accompanies the checks deposited with the TOS. All agencies have the ability to use this option.

Agencies process revenue transactions in OAKS in three primary steps:

- Entering pending (open) items manually or through an automated interface.
- Recording deposits of miscellaneous revenues and customer payments.
- Applying deposits as payments for customer open (unpaid) items or as miscellaneous revenue.

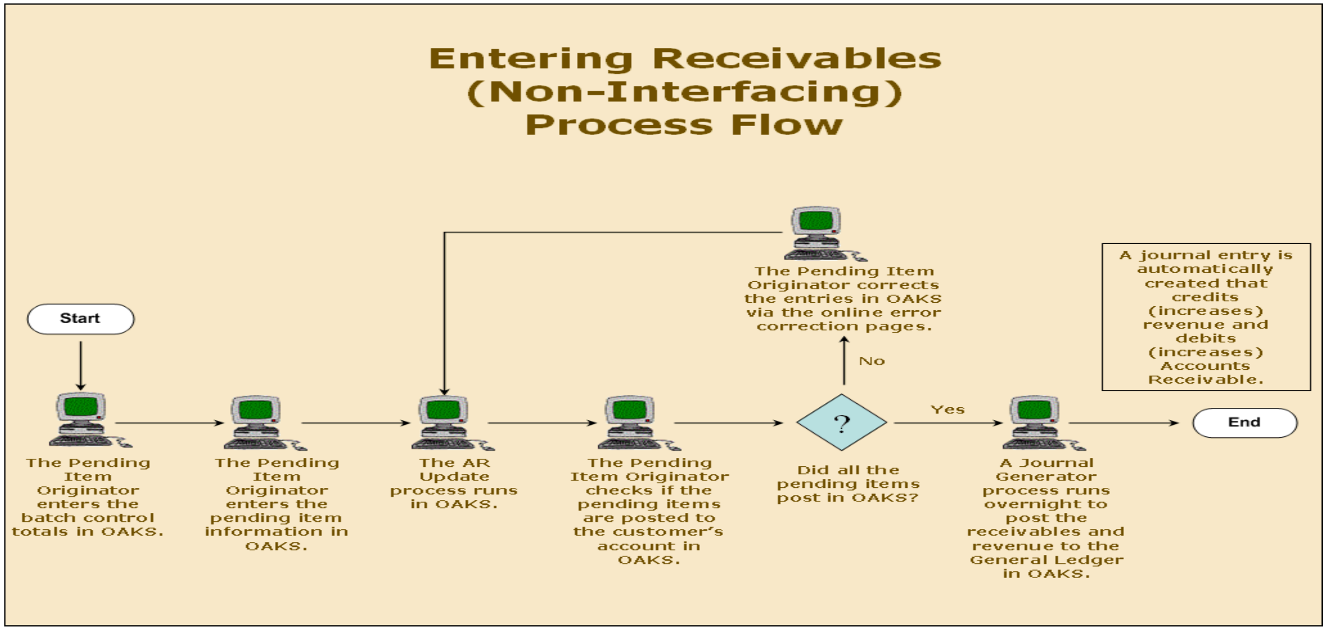
Pending Items (Receivables)

When agencies enter pending items into OAKS in groups, they must enter group totals, called control totals, as well as each pending item. After all of the items in the item group have been entered, OAKS automatically balances the items against the control totals. This allows the agency to validate that they entered all the items for the group.

The revenue is required to be approved. Cognos queries may be run for revenue transactions to identify the transaction approval date, creator ID and approver ID.

OAKS will then automatically run the ARUPDATE process as scheduled. The Budget Check process then runs, followed by the Journal Generator batch process, summarizing the receivables accounting entries and creating journal entries in the OAKS General Ledger. After ARUPDATE and Budget Check are completed, agencies can review the results on the OAKS online error correction pages to determine if there were errors in any groups that need to be corrected.

The following flowcharts reflect the process of entering receivables for both non-interfacing and interfacing agencies:



Entering Receivables (Non-Interfacing) Process Flow

Start

The Pending Item Originator enters the batch control totals in OAKS.

The Pending Item Originator enters the pending item information in OAKS.

The AR Update process runs in OAKS.

The Pending Item Originator checks if the pending items are posted to the customer's account in OAKS.

Did all the pending items post in OAKS?

No

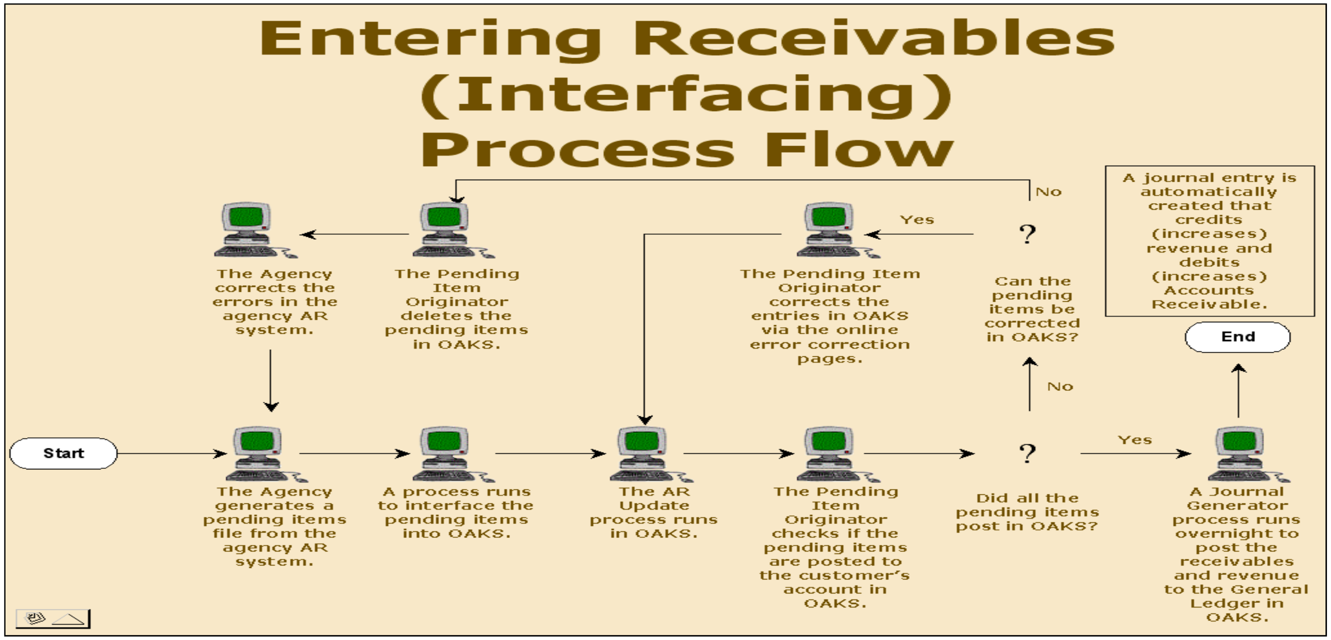
The Pending Item Originator corrects the entries in OAKS via the online error correction pages.

Yes

A Journal Generator process runs overnight to post the receivables and revenue to the General Ledger in OAKS.

End

A journal entry is automatically created that credits (increases) revenue and debits (increases) Accounts Receivable.



Entering Receivables (Interfacing) Process Flow

Start

The Agency generates a pending items file from the agency AR system.

A process runs to interface the pending items into OAKS.

The AR Update process runs in OAKS.

The Pending Item Originator checks if the pending items are posted to the customer's account in OAKS.

Did all the pending items post in OAKS?

No

Can the pending items be corrected in OAKS?

Yes

The Pending Item Originator corrects the entries in OAKS via the online error correction pages.

No

The Pending Item Originator deletes the pending items in OAKS.

The Agency corrects the errors in the agency AR system.

Yes

A Journal Generator process runs overnight to post the receivables and revenue to the General Ledger in OAKS.

End

A journal entry is automatically created that credits (increases) revenue and debits (increases) Accounts Receivable.

The Accounting Date of the receivable determines the fiscal year and accounting period to which the pending item will be posted. OAKS automatically sets the Accounting Date to the current date. Accounting Dates are used as the basis for calculating due dates and aging. The Accounting Date is normally the date when pending items were actually created. Pending Items and Payments must have an accounting date within the current accounting period. Once a period is closed, an item can no longer be posted to it.

When agencies have similar items to enter into OAKS, Groups are used to batch the items together. Groups are collections of pending items that are ready to post. OAKS defines pending items by Group Types and Origin. For example, a Billing Group (B) is created when items are entered online. Agencies have been instructed to always use the value OBILL (Online Billing) for the Origin ID when entering pending items in OAKS. The Billing module uses the value "XBILL" for items created by the Billing module. The Control field is used to record the total amount of the items in the group, and the Count field is used to enter the total number of lines of the pending items in the group. The Control Data field area is used to record agency processing information. OAKS automatically sets the Received and Entered date fields to the current date; however, they are modifiable by the agency to reflect the actual date the items were received for processing, or the actual data entry date. The Assign field is used to identify the User ID of the person who is assigned to complete the group. OAKS automatically sets this field to the User ID of the person creating the group. OAKS uses the Group Status field area to display current status information for the group. Pending Item groups must be in balance and the posting status manually set to "Batch Standard" to post during ARUPDATE. The Entry Type field identifies the type of the pending item. Entry Type codes are:

- **INV** - Third-party invoice
- **CR** - Third-party credit memo
- **DR** - Third-party debit memo
- **ISTV** - Interagency transfer invoice
- **ISTCR** - Interagency credit memo
- **ISTDR** - Interagency debit memo

The following search options are available to agencies to find pending items:

- **Not Posted** - No one has set the group ready to post.
- **Complete** - OAKS has processed and posted this group.
- **Errors** - OAKS encountered errors in at least one pending item in the group and did not post the group.

OAKS does not allow for the entry of a pending item with a duplicate group ID number.

Receiving and Processing Payments

Payments may be in the form of cash, check, or any other negotiable document the state accepts. The state (or individual agency) designates a bank or banks to receive the deposit, consisting of all payments processed by an agency or its bank. The Treasurer of State's office (TOS) confirms all deposits. Customer payments may be received in OAKS in multiple ways:

- Mail-in and over-the-counter cash and checks.
- Lockbox interface - Payments received at a bank.
- Automated Clearing House (ACH) interface for credit card transactions.

- Electronic interface - Non-OAKS agency file transfers.
- Manual ACH deposits.
- Ohio Business Gateway (OBG).

OAKS requires a Deposit ID for each entry of a deposit that must be a unique number for each agency. A Deposit ID can be system created or manually assigned. When receipts are entered in batch, control totals must be in balance with the details of the batch before accounting entries can be created. Batch control totals ensure that a deposit group is balanced before it can be posted. OAKS deposit groups are also assigned a deposit type, which defines the deposit category for the entire batch. Each batch contains only deposits of a single type. The deposit type varies depending on the nature of the transactions. The deposit types include:

- **A -** AG Receipts.
- **B** - Buy-Back.
- **C** - Customer Receipts.
- **D** - Credit Card Receipts MAF. (Multiple Alignment Format)
- **E** - Employee Receipts.
- **F** - EFT Receipts ACH.
- **L** - Lockbox Receipts.
- **M -** Miscellaneous Receipts.
- **X** - Deposit Modifications.

When the agency receives the deposit item, the deposit entry is made into OAKS. If an agency receives a lockbox deposit from the bank, a nightly process runs to upload a formatted lockbox deposit file from the bank into OAKS. AR payments can be applied three ways:

- Automatically to pending items using the Payment Predictor method.
- Manually to a pending item.
- Journalled directly to apply the accounting entry for miscellaneous revenue.

Next, the ARUPDATE process will run in OAKS. If the deposit entry passes the ARUPDATE process, the Payment Detail Report is printed from OAKS by the AR Administrator. If it does not pass ARUPDATE, the Revenue Processor corrects the deposit errors and resubmits the deposit for the ARUPDATE process. The AR Administrator reviews, approves, and signs the Payment Detail Report. The AR Administrator then submits the Payment Detail Report, plus any deposit items, to the TOS. If the TOS confirms the deposit, the budget check and Journal Generator processes run overnight to post the deposit to the General Ledger.

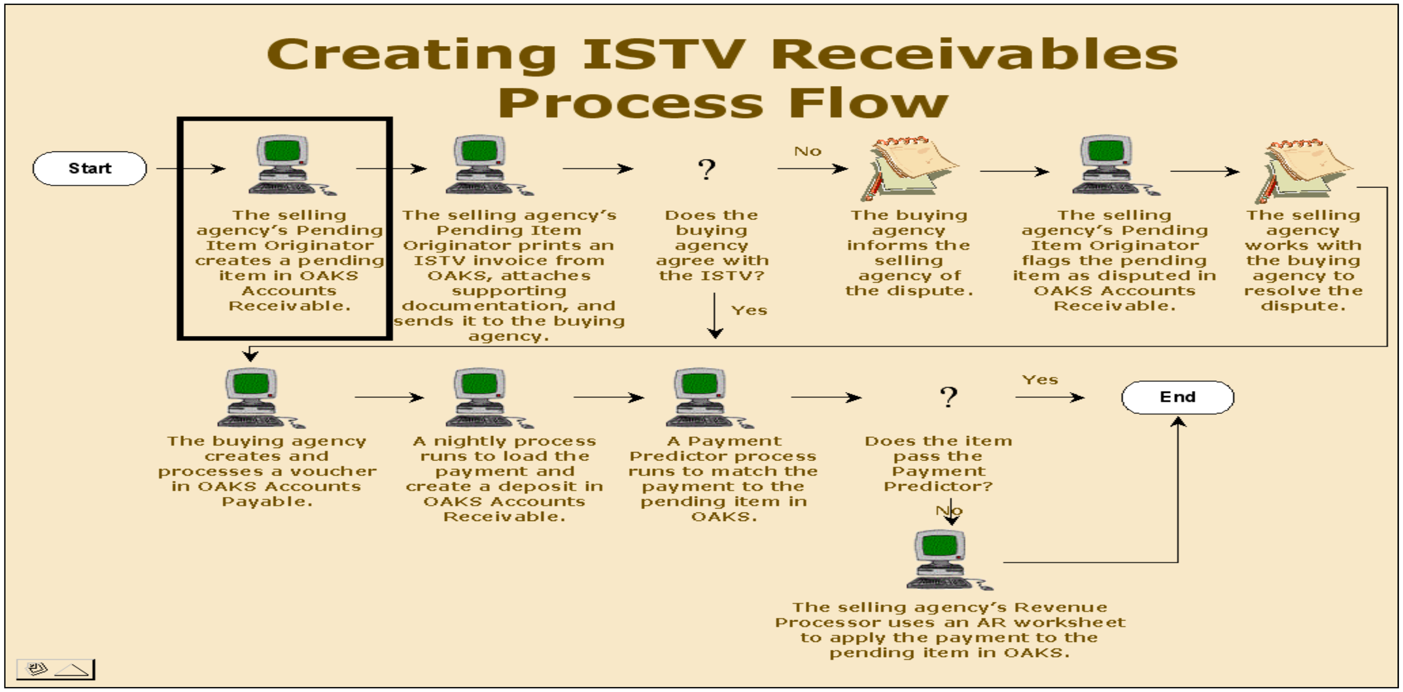
Direct Journals

Agencies use the Direct Journal application method to process miscellaneous revenue in OAKS Accounts Receivable. The Accounts Receivable module supports the direct journal life cycle**,** which includes these steps:

1. Agencies enter the deposit into OAKS.
2. The revenue processor enters the revenue accounting distribution information in OAKS AR as a direct journal.
3. The Treasurer of State confirms the deposit.

4. Budget Check process validates accounting entries.
5. Journal Generator sends Accounts Receivable (AR) accounting entries to the General Ledger

ISTV Receipt of Payment



Creating ISTV Receivables Process Flow

The selling agency's Pending Item Originator creates a pending item in OAKS Accounts Receivable.

The selling agency's Pending Item Originator prints an ISTV invoice from OAKS, attaches supporting documentation, and sends it to the buying agency.

Does the buying agency agree with the ISTV?

The buying agency informs the selling agency of the dispute.

The selling agency's Pending Item Originator flags the pending item as disputed in OAKS Accounts Receivable.

The selling agency works with the buying agency to resolve the dispute.

The buying agency creates and processes a voucher in OAKS Accounts Payable.

A nightly process runs to load the payment and create a deposit in OAKS Accounts Receivable.

A Payment Predictor process runs to match the payment to the pending item in OAKS.

Does the item pass the Payment Predictor?

The selling agency's Revenue Processor uses an AR worksheet to apply the payment to the pending item in OAKS.

When a state agency bills another agency for services, an IntraState Transfer Voucher (ISTV) must be entered as an ISTV pending item in OAKS Accounts Receivable. The ISTV pending item is created in the same manner as a regular accounts receivable item. Required verification fields for a pending item (including an ISTV entry type) force the user to enter a group unit, group ID, group type, origin ID, format currency, count, item ID, customer, amount, business unit, entry type, and reason for an ISTV entry type before the transaction can be processed. When selecting the vendor for an ISTV, the user must enter a state agency or select from a pre-populated drop down listing of all state agencies. Each agency is defined as both a customer and a vendor. Buying agencies are customers for selling agencies in OAKS Accounts Receivable. The person who creates the item is known as the Pending Item Originator. The Pending Item Originator is able to create and approve ISTVs without additional approval.

After the selling agency creates the pending ISTV item, the selling agency prints an ISTV invoice from OAKS, attaches supporting documentation, and sends it to the buying agency. If the buying agency does not agree with the ISTV, they will flag the pending item as disputed in OAKS AR, and will work with the selling agency to resolve the dispute. If the buying agency agrees with the ISTV, the buying agency creates and processes a voucher in OAKS Accounts Payable. The PayLoader process will create a deposit in OAKS Accounts Receivable. Then the Payment Predictor process (see ISTV process flow diagram) runs to match the payment to the pending item in OAKS. If the payment does not pass Payment

Predictor, the selling agency will create an AR payment worksheet to manually apply the payment to the pending item in OAKS. OAKS does not allow for the entry or posting of an ISTV with a duplicate bill number, dollar amount, vendor, and item ID.

ISTV payments received by the selling agency are identified by the User ID “OHBATCH”. Any transactions identified under this User ID are ready for processing/receipt by the selling agency. When processing ISTV revenue transactions, agencies have the ability to use an automated process, known as Payment Predictor, which can be used to match payments to open receivable items. A reason code is required for pending items to designate standard coding to reduce data entry time and input errors. The reason code will automatically populate the appropriate fields with pre-established coding based on the customer number, bill number, and amount. The collection will post when the AR update runs (done 7 times per day). If Payment Predictor does not work (not accepted by OAKS because something did not match), then the processor must create a payment worksheet in OAKS to manually apply the payment to an open item or apply the payment using the “Journal Directly” option. Once the coding information is entered, the system will create the cash side of the journal entry and post the transaction. For ISTV deposits only, after all the payments have been applied or directly journaled, the approval boxes are automatically checked. However, receiving agencies are not notified automatically when ISTVs have been paid. In addition, although agencies have been asked not to do so, OAKS does not prohibit agencies from paying ISTVs via check.

If there is a problem with an individual payment in a batch, the entire batch is held until the correction is made. If the agency cannot resolve the issue immediately or if a payment has already posted, they can “credit” the problem transaction, which cancels it so the rest of the batch can be processed. The problem item will then have to be re-processed. This can be tracked in the customer account screen.

Other than the approval process noted above, ISTV accounts receivables are processed in the same manner as regular accounts receivables.

Cash Deposits

Cash or checks received by the agencies must be deposited with the Treasurer of State. The agency prepares a Payment Detail Report in OAKS that must be approved by an appropriate reviewer prior to submitting the deposit to the TOS. This report contains one line for each type of payment with a summary total of all the individual collections. The agency has the option of using Payment Predictor, which automatically matches the payments to the open pending items, or Journal Directly which provides for manually matching the payments to open pending items, and must also enter a control total. This document is similar to the old revenue receipt document in CAS. Once the AR Revenue Processor (Processor) at the agency enters the revenue information into OAKS for all the payments, the Processor will notify the agency AR Administrator that the deposit is ready for approval.

Required verification fields for a regular deposit force the user to enter a deposit unit, deposit ID, bank code, bank account, deposit type, count, payment ID, currency, and accounting date before the transaction can be processed. When an AR Administrator creates an AR transaction, they have the ability to approve their own transactions. Deposits must be approved by the agency AR Administrator before being transferred to and approved by the TOS. Once the deposit is approved, the Revenue Detail Report is printed and the agency is required to manually include the agency contact information for the deposit (agency, name, department, phone number) on the Payment Detail Report. Each agency is responsible for maintaining the detail information regarding the individual transactions comprising the deposit.

The printed Payment Detail Report and cash/checks are then presented to the TOS for deposit. The TOS will confirm the deposit made by the agency in OAKS, which allows the receipts to post, and prepare a receipt similar to an ATM withdrawal slip to acknowledge the deposit. Because this is an automatic approval by TOS, the deposit and approval dates will always be the same.

OAKS is updated with the TOS Deposit approval status (whether the deposit is approved or rejected), along with the confirmed date. If the deposit is accepted, the TOS will forward a receipt back to the agency with the total amount credited to the account. If the deposit is rejected, the agency must review the deposit to determine the reason for the rejection. OAKS does not automatically notify A/R administrators of payments submitted but not approved.

The OAKS application provides users with pre-populated data entry options in the key fields of pending item entry and deposit/payment processing to reduce input errors. Data input that does not match one of the entry options is rejected and the user receives an error.

Automated Processes

OAKS uses batch processes to update financial information, to send information between OAKS financial modules, and to post accounting information to the General Ledger. Many of these processes run two or three times a day on a fixed, sequenced schedule.

OAKS runs the following automated posting processes to update both Accounts Receivable and the General Ledger:

- ARUPDATE (revenue).
- Budget Check (expenditures).
- Journal Generator (revenue and expenditures).
- Journal Post (revenue and expenditures).

ARUPDATE is the most important of these processes for Accounts Receivable. ARUPDATE is a process that runs to update financial information, create accounting entries, and post items to the customer accounts.

Once ARUPDATE is complete, two additional processes are run. Budget check validates the accounting entries that were created in AR to ensure that appropriation and cash exists. Next, Journal Generator summarizes the receivables accounting entries and creates journal entries in OAKS General Ledger. The pending item and deposit/payment processes automatically update the corresponding commitment control budgets.

Finally, the Journal Post process runs and posts the journal entries to the General Ledger. This process may also be used to post budget journals to the appropriate budget ledger.

Refunds

Any refunds received from vendors, etc. must be entered as a deposit in the AR module. The processor must determine the original coding/entries from the voucher in the AP module (the transaction where the overpayment occurred). The processor must process the transaction as described in Cash Deposits above using the original payment coding information. The system will create the cash side of the journal entry and post the transaction. Refund transactions must then be approved by the AR Administrator.

Miscellaneous Options

OAKS also allows agencies to perform a variety of receivables maintenance functions, some of which include:

- Monitoring customer accounts, including follow-up communications.

- Aging pending items to summarize customer items by days past due.
- Transferring posted items between customers.
- Writing off uncollectible items.
- Creating adjusting entries.

When AR Posting errors occur, the errors and related information are available for the agencies to view and correct within OAKS.

Billing

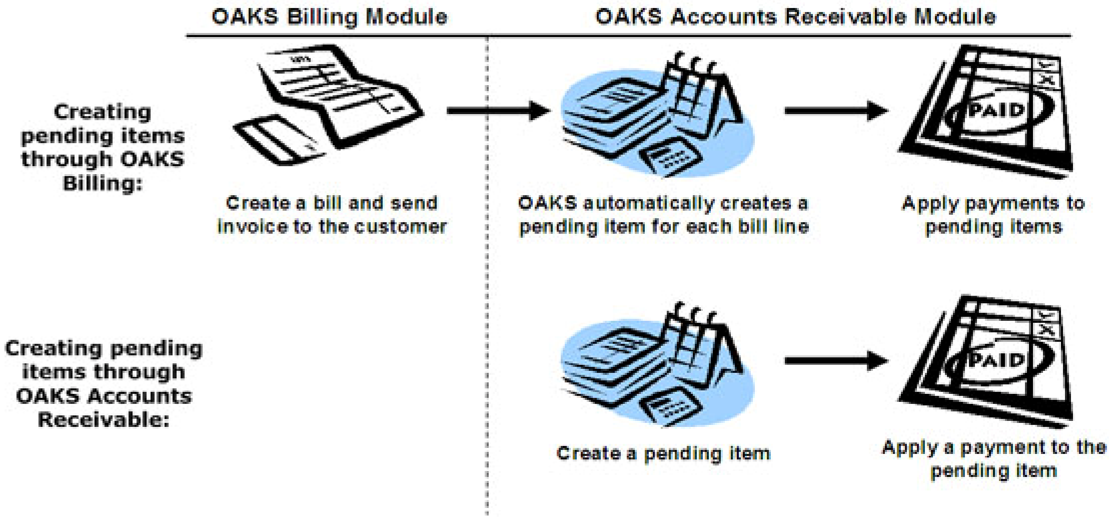
In January 2008, agencies began using the OAKS Billing module, which is used to create bills and print invoices. The Billing module automatically sends invoices to Accounts Receivable (AR) as pending items. OAKS posts revenue created from AR directly to the General Ledger (GL).

Customer information is shared between the OAKS Billing and Accounts Receivable modules. Any changes made to customer information in one module are effective for both modules.

Agencies can create a pending item to which a payment may be applied in two ways: create pending items through bills in OAKS Billing or create pending items in OAKS Accounts Receivable. Agencies can use either method to indicate a customer owes payment for products or services.

In OAKS Billing, an agency Billing specialist creates a bill and the nightly OAKS Billing batch process automatically creates a pending item with the same invoice number in OAKS Accounts Receivable (shown below in row one).

Agencies can also create a pending item directly in OAKS Accounts Receivable (shown below in row two).


OAKS Billing Module
OAKS Accounts Receivable Module
Creating pending items through OAKS Billing:
Create a bill and send invoice to the customer
OAKS automatically creates a pending item for each bill line
Apply payments to pending items
PAID
Creating pending items through OAKS Accounts Receivable:
Create a pending item
Apply a payment to the pending item
PAID

Asset Management

In July 2008, agencies that previously used the Fixed Asset Management System (FAMS) began using the Asset Management (AM) module. Asset records from FAMS were converted into the OAKS AM module by the OAKS team. This change was designed to provide a link between the AM and the Purchasing and AP modules. This link allows much of the asset record to be established automatically without redundant data entry into a separate asset management system. The AM module will manage both stewardship assets (non-fixed assets) and capital assets (fixed assets). Capital (fixed) asset activity is used by OBM to prepare and issue the state's Comprehensive Annual Financial Report (CAFR).

Agencies that did not use FAMS will not use the AM module initially, but have the option to convert their capital asset data from their existing system to the AM module.

OAKS Financials Self-Service Reporting

Agencies can run their own reports to get information when they need it. Agencies can select the format of the report with options such as PDF, Excel, or HTML (a webpage). Several tools are available to run reports. OAKS provides a number of existing reports for agency use from production data. These include SQR (Structured Query Reporter in PDF), PS/nVision (in Excel), and Crystal (in Excel) reports. If users need information that is not available in an existing report, OAKS also has other tools to create, view, and download custom reports. Agencies can use the Cognos query and data analysis software or the PeopleSoft Query (PS Query) to create customized reports from the data warehouse environment. They can choose to share their reports with others or keep them private. PS Query can also be used to analyze data and produce reports from the production environment.

EPM

In addition to the FIN production application, OAKS also has a data warehouse environment known as the EPM (enterprise performance management). EPM is used by OAKS users for producing financial reports and retrieving read-only data for analysis. This data warehouse environment is created by formatting and extracting detail financial data from hundreds of financial and payroll production tables and loading them on a nightly basis into a non-real-time data warehouse. The majority of these nightly updates are incremental; however, depending on the size of the table, a full synchronization of the table may be performed daily. In addition, a near full synchronization of the data warehouse with production is performed weekly for financial data and bi-weekly for payroll data. History is maintained for data in the EPM.

One of the advantages of the EPM is the significant reduction in time to run reports. Only necessary transaction information is copied to the EPM; standing data that does not change often is not copied to the data warehouse. In addition to the OAKS EPM, the OAKS data warehouse environment also contains conversion data from the HR legacy data warehouse and partial financial legacy data (CAS Data Mart) which can be reported out of the OAKS Cognos environment.

For the period of November 2009 through March 2010, a manual process was in place to reconcile date contained in the FIN and HCM databases to data contained in the EPM database. SQL scripts were run against the FIN, HCM, and EPM databases, and on a weekly basis these tables were reviewed by the EPM team with the FIN and HCM teams at the weekly FIN and HCM production meetings and any discrepancies were researched and corrected.

Starting in March 2010, an automated process was put in place to perform the audit between HCM, FIN and EPM data on a nightly basis as data was uploaded to EPM from FIN and HCM databases. This audited information is written to tables and a weekly Cognos report is generated detailing any discrepancies that were noted. These Cognos reports are reviewed as needed by the EPM team and/or the FIN and HCM teams at the weekly FIN and HCM production meetings. Any discrepancies are researched and appropriate actions taken in possible given existing system limitations.

Error reports are also generated during nightly processing if any errors occur during updating. An Incident Report is prepared and posted to the Sharepoint website, and an Alert is posted on the OAKS website. If the error is generated for a critical table, the error receives priority and is fixed immediately. If the error is generated for a table not frequently used, the error will be corrected and updated in the next batch window.

Monitoring Tools

In addition to the OAKS reports and query tools, the agencies can monitor vendor activity using the Controlling Board Threshold search. This allows the agency to determine how much has been paid to/encumbered for a particular vendor so the agency can stay within the $50,000 limit.
The agencies can also identify all voucher activity during a specified period of time using Voucher Activity Report. The report lists all vouchers with the corresponding invoice number and amounts (no vendor names). It also indicates the PO number if applicable and if there were any discounts. Agencies can determine if the payment has been made if the amount is reported in the Payment Amount column. If the payment is still pending, the amount will be shown in the Remaining Amount column. Typically, the review of all activity is limited to a specific agency by the Business Unit; however, viewing the payments made to a particular vendor for any agency state-wide is possible through the AP Payment screens.

In addition, the agency can determine if a check has been paid or redeemed using the AP Voucher screens. Once the particular voucher in question is identified (by entering the number or selecting it from the list of items entered), Payment Information can be selected to provide a payment reference ID, the Payment Date, Payment Amount, Voucher Amount (often different from the pay amount), Paid Status, the Reconcile Status, and the Reconcile Date. If "Recon" is noted with a date, the warrant has been redeemed. Through the AP Payment screens, agencies may view statewide payments made to a particular vendor.

Roles/Security

The OAKS application is designed to provide a segregation of duties between the requisition/PO, voucher, and receipt processing of state transactions. There are several types of viewer modes that are available within OAKS, such as PO, Vendor, Voucher, Travel Expense, P-card, AR, and GL viewers. For example, the AR viewer gives read only access to all AR customer accounts, items, deposits, payments, customer and contact information, as well as generated and printed customer correspondence in OAKS. These views are determined by the PeopleSoft roles and attached permission lists (each role can have one or more permission lists) to define what each agency user can see and do in OAKS.

For more information on roles and security, see the IT Security narrative in Section II and III of this report.

OAKS System Issues and Alerts

OBM makes available a weekly FIN newsletter (Financials Weekly) that contains communications relevant to OAKS and instructions for addressing system issues and agency errors that arose because of incorrect data entry or use of the OAKS system.

The current weekly newsletters, as well as an archive of previous newsletters, are available through the OBM website and announce various system modifications, enhancements and outages, new job aid postings, OAKS system availability, and other helpful information suggested by members of the OAKS management in the Service Assurance group. In addition to being posted on the OAKS website, these items are e-mailed to agency liaisons and agency leadership, as appropriate. The web page (http://www.oakspmo.ohio.gov/oaks/Oaks_Alerts.asp) includes weekly OAKS alerts summary, previous issues, and a list of all OAKS issues to date.

The FIN-related alerts issued during the audit period can be classified/(quantified) into the following categories:

- Batch Processing. (10)
- EPM Data Availability. (72)
- ARUPDATE Process. (5)
- FIN Processing. (18)
- Help Desk / Customer Service. (2)

FINANCIAL APPLICATION CONTROLS FOR OAKS_HCM

On December 18, 2006, the State of Ohio's mainframe-based legacy HR2K payroll system was replaced with a PeopleSoft Human Capital Management (HCM) Enterprise Resource Planning (ERP) system that was designed to create a paperless process from input to payday. The OAKS payroll system is specifically customized for use by state agencies.

The first phase of OAKS implemented the Human Capital Management (HCM) components. These elements include:

- Human Resources: Hiring and maintenance of the workforce. (This element is used by both interfacing and online agencies.)
- Benefits: Calculation of eligibility and enrollment into benefits.
- Payroll: Payroll processing and administration.
- Time and Labor: Time collection and validation.
- ePay: Allows state employees to access their own payroll records online.
- Enterprise Performance Management (EPM): Enables the organization to align information and resources to strategic objectives.

HCM Release 1 was live in production on December 18, 2006, and included Core HR, Payroll, Base Benefits, Time and Labor, ePay, Enterprise Performance Management (EPM) for HCM modules, and HR2K Data Warehouse.

Base Benefits was a manual system that required the manual entry of employee benefit and life event information. Employee benefit (i.e. dental, vision, health, retirement, life insurance) enrollments or changes, one year anniversary changes, updates, as well as changes in employee status, and increase in an employee leave tiers had to be manually entered. During this phase, base benefit data entry was centralized within the Benefits Administration Services (BAS) office within DAS.

HCM Release 2 went live March 27, 2007, and included Benefits Administration, COBRA, eBenefits (open enrollment only), and EPM for Benefits Administration and COBRA.

HCM Release 4 went live in December 2007, and included year-end processing. In January 2008, Time and Labor self-service was started as a pilot program with DAS. Time and Labor self-service allows employees at non-interfacing agencies to directly enter time into HCM using work schedules, as well as request and approve leave time online through OAKS. In February 2008 self-service eBenefits was released.

HCM release 4.1 went live on May 18, 2008, and involved adding additional pilot agencies to the Time and Labor self-service program. There were six agencies in the second pilot program, and currently there are 34 agencies using Time and Labor self-service. Nine agencies have opted out of the Time and Labor Self-Service program and will continue to use their existing systems to interface time to OAKS.

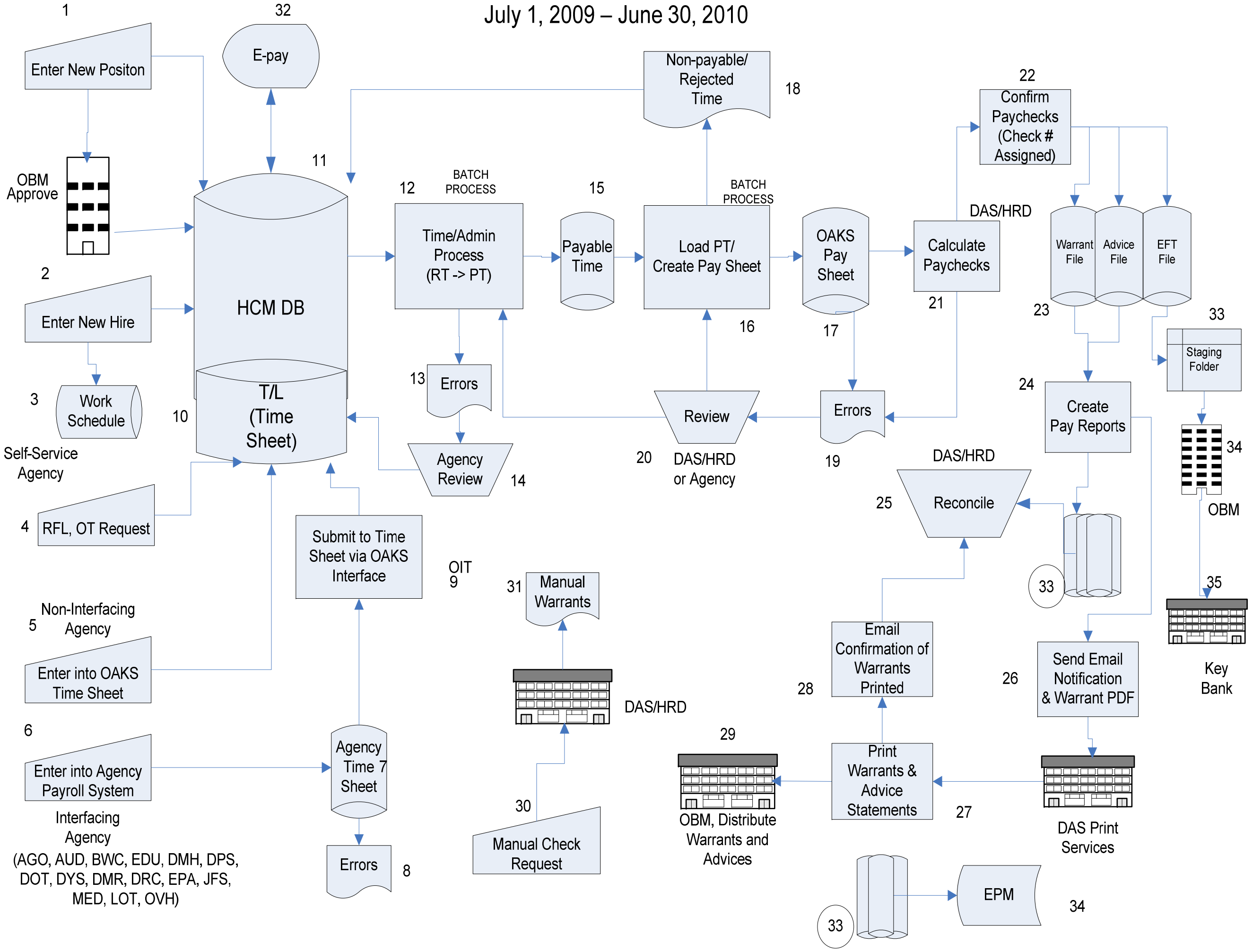
When information is entered into one area of HCM, OAKS automatically shares that information with other HCM components as necessary.

HCM users are grouped according to PeopleSoft (OAKS) roles given to them with different degrees of access. User roles in PeopleSoft are defined based on job responsibilities and have uniquely-defined user access levels to help prevent unauthorized changes to data. User privileges range from full access to read-only to self-service (view paycheck only) access. Each role grants access to specific menu functions and pages to a specific set of users within OAKS.

In addition to roles, row-level security prevents agencies from viewing or changing data from other agencies. Agencies can only submit changes to employees and positions assigned to their agency. Ohio row-level security, which allows access to all OAKS agency payroll data regardless of the associated agency, is restricted to authorized users. Employees may be granted row-level security of OHRL_OHIO for full access to all state agency payroll data (mostly for DAS employees). Limitations are imposed at the agency level by using row level security to restrict agencies from viewing or changing the data of another agency or department within the agency, and can be further restricted as needed by adding a suffix for a particular department within an agency. For example, OHRL_AUD123456 represents a role that allows the user to only access Auditor of State information for department 123456, as indicated by the "AUD" code and department ID suffix.

The following flowchart of the OAKS HCM phase depicts an overview of the payroll process for state agencies. Numbered items in the description of these OAKS HCM controls in the subsequent pages correspond to the numbered items in the flowchart. Numbers are in parentheses.

OAKS Human Capital Management (HCM) Payroll Processing July 1, 2009 – June 30, 2010



Organizational Development

Position information is maintained in the HCM Organizational Development menus. The menus allow maintenance of positions and budgets and creation of job requisitions; review of positions and budget information, including summary, historical, and vacant budgeted position information; creation of reports showing the status and history of positions in the organization; and organization structure and position interface options.

Position Management

All permanent, non-exempt, and non-elected official agency positions and their corresponding pay rates must be approved by an OBM budget specialist prior to assigning an employee to the position. If an existing non-vacant position number is reclassified to a different category, a personnel action form must be sent to DAS for approval (1). Functionally, this requires a manual modification in the system to change a position from “proposed” to “approved.” Elected officials, as well as legislative and judicial agencies, are not required to submit these requests, nor do temporary positions require approval.

Only authorized OBM budget specialists and elected agency payroll officers are assigned the roles that allow approving positions within OAKS HCM. OBM budget specialists are assigned a role that allows approval of new positions. In addition, for elected official agencies and exempt agencies, a role can be assigned to users in the human resources department that allows them to approve positions for their agency. Agencies create the new positions as necessary, but cannot assign employees to the position until it is approved by OBM. Periodically, positions are reclassified in the system and require OBM to approve the reclassification, or require a personnel action form to be sent to DAS for approval. Vacant position reclassifications do not require OBM or DAS approval.

New positions are created at the agency level. The agency position specialists enter the proposed position into OAKS (1). When a position is created in OAKS, a unique position number is automatically generated to allow for tracking and approval of all positions. The agency then notifies OBM that a position has been submitted and, if the position is for a non-elected agency, requests approval. All requests for approval are submitted to a central repository at OBM. The requests are then distributed to the OBM budget analysts for review and approval. The budget analysts at OBM approve the position if all required information is present and if the position is within the personnel limits of the agency. OBM can also freeze the position if the required information was not submitted. Once the position is approved by OBM, the agency enters a budget for the position. Agencies may assign employees to a position before the budget is submitted to OBM (there is not an edit in place to require the agency to submit a budget first).

Beginning in the summer of 2008, OBM began using the SOPPS application (State of Ohio Payroll Projection System) to monitor the budgets and payroll spending. SOPPS pulls data from OAKS bi-weekly and can be used for forward projections as well as current monitoring and analysis. This system provides payroll projection reports for all agencies through the OBM website. Agency payroll projection reports can be downloaded from SOPPS into Microsoft Excel, which allows for sorting and filtering the report data to meet the agency’s budget needs.

During state fiscal year 2010, OBM analysts performed their HCM-related role in accordance with two OBM directives that were issued to state agencies during state fiscal year 2008:

- Memo issued by the Director on May 1, 2007 – Termination of the Temporary Hiring Control Process. This guidance enabled agencies to initiate and process personnel actions in the OAKS system without OBM involvement. In the HCM system at that time, positions that became vacant after OAKS HCM go-live remained approved in the HCM system. If an agency sought to fill a newly created permanent position, justification was required from OBM. In these cases, agencies were required to submit their requests to OBM prior to posting and filling positions.

- Memo issued by the Director on January 31, 2008 – Implementation of Hiring Control Process. This guidance increased OBM analyst involvement in the personnel action arena relative to the previous eight month period. With the exception of job codes that were explicitly exempt from the hiring controls process (e.g., specific classifications related to revenue generation, safety and security, or direct care in institutional settings) agencies were required to obtain approval by either the Governor's Office or OBM (depending on the type of position) prior to posting and filling a position.

Payroll can be submitted for employees who are assigned to positions where the budget exceeds the approved budget or where a budget has not been assigned. When the payroll file is sent from HCM to FIN for payment, all transactions (combined into journal IDs) must go through an edit check, then a budget check. If the journal ID fails budget check, an error report is then generated in FIN and the agencies must log on to FIN to address the errors. Agencies then have two options: they must either adjust their budget so that the lines in error contained within their journal ID are within their budget, or move the journal ID lines to chartfields where funding is available. Journal IDs with less than 30 lines of error are corrected directly in FIN. If a journal ID has more than 30 lines of error, the original journal ID starting with a "P" must be deleted. A new journal ID that starts with a "C" (correction) is created in FIN to replace the deleted journal ID. The correction journal ID must have the same total expense amount as the original journal ID, although the total debit and credit amounts may differ from the original journal ID. The journal will also likely have different fund, account, or ALI allocations. Personnel from OBM monitor these errors to make sure agencies address the errors and follow up with agencies that do not address errors in a timely manner.

Each position requires a valid effective date. The employee personal data effective date must be on or before the effective date the employee is hired into a position or assigned a work schedule. The system also produces a warning message if the effective hire date is more than 30 days in the past or future. When a new position is created, there must be a valid beginning date that is before the date the employee is assigned to the position. OAKS also has edit checks to assure the effective date entered is a valid date.

Positions must be assigned one or more combo codes, each of which indicates the account to be charged for various payroll expenditures (earnings, deductions, taxes, etc). The combo code distribution percentage for a position must equal exactly 100%. Employees may be assigned to one or more combo codes. The combo codes are essentially fund codes used for payment allocations.

Row-level security prohibits agencies from using a combo code that belongs to another agency. A drop down box allows only the authorized combo codes to be available to the user. Combo codes are assigned to employees based on their agency. An agency is not able to view the combo codes for other agencies.

Workforce Administration

The *Workforce Administration menus* allow a user to maintain information about employees, maintain information about a person tied to a specific job record, and administer workforce agreements, layoffs, recalls, and disciplinary actions. The menus in Workforce Administration are *Personal Information*, *Job Information*, and *Labor Administration*.

A Personnel Action (PA) request form is used to document any activity significantly affecting an employee in state service, including hires, reassignments and transfers, promotions, demotions, terminations, and leaves. The PA is used as a paper trail for an adjustment in payroll records to help ensure appropriate compensation for services performed. PA forms are completed manually, so the system does not require a PA for a change.

Regardless of whether an agency interfaces payroll data or enters payroll directly into OAKS, all agencies must directly enter position and employee additions and modifications directly into OAKS (1 & 2). For self-serving agencies (agencies that enter time and labor directly into OAKS) using work schedules, the only time a transaction is entered is when the employee takes leave or works overtime. Self-service employees enter requests for leave (RFL) directly in OAKS, and the hours on their timesheet are calculated accordingly.

HCM's Time and labor function has edits in place to detect errors in the payroll timesheets submitted by the agencies. The Time Admin process applies business rules to reportable time submitted and determines exceptions (12). Agencies must review the Manage Exceptions Page (13, 14) and resolve all exceptions before the reportable time is converted to payable time and a pay sheet can be subsequently created (15, 16).

Online edit checks require the data fields Name, Organizational Relationship, Address, DOB, and SSN on the personal information page and the data fields Permanent / Temporary Indicator / Title / Company, Classification Indicator, Department, Job Code, Appointment Type/Bargaining Unit Flag, Retirement Plan (Empl Class), Officer Code, Paygroup, Rate Code, Benefits Enrollment, and Compensation on the job information page be entered before an employee record is accepted (1 & 2). Edit checks exist when entering a new position or a new employee for an existing employee for a payroll cycle. Each screen within OAKS has specific fields that require data to be entered before the record can be added or updated.

Online edit checks, including formatting and logic checks, are also used to verify that employee and position data entered is accurately recorded during payroll processing. Error messages are displayed for erroneous data, and further processing is prohibited until the errors are resolved. OAKS has edit checks in place to assure valid information is entered into fields within payroll. In addition, many screens offer pull-down menus or the option to click a magnifying glass and view the available options for the particular field and for the agency.

Only authorized personnel have access to the corrections roles that allow the updating of historical data for approved positions, pay rates, and benefits data in OAKS. There are 14 corrections roles available for benefits, payroll, time and labor, and human resources, and security functions within OAKS. The roles allow corrections to standing data in the system, such as employee and job information. The roles are mainly assigned to DAS employees.

Personnel Information

The *Personnel Information menus* allow users to add or modify information related to an employee and create personnel and organizational relationships.

When they are first entered into OAKS (2), each employee (with SSN) is automatically assigned a unique employee ID to allow for tracking and monitoring of the employee status. Online edit checks are used to prevent an SSN from receiving duplicate employee IDs. The National ID (SSN) field is required to add an employee. The SSN entered is compared to the employee master file to determine whether the SSN already exists in OAKS. If the SSN does exist, the employee ID assigned to that SSN will be displayed along with an error. If the employee was previously employed with the State of Ohio, they will have an SSN and employee ID in the system, and the employee record is re-activated rather than assigning a new employee ID (e.g. the employee ID stays with an employee forever). The SSN field also has validations that prevent all 0's, all 1's, letters, etc. to help assure the SSNs entered meet Social Security Administration (SSA) standards; however, OAKS currently does not validate SSNs against any data from the SSA to assure the number is a current, valid SSN for the employee. Employees can be created and temporarily accepted with an SSN of 999-99-9999. This is typically used if the SSN is not immediately known for a new employee; however, the employee cannot be hired into a specific position until a valid SSN is entered. There is no field available to manually assign an employee a specific employee ID.

Job Information

The *Job Information menus* in HCM allow users to hire employees into positions, including permanent and temporary positions. Each new job position is automatically assigned a unique number to allow for tracking and approval of the position. Additionally, users can add additional employment instances for employees with more than one position assigned.

New hires are added by the agency HR specialists at each agency. All required fields must be entered before the record can be saved. OAKS automatically assigns the employee an eight digit random Employee ID number (employee IDs are used to identify employees in OAKS rather than SSN). The employee also must be assigned to one or more combo codes. Combo Codes, which were called RefNos before OAKS, associate reported time, earnings, deductions, or taxes with their respective financial accounts (2). OAKS will only display the Combo Codes available to the time reporter being processed.

Each user is limited to only one pay group, which determines the frequency and timing of payroll processing for the user. Once a pay group has been submitted and confirmed, the group cannot be reprocessed. When employees are assigned to a pay group, they may be assigned to a bi-weekly current, bi-weekly delayed, or monthly pay group. Bi-weekly delayed groups are further split out into additional groups based on the employee's last name. The pay group will determine when the employee gets paid. The employee's pay group should not change, even if their name changes. However, their pay group will change if the employee changes from biweekly delayed to monthly.

Labor Administration

The *Labor Administration menus* in HCM allow users to enter and review information related to layoffs and recalls, disciplinary actions, grievances, and job changes. In addition, users may generate reports related to labor administration data.

Benefits Administration

When employees are assigned to a position in HCM, they must also be assigned to one or more benefit plans. Benefit plans are set up by the OAKS configuration team and include:

- Personal Leave. (19 different plans)
- Sick Leave. (10 different plans)
- Vacation Leave. (99 different plans)
- Cost Savings Plan. (1 plan)
- Disability. (3 types, with a total of 10 different plans)
- Old Sick Leave. (2 plans – holding plan only, no leave is accrued to this plan)
- Firefighter Holiday Leave. (1 plan)

Different benefit plans are set up based on varying levels of service, as well as to accommodate union contracts and specific agency leave plans that differ from the standard statewide plans. Access to create and modify the benefit plans is restricted to the configuration team. Users must be assigned either the OH_BN_CONFIGURATOR or OH_BN_OAKS_ADMINISTRATOR roles in order to create and modify the benefit plans.

Within each benefit plan, the options can be customized to suit the needs of the plan. For example, a general vacation leave plan for an employee with less than five years of service can be set up so that the employee accrues 3.1 hours of VL each pay period. A personal leave plan can be set up so that each year in the first week of December, the employee accrues 32 hours. Plans can be assigned different options, depending on the type of plan:

- Effective date.
- Accrual Process Date.
- Plan Year Start.
- Accrual Calculation characteristics, including:
  - Service Units.
  - Accrual Rate Units.
  - Award Frequency.

- Automatic Accrual Processing limits, including:
  - Maximum Leave Balance.
  - Maximum Leave Carryover.
  - Maximum Plan Year Accrual.
  - Maximum Pay Period Accrual.
- Manual Accrual Processing Options, including:
  - Pay in Lieu of Time Off.
  - Pay at Termination (and %).
  - Allow Negative Balance (and maximum negative allowed).

Payroll Processing

The payroll process is a collaborative process between agencies and the Human Resources Division (HRD) of the Ohio Department of Administrative Services (DAS). Agencies submit time and exceptions while DAS HRD finalizes the payroll process. There are two options for entering time into OAKS: electronically interfacing with OAKS or entering information online directly into OAKS. The interface option allows agencies to keep their existing timekeeping system. Interfacing agencies use an automated tool that allows an agency's existing timekeeping system to automatically send information to OAKS. Non-interfacing agencies use the OAKS timesheet to report time. Once the online timesheet data or interfaced timesheet data reach Time and Labor (8), the payroll process is the same for both interfacing and non-interfacing agencies.

Report Time - Time and Labor Self-Service (3-4)

A pilot program of Time and Labor Self-Service (T&L SS) began in January 2008. The pilot program began with DAS, and there are currently 34 agencies participating in T&L SS. Although some agencies will be moving away from using their agency timekeeping systems, there are nine agencies (AUD, CSR, EDU, ELC, JCR, JLE, LSC, REP, and SEN) that have opted out of participating in the T&L SS program. This feature provides the ability for employees at non-interfacing agencies to utilize work schedules, and only requires system entry when the employee takes leave or works overtime. T&L SS allows for direct supervisor approval, including displays of total hours, overtime and absences, as well as employee review of balances.

For agencies that use T&L SS, employees are automatically assigned to a 40 hour per week work schedule (3) with five eight hour days. Employees submit an online request for leave (RFL) or overtime request in HCM (4). Their supervisor receives an automated e-mail the next day to inform them that there is a leave request or overtime request awaiting approval. Once the supervisor approves the RFL, the employee's regular hours on the timesheet are automatically reduced by the number of leave hours approved. In addition, the employee's leave balance is shown as reduced once the leave is approved, even if the leave is for a future date. If an RFL is deleted, the employee's leave balance will be updated accordingly to add the leave back in.

T&L SS uses a Reports-To structure that allows supervisors to see and approve timesheets of their direct subordinates, as well as their subordinates' employees. Each agency using T&L SS set up a Departmental Tree that defines the reporting structure for their agency.

Report Time – Online (5)

Non-interfacing agencies use the OAKS Timesheet to report employee time. They may assign work schedules to full-time employees on an employee-by-employee basis. The employee's time is automatically reported based on his or her assigned work schedule, and any exceptions to work schedules are entered on the OAKS Timesheet (5). OAKS has online edits that prohibit entering hours into a timesheet for an individual that is not an active state employee in HCM.

Report Time – Interface (6)

Interfacing agencies track time using their current timekeeping system (4) and send it to OAKS through the Time and Labor interface (9). They do not use work schedules in OAKS, so employees are paid according to time entered into the agency timekeeping system and sent to OAKS via the interface. Interfacing agencies send all time, including exceptions, through the interface (7 & 8). There is currently no requirement or deadline for interfacing agencies to abandon their current payroll systems and exclusively use OAKS to enter payroll. The following were interfacing agencies as of the beginning of FY10:

1. Attorney General.
2. Auditor of State.
3. Bureau of Workers Compensation.
4. Department of Education.
5. Department of Mental Health.
6. Department of Public Safety.
7. Department of Transportation.
8. Department of Youth Services.
9. Dept of Mental Retardation.
10. Dept Rehabilitation and Corrections.
11. Environmental Protection Agency.
12. Job and Family Services.
13. Medical Board.
14. Ohio Lottery Commission.
15. Veterans Home.

Report Time Processing

All agency timekeeper specialists collect time data from their employees. For non-interfacing agencies, the timekeeper specialists enter work schedule exceptions and time using the Timesheet in OAKS. For interfacing agencies, the time and labor interface coordinators send the time and exceptions to OAKS through the interface and the central time and labor specialist at DAS loads the information into the OAKS Timesheet.

There are two types of time reporters in OAKS: Positive Time Reporters and Exception Time Reporters.

Positive time reporters do not have predefined schedules in OAKS and are only paid for time entered. Positive time reporters include time reporters from interfacing agencies and seasonal, intermittent, and some part-time time reporters from non-interfacing agencies.

Exception time reporters have predefined schedules in OAKS and only need to have their time exceptions (e.g. sick leave, vacation, etc.) entered on the OAKS timesheet. Exception time reporters include full-time and some part-time time reporters in non-interfacing agencies.

Agencies may assign their time reporters to "work schedules," whereby OAKS automatically enters the time reporters' work hours in OAKS according to the appropriate work schedule (e.g. 8 hours a day, M-F). If an employee is assigned a work schedule, manual time entry is only required if the employee has an exception to their payroll, such as leave or overtime.

In OAKS, every employee's time is eventually recorded on an electronic timesheet regardless of whether or not their agency is an interfacing or non-interfacing agency. OAKS timesheets automatically report time for employees with work schedules, and report time with more detail, such as the number of hours worked each day for the pay period.

The payroll processing menus allow users to review EFT errors, review payroll, and generate periodic reports containing payroll information for specific pay periods. The Payroll Register, Payroll Summary, and Deduction Register are available through the payroll processing menus.

Within the Manager Self Service menus, the user can manage schedules for employees, approve time and exceptions, and report and view time entered.

Time and Labor

During payroll processing, a nightly batch job is executed to run the Time Admin process (12), which applies delivered and custom business rules, determines exceptions (13), and converts reported and scheduled time into payable time. The process is run every day during processing week at noon and each night in batch. Agencies then have the ability to review any exceptions that posted during the processing (14). Payroll officers are locked out of the system at 7:00 P.M. on Thursday, so any corrections made by the agency must be completed by this time. The Time Admin process can also be run by DAS HRD at any time as needed.

The agency timekeeper specialist at each agency uses the Manage Exceptions page in OAKS to view errors and exceptions. For example, an employee could have submitted time worked but was inactive on the dates requested or an employee could not have available leave balances for the submitted leave time. If there are exceptions on the Manage Exceptions page, the agency timekeeper specialist is responsible for adjusting and resolving the errors. These adjustments will be re-run through the Time Admin process by DAS until the error is corrected.

After all exceptions have been resolved, some agencies require the payable time to be approved before the time is loaded into OAKS Payroll. All Time and Labor self-service agencies must approve payable time. The agency time and labor supervisor uses the Approve Payable Time page to approve payable time for employees. Once all time is approved (if applicable), the time gets loaded into OAKS Payroll. Time for interfacing agencies is considered approved when submitted by the agency (15).

OAKS HCM automatically calculates an employee's gross pay based on the employee's hourly rate and the hours submitted. The gross pay calculation is done automatically in the system. HCM uses the hourly rate from the employee's job information screens.

HCM has edits in place that prevent submitting leave hours that exceed an employee's balances, or hours that exceed 24 hours for one day. For non-interfacing agencies, if an employee attempts to submit leave that is greater than their available balance, an online error message appears and will not allow the leave to be saved. For interfacing agencies, if the leave submitted is greater than the balance, an error will be generated during the Time Admin process and the employee will not receive compensation for the day. For both interfacing and non-interfacing agencies, if an employee submits time that totals more than 24 hours for one day, an error will be generated when the Time Admin process runs. Employees who submit leave requests that exceed their balance will not be processed.

> For example, if an employee requests 8 hours of sick leave for Monday and 8 hours of sick leave for Tuesday, but the employee only has 10 hours of sick leave available, the leave for Monday will be accepted but the entire request for Tuesday will create an exception. The system will not process the 2 available hours, but will deny the entire request for Tuesday. After the Time Admin process has identified exceptions, it is the agency's responsibility to clear all exceptions before payroll is run, or the exceptions will not pay.

Leave balances for each employee are accumulated according to the benefit plan contained in OAKS and are updated with any leave taken during payroll processing. A history of leave accruals and balances is available in OAKS. Employee leave balances are accrued based on their years of service and the benefit plan in which they are enrolled. For example, employees who have less than five years of service accrue 3.1 hours of vacation each pay, while employees who have between five and ten years of service accrue 4.6 hours each pay. The leave plan is indicated on the employee record in OAKS. In addition, OAKS maintains the historical balances, as well as leave used and accrued. This historical information is not available to employees on their paycheck statement; however, payroll and benefits specialists at each agency may access this information.

Verification of Payroll

The approved payable time (15) is then loaded into the pay sheets (17) in OAKS Payroll. This is done as a central batch process (16). An additional recalculation batch job runs nightly and creates an error report for any payroll verification failures or errors (16).

The Confirm and Calculation process (21 & 22) is then run to finalize the payroll and run accruals, as well as assign check numbers. The final payroll is interfaced with OAKS Financials (FIN). On Monday, the payroll amounts and deductions are reconciled by the DAS/HRD management analyst supervisor. For each pay cycle, DAS/OAKS performs a reconciliation to confirm the payroll and deduction amounts in HCM payroll balance (25). Payroll runs are confirmed by the DAS payroll supervisor (22) prior to the final run.

The DAS payroll supervisor sends an e-mail (24) to the OAKS batch team to inform them the payroll has been reviewed and confirmed and is ready for processing. Checks are written by DAS Print Services (27). DAS Print Services sends an e-mail confirmation of warrants printed to the DAS/HRD management analyst supervisor (28).

Printing / Distribution / Validation of Payroll Processing

For each pay cycle, DAS/OAKS performs a final reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing. An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed (25). The DAS management analyst supervisor compares amounts produced in HCM to confirm payroll balances and also compares the payroll to the input to the FIN module to help ensure the two amounts agree. The management analyst supervisor also sends a confirmation to DAS printing, indicating the beginning and ending check number, payee, amount, and total of checks to help ensure all checks are printed.

Regular check numbers are automatically assigned during the Confirm Paycheck step (22).

OAKS HCM utilizes earnings beginning and ending dates when issuing paychecks to help prevent payments for the same earnings period and gross amount. Earnings on a paysheet must be associated with an earnings period. For regular checks, earnings periods are automatically created based on timesheet earnings dates. When manual checks are issued, the earnings period automatically populates with the current earnings period. If a manual check is being issued for a previous earnings period, the dates must be manually changed.

An outbound interface provides the total amount paid for each agency to ensure the amount paid equals the amount submitted. The agencies receive the employee master for internal reporting and load the data into their own systems (34).

The employee master file is kept as the official record of what was processed in payroll for the pay period and is used as the source file if payroll needs to be reprocessed. This master file is stored in EPM, and is created after the HCM data has been interfaced to FIN.

Manual Checks

Each off-cycle / manual check is automatically assigned a unique number, if the user does not manually enter a number. When entering information into OAKS to process a manual check, check numbers are automatically assigned for each payment unless they are manually entered by the user. Manual check numbers may be changed after they are saved. When this occurs, the check source is changed to "*****" to indicate the number was changed.

When a manual / off-cycle check is issued and recorded through OAKS, pay period end dates are automatically populated with the current pay period. Earnings beginning and end dates are required for all manual checks. Manual checks (31) are generally written when there are errors in the payroll data, but are also written for issues such as EFT failures and misplaced or destroyed checks. A Request for Off-Cycle Manual Paycheck form must be signed and approved by an authorized agency payroll representative and sent to DAS for all manual checks. The agency must provide DAS with a valid reason for manual check requests (30), then adjust time for errors, and clear any exceptions in OAKS. Manual checks are written by six payroll employees at DAS. The blank check stock is maintained by the business office in a safe at the Rhodes State Office Tower.

OAKS maintains a history of all manual and automated checks after they have been issued. The historical data can be queried in OAKS.

EPM (OAKS Data Warehouse)

In addition to the HCM production environment, OAKS also has a data warehouse known as the EPM (enterprise performance management). EPM is used by OAKS users for producing payroll and financial reports and retrieving read-only data for analysis. This data warehouse environment is created by formatting and extracting detail financial data from hundreds of FIN and HCM production tables and loading them on a nightly basis with a series of batch jobs into a non-real-time data warehouse. The majority of these nightly updates are incremental; however, depending on the requirements specified on the table, a full synchronization of the table may be performed daily. In addition, a total refresh of the data warehouse with production is performed weekly. History is maintained for data in the EPM.

Because the EPM tables are separated from production, one of the advantages of the EPM is the significant reduction in the time it takes to submit transactions or run reports. Only necessary transaction information is copied to the EPM; standing data that does not change often is not copied to the data warehouse. In addition to the OAKS EPM, the OAKS data warehouse environment also includes the HR legacy data warehouse and the financial legacy data warehouse (CAS Data Mart).

OAKS has a query available to identify the total records in HCM production for comparison to the total records in the EPM data warehouse. The query compares the record count of the original HCM tables to the record count of the EPM tables. The query is run on an ad-hoc basis and must be initiated manually. These queries are predominantly used as tools to research errors as opposed to monitoring the completeness of the data warehouse since it is fully restored from production each week. In addition, design documents and a CRM have been created to implement an automated job that will verify the records transferred to EPM successfully; however the CRM has not yet been approved.

Error reports are also generated during nightly processing if any errors occur during updating. An Incident Report is prepared and posted to the Sharepoint site, and an Alert is posted on the OAKS website. If the error is generated for a critical table, the error receives priority and is fixed right away. If the error is generated for a table that is not frequently used, the error will be corrected and updated in the next batch window.

OAKS System Issues and Alerts

DAS makes available a weekly newsletter that contains communications relevant to OAKS and instructions for addressing system issues and agency errors that arose because of incorrect data entry or use of the OAKS system. The weekly updates are available through the DAS web site.

Additionally, a list of current OAKS alerts is available on the OAKS web site. OAKS alerts announce various system modifications, enhancements and outages, new job aid postings, OAKS system availability, and other helpful information suggested by members of the OAKS program management office (PMO). In addition to being posted on the OAKS website, these items are e-mailed to Agency Liaisons and agency leadership as appropriate. The web page (http://www.oakspmo.ohio.gov/oaks/Oaks_Alerts.asp) includes a weekly OAKS alerts summary, previous issues, and a list of all OAKS issues to date.

The HCM-related alerts issued during the audit period can be classified into the following categories:

- Availability of HCM data in EPM.
- Time and Labor Self Service Module.
- Batch Processing and Payroll Processing.
- Security access (passwords)

- ePay.
- Wage Progression.
- HCM Query and Reporting Tools.
- Helpdesk and customer service.

FINANCIAL APPLICATION CONTROLS FOR OAKS WARRANT WRITING

OVERVIEW OF ORGANIZATION

The OAKS application processes warrants and EFTs for the majority of agencies, boards, commissions, and related organizations within the three branches of state government. It also processes warrants and EFTs for state universities and state community colleges. The specific types of warrants and EFTs processed are as follows:

- State payroll.
- Maintenance and EDI payments (payments to vendors).
- Income tax refunds.
- Medicaid payments.
- TANF payments.
- Dependent care and aid to dependent children.

Although the Office of Budget and Management (OBM) is responsible for ensuring warrants are processed accurately, the Department of Administrative Services (DAS) is responsible for the actual printing and distributing of the warrants.

The Office of Budget and Management (OBM) is a cabinet-level agency within the executive branch of the Ohio state government. The mission of OBM is to provide financial management and policy analysis to help ensure the responsible use of state resources. In fulfilling its mission, OBM coordinates, develops, and monitors agency operating and capital budgets, and reviews, processes, and reports financial transactions made by state agencies.

DAS is committed to providing quality centralized services, specialized support, and innovative solutions to state agencies, boards, and commissions as well as local governments and state universities. DAS has more than 30 program areas serving Ohio government customers who, in turn, directly serve the interests of Ohio citizens. DAS helps procure goods and services, deliver mail, recruit and train personnel, promote equal access to the state workforce, oversee state construction projects, lease and manage office space, process payroll, print publications, and perform a variety of other services. To provide these services, DAS is organized into four divisions: Equal Opportunity, Human Resources, Office of Collective Bargaining, and General Services.

DAS's General Services Division Office of State Printing and Mail Services is responsible for the printing and distributing of warrants/EFT remittances that are processed through OAKS. The Office of State Printing and Mail Services is under the control of the Deputy Director of General Services, who reports to the Director of DAS. The Office of State Printing and Mail Services consists of approximately 13 people in the printing department and approximately 25 in the fulfillment/mailing department and they provide the following services:

- Print, cut, and insert warrants/EFT remittances.
- Distribute warrants to recipients and other agencies.

The Office of State Printing and Mail Services is limited to printing and distributing of the various state agency's warrants/EFT remittances. The agencies or departments are responsible for authorization and initiation of all transactions. Management reinforces this segregation of duties by restricting logical and physical employee access to all user data. OAKS warrant file datasets on the OIT mainframe are RACF protected from unauthorized access. Once the OAKS warrant files are sent via FTP to the OIT IBM mainframe, they are logically restricted from any modifications to the warrants/EFT remittances. READ access to the warrant files is restricted to authorized DAS Office of State Printing and Mail Services personnel.

During the FY10 audit period, the Office of State Printing and Mail Services printed and distributed:

- 39,817 HCM Payroll Warrants.
- 229,477 HCM Payroll EFT Remittances.
- 2,212,293 FIN Warrants
- 1,744,584 Ohio Income Tax Returns.

WARRANT PRINTING

OAKS Financials (FIN) Submittal

A process is in place to notify the DAS mainframe print center when an OAKS FIN warrant file is ready to be printed to help ensure all warrants are printed and recorded. The DAS mainframe print center is notified via an automated e-mail process when an OAKS FIN warrant file is ready to be printed. The file, in line data record format when it is output from FIN, is then converted using Advanced Function Printing (AFP) resources to produce the final warrant file.

The Office of State Printing and Mail Services programmer specialist* must then access the mainframe's TSO environment using a unique user ID and password. The programmer specialist will select the dataset for editing. There are two different types of print jobs: CUT for RTA (Return to Agency) cutsheet submissions, and ROLL for files that are to be printed and given to the Fulfillment area for inserting and mailing. The OAKS Financials Report Log is reviewed prior to submitting a print job, and updated subsequent to each print job by print center employees to avoid duplicate print runs. The programmer specialist will edit the dataset name to match the number next in line after the last printed job run number, which should also match the job run number from the original e-mail. * Note: The computer operator supervisor 1, computer operator manager 1, and computer operator manager 3 may also perform the functions of the programmer specialist.

Next, the programmer specialist submits the job to the printer where it will be processed. When the job is printed, the warrants will be printed with Print Sequence Numbers (PSNs) as an added control to ensure completeness of the FIN warrants printed. All issued warrants are accounted for and uniquely identified during the warrant writing process. This is accomplished via the use of job IDs for print runs, print sequence numbers for each FIN print run, and warrant numbers for each warrant issued.

OAKS Payroll (HCM) Submittal

Control totals and other reconciling information are confirmed by Print Center staff to provide for completeness and accuracy prior to OAKS payroll warrant payment files being processed in the print queue. When an OAKS payroll warrant file is ready to be printed, HCM Support Staff will ftp the warrant file as an Adobe Acrobat file (PDF) to the DAS Mainframe Print Center for conversion to AFP format and placement on the print queue. The Support Staff will also send an e-mail that contains the following information for reconciliation purposes: the name of the payee on the first and last warrant, the pay amount of the first and last warrant, the warrant number of the first and last warrant, and the count of the warrants on the file.

The Mainframe Print Center computer operator will then manipulate the AFP job on the mainframe print queue to send it to the printer.

There are four different HCM payroll files that are printed: Biweekly Delayed, Biweekly Current, Current Monthly, and Monthly Advanced. There is an additional advice file, which includes the HCM EFT remittances.

Printing

The printer is inspected for proper setup before a production job is performed. As the warrants print, the operator will visually inspect the warrants. After printing is complete, a sample warrant is checked to ensure the warrant numbers were placed in the correct boxes. The MICR gauge will also determine whether the magnetic ink is legible and acceptable. In addition, a clear plastic viewer is used to ensure the MICR line at the bottom of the warrant is properly aligned to permit scan reading.

The following key warrant information is recorded on the OAKS Check Log:

- Start and stop check sequence numbers.
- Void/good total count of checks written.
- Reason for void/good determination.
- Operator initials for the beginning voided warrants.
- The acceptable warrants.
- The ending voided warrants.

OAKS check stock is compared to actual printed warrants each time OAKS warrants are printed via the updated and signed OAKS check log. The OAKS Check Log is maintained near the cutsheet printers.

If a mechanical problem occurs during printing of an OAKS print job, it is necessary to stop the job and remove the damaged documents. When re-setting the print job, both the damaged warrants and also some acceptable/undamaged warrants may be printed. Procedures and controls are in place to control these duplicate printed warrants. Any duplicates that printed in the start-up must be recorded on the OAKS Check Log, marked void, verified by the supervisor, and placed in the voided document box in the locked print center cage.

Post-Printing Confirmation

Post-printing confirmation information is communicated to OAKS FIN/HCM support staff by the Office of State Printing and Mail Services for the purpose of reconciliation and validation of print jobs. The e-mail contains information from the first and last warrants (name on warrants, pay amounts, and warrant numbers), the count of warrants on the file, and the number of warrant stock voided out for the setup purposes. A copy of this e-mail is enclosed in the lock box of warrants picked up by the delivery driver.

Fulfillment (Cutting/Stuffing/Mailing)

Fulfilment is the next step after the warrants have been printed. All roll file warrants are transported from the Print section to the Fulfillment area where they are stuffed into envelopes and placed in mail trays to be sorted and mailed. DAS Fulfillment Service Job Logs are completed and used by DAS management to account for the disposition of warrants during transport from the Print section to the Fulfillment area for stuffing into envelopes.

Once the OAKS roll file warrants have been printed, stuffed, and placed in mail trays, Courier Pick Up Slips, accounting for all warrants taken for mailing and distribution, are completed and approved by DAS and the courier. The courier will pick up the mail and inspect the Pick Up Slip for accuracy and have DAS initial the Pick Up Slip to signify they have verified accuracy of the mail to be taken. The mail is then taken to the courier mail facility to be sorted and verified by a United States Postal Service (USPS) clerk for subsequent mailing to the recipients.

Warrants marked as “Return To Agency” (RTA) are not forwarded to the Fulfillment area for stuffing and mailing. The RTA cut sheet warrants are placed in a lock box to be returned by courier to the agencies.

DAS Mainframe Print Center management maintains formal instructions relating to check printing and documentation. The instructions include: submitting a job for print, preparing printer for jobs, warrant delivery procedures, void handling procedures, and RTA review procedures.

Voids

Voided checks can occur in two ways. They can be the result of printer errors or other problems that occur during the printing process or can be the result of damage that occurs after the printed warrants have been transferred to the Fulfillment section. Voided warrants for each of these scenarios are handled differently.

Print Process Voids

When check stock has to be voided during the printing process, voids are stamped and accounted for by the Print Center Manager, and stored in a secure location until destruction. These voids all are marked by a void stamp or printer, listed on the OAKS Check Log, and stored in a locked cage at the print facility until they are shredded. Daily, the mainframe print center manager will compare the voided checks to the Check Log. If there are no missing voids, the log sheet will reflect this with the manager’s approval. Print center voids are shredded on the third Friday of every month by the print center manager and an OBM representative. A log of all shredded documents is maintained and signed by both DAS and OBM.

Fulfillment Voids

If warrants are damaged during the fulfillment process, they are put aside until the job is completed. All printed warrants voided by the fulfillment section are properly accounted for and returned to OBM in a secure manner. The warrants are placed in a blue bag and given to the print center manager to be placed in the lock box with the RTAs to be returned to OBM. The voided warrants are then returned to OBM with the RTA warrants via the lock box process.

The Fulfillment manager is responsible for notifying the OAKS FIN/HCM Support Staff that the checks will need to be reprinted. OAKS HCM staff will either re-issue the checks on a later run or Payroll has a desk top printer where the checks can be reprinted.

Lock Box

All RTA (return to agency) warrants are placed in a lock box and stored in a locked cage of the print facility until a courier picks them up and returns them to OBM. Access to all the voided and Return to Agency (RTA) warrants before they are destroyed or returned to OBM is restricted to authorized DAS mainframe print center management. A copy of the OAKS Warrant Delivery Log Sheet, which documents the warrant numbers of included checks, is secured.

Warrant Delivery Logs are signed and dated by both the OBM delivery representative and the OBM recipient representative confirming the integrity of the lock box security and agreement between the delivery log and actual contents of the lock box. RTA warrants along with the completed and approved OAKS Warrant Delivery Log are picked up daily from the print facility and couriered directly to OBM via a secured lock box. The Office of State Printing and Mailing and OBM both have a key to the lock box. In addition, a wire lock contains a number that must correspond with the paperwork inside the lock box. The wire lock is used to help ensure the box is not opened when being transported by carrier between the print center and OBM. When OBM receives the container, they will cut the disposable lock and inventory the warrants to ensure they match to the Delivery Log. If everything matches, OBM will sign the inventory sheet, put the Delivery Log and inventory sheet back in the container, and lock the key lock on the box. The locked container is then returned to the Office of State Printing and Mailing where the Logs are then stored.

Physical Security

The Office of State Printing and Mail Services uses the print facility to print and distribute all OAKS warrants. The facility is monitored via 12 separate security cameras throughout the property. The security cameras are monitored 24 hours a day 7 days a week in the Office of State Printing and Mail Services' office and also by the DAS General Services Division security unit.

Access to the print facility where all the OAKS warrants and state checks are stored, printed, and processed, is restricted to authorized DAS Office of State Printing and Mail Services personnel. The print facility is physically protected from unauthorized external access to the building by securing the doors and gated entrances. Card reader security is installed at the two main entrances on the front side of the building. The remaining four doors are emergency exits and are dead bolted from the inside.

Logical IT Security

The Office of State Printing and Mail Services has its own LAN at the print facility. The LAN uses unique user IDs and passwords and allows basic access to network resources. The door to the room that houses all the hardware and devices for the LAN at the print facility is secured.

In order to submit the FIN OAKS warrant file for printing, programmer specialists need logical access to OIT's mainframe. The three OAKS warrant files that are downloaded for print processing are defined by RACF security because they are housed on the mainframe.

For more information on the security of the mainframe and firewall, see the IT Security control objectives in Section II and III of this report.

Blank Check Inventory

The blank check stock inventory is maintained by the mainframe print center manager using an inventory listing sheet.

The blank check stock inventory is received in boxes of cut sheet warrants containing five shrink wrapped bundles of 500 warrants per box.

When the manager receives the blank cut sheet stock, he records the skid number, start and end check stock numbers, quantity of checks on each skid, the number of boxes in each skid, and the shipment date on the inventory listing. The mainframe print center manager completes a sight inspection of the inventory about once every two weeks.

The blank check stock is stored in a physically and environmentally secured warehouse room of the print facility. There are millions of blank warrants in inventory. The warehouse room has three internal doors: one from the fulfillment section, one from printing, and one from the ODJFS printing room. The warehouse room also has four loading docks that are gated and have padlocks. There is also a security camera covering the inventory at all times.

FINANCIAL APPLICATION CONTROLS FOR EFT PROCESSING

OVERVIEW OF ORGANIZATION

The Office of Budget and Management (OBM) is responsible for paying the State of Ohio’s obligations via electronic fund transfers (EFTs).

OBM processes EFTs for the majority of agencies, boards, commissions, and related organizations, within the three branches of state government. It also processes EFTs for state universities and state community colleges. The specific types of EFTs processed are as follows:

- State payroll.
- Maintenance and EDI payments (payments to vendors).
- Income tax refunds.
- Medicaid payments.
- Welfare payments.
- Dependent care and aid to dependent children.
- HEAP vouchers (state aid for heating bills).

The Appropriations Control and Cash Reconciliation section prepares and maintains appropriation dollar amounts in the accounting system and reconciles agency appropriations and expenditures to ensure the accuracy and integrity of the information in the accounting system. Monthly cash balance reconciliations are made with the Treasurer of State's (TOS) office and accounting records are reconciled to the ’s EFT and warrant writing activities.

The Payment Issuance Team consists of three employees who provide the following services:

- Process EFTs.
- Distribute warrants to other agencies (RTA warrants held by OBM to be returned to agencies for mailing).
- Manage the EFT process with the designated banks.
- Process warrant rewrites, cancellations, and stops.
- Process EFT applications, rejections, and cancellations.
- Process EFT applications at OSS.
- Process Medicaid EFT applications.
- Perform reconciliation of outstanding and voided warrants.
- Perform bank reconciliations for EFT transactions.

The Payment Issuance Team is limited to processing the various state agencies’ transactions and processing the related data. The agencies or departments are responsible for authorization and initiation of all their own transactions. OBM management reinforces this segregation of duties as a part of its new employees' orientation process, through on-the-job training, and by restricting employee access to user data. Changes to user data are never made by OBM. If an e-file does not balance, it is returned to the agency to be corrected and resubmitted.

Transmitting to Bank

As of November 2008, OBM transmits all EFT payments, including bi-weekly payroll, through Key Bank.

Vendor Information

Vendors that are paid by EFT are required to complete and sign a direct deposit authorization form. The banking information is entered at OBM OSS.

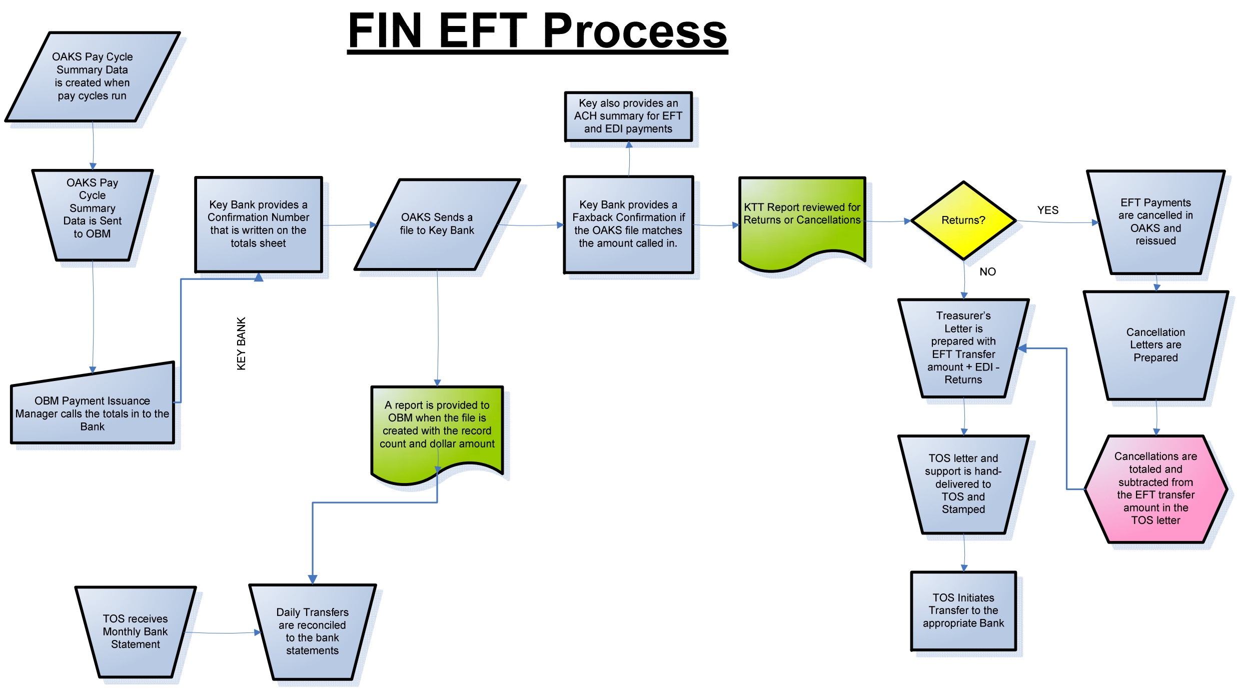
New or modified OAKS vendor EFT information is sent directly to OSS on an Authorization Agreement for Direct Deposit of State Warrants form. OSS enters the vendor information, including vendor ID (or employee ID), bank account and routing number, and account type into the OAKS FIN Vendor Database. The forms are maintained at OSS. EFT authorization and change forms must be accompanied by an original cancelled check. As of September 2009, the OSS does accept fax or e-mail copies. The vendor name and address must match the name and address on file for the vendor, or the OSS will not add or change the EFT information and a letter will be sent to the vendor detailing the missing information.

Beginning in FY10, vendor changes were entered by the OBM Office of Shared Services (OSS).

When a vendor is set up in OAKS, the default payment type under the “Location” tab of the vendor information screens is set to “Check.” Once EFT information is received, the default payment type is changed to EFT. The bank name, routing number, account number, and account type are entered into the vendor payables options screen. OBM checks the “Pre-Notification Required” box on the EFT options section and selects “Payment Only” in the transaction handling section to automatically place a seven-day waiting period on paying the vendor via EFT. When the next pay cycle is run, the routing and account numbers are automatically validated with the bank and the vendor is paid by check. If the information is not valid, an error is received on the Key Total Treasurer (KTT) report; if the information is valid, the vendor will be paid by EFT the next time a payment is submitted.

OAKS has an edit in place to prohibit the submission of an EFT voucher for a vendor without EFT information in the FIN system. If an agency attempts to submit a voucher with a location type of EFT but there is no EFT information entered in the system, the payment will automatically default to a warrant during processing.

FIN EFT Processing Flowchart


FIN EFT Process
OAKS Pay Cycle Summary Data is created when pay cycles run
OAKS Pay Cycle Summary Data is Sent to OBM
OBM Payment Issuance Manager calls the totals in to the Bank
KEY BANK
Key Bank provides a Confirmation Number that is written on the totals sheet
OAKS Sends a file to Key Bank
A report is provided to OBM when the file is created with the record count and dollar amount
Key also provides an ACH summary for EFT and EDI payments
Key Bank provides a Faxback Confirmation if the OAKS file matches the amount called in.
KTT Report reviewed for Returns or Cancellations
Returns?
YES
NO
EFT Payments are cancelled in OAKS and reissued
Cancellation Letters are Prepared
Cancellations are totaled and subtracted from the EFT transfer amount in the TOS letter
Treasurer's Letter is prepared with EFT Transfer amount + EDI - Returns
TOS letter and support is hand-delivered to TOS and Stamped
TOS Initiates Transfer to the appropriate Bank
TOS receives Monthly Bank Statement
Daily Transfers are reconciled to the bank statements

The above flowchart summarizes the FIN EFT process from the time OAKS sends the payment data to OBM through the TOS transfer of funds to the banks for payment. First, OBM receives the dollar amount of the EFT files each day from OAKS and confirms the amount with the respective banks. The amount is compared to the amount of the file created and sent to the bank by the OAKS batch team. Daily, the Pay Cycle Summary Data for the pay date is sent via e-mail from the OBM to the Payment Issuance Team. The Pay Cycle Summary Data is automatically forwarded from OAKS to the OBM Payment Issuance Team. The Pay Cycle Data includes vendor payments, employee expense reimbursements, Medicaid payments, and income taxes. The e-mail from OAKS alerts OBM that an EFT pay cycle run is ready to be processed. The e-mail is separated by pay cycle type (for example, CRIS-E JFS benefits, Key Bank EFT payments Regular, Regular US Mail Pay Cycle, ISTVs, TRBK, and Return to Agency Pay Cycle). For each cycle, the notification contains the Bank, Bank Account, Payment Method (CHK, EFT, or ACH), Currency, Number of Scheduled Payments, Paid Amount, Gross Paid Amount, Discount, and Late Charge. Each summary also contains a total of all payment methods for each pay cycle.

The Payment Issuance Manager then reviews the notification for EFT payments going to Key Bank and calls the bank to enter the total EFT amounts. Key Bank provides a confirmation number for the payment summary sheet. Next, the OAKS Batch Team sends a file to the bank for each pay cycle. A report is generated when the file is created that details the file name, line count, and the total file amount. If the amount submitted by the Payment Issuance manager over the phone matches the amount of the file, Key Bank will provide a faxback confirmation to OBM that contains the confirmation number, the total amount entered, and states that the amounts agree. Key Bank will also fax back an error report if the totals do not match. The error report states that the amount called in differs from the amount of the file received and requests OBM to call the bank immediately to resolve the difference.

DAS obtains the EDI interface file from OAKS and FTPs (sends via file transfer protocol) the file to the bank to identify the correct payees. Key Bank provides OBM a separate ACH Activity Summary for EDI and EFT payments that contain the original debit amount, plus or minus any adjustments, and the total amount to be debited/credited to the state's bank account each day.

TOS EFT Letter

After the dollar amounts of the EFT files have been reconciled between the OAKS file and the bank, OBM prepares and delivers a letter to the Treasurer of State's office requesting the funds be transferred to the appropriate accounts for subsequent payment. The Treasurer's letter reflects any returns or cancellations for the current period. OBM uses a report generated by OAKS that includes the bank, account (Maintenance, Tax, Medicaid, etc), sequence number, cancelled by, ACH amount, EFT amount, and the total amount. After the dollar amounts of the EFT files have been reconciled between the OAKS file and the bank, and after pay cycles are complete, a report is generated by OBM staff and sent by e-mail to the TOS office to transfer funds to Key Bank for the four accounts held at Key which are owned by TOS. A copy of the Pay Cycle Summary Data, any confirmations received from the bank, and any support documentation for returns are attached to the letter.

The Payment Issuance Manager hand-delivers three copies of the TOS EFT letter to the Treasurer of State's office and obtains a stamp with the received date and time on each copy. One copy is left with the TOS, one copy is sent to OBM, and one copy is maintained with the Payment Issuance Manager in a folder of all daily EFT activity.

Returns / Cancellations

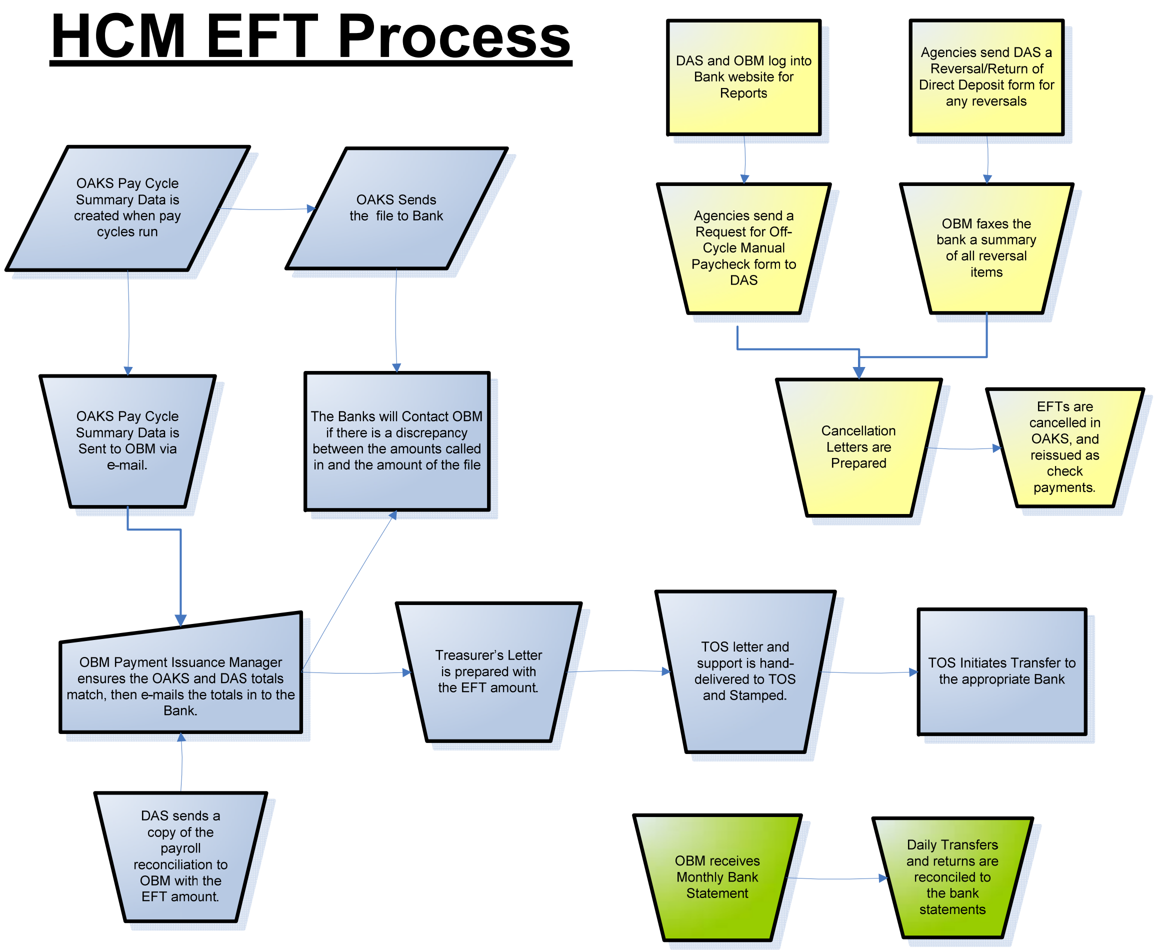
Key Bank sends a daily report to OBM called the Key Total Treasurer (KTT) report. The report contains the detail of all EFTs that were not fully processed during the last processing cycle and the reason for the cancellation. OBM receives this KTT report on a daily basis from Key bank and the money is swept back into the account automatically. EFT returns are cancelled in OAKS and supporting documentation is provided to the Treasurer's office. Periodically, EFT payments do not process completely because the account was closed or the account information was invalid. There is at least a one-day lag time for returns.

OBM notifies the appropriate agency of the error and waits for the agency to send a Warrant Cancellation or Erroneous EFT Transmittal form to authorize the cancellation. Once the cancellation authorization is received, the Payment Issuance Team cancels the EFT payment, enters a Cancel Action (i.e. reissue, put on hold, close liability), and enters a description of why the EFT failed.

OBM prepares a separate cancellation letter, which contains the EFT amount and fund. The payment cancellation screen in OAKS is printed and maintained with a screen print of the payment being reissued (if applicable). The warrant re-issue is marked as RTA, and the agencies receive a copy of the TOS cancellation letter attached to the RTA warrant.

The OBM Payment Issuance Manager writes the total amount of the returns processed for the day on the Pay Cycle Summary sheet and subtracts the amount from the total EFTs. The new total is the amount used for the transfer request in the TOS EFT Letter.

HCM EFT Processing


HCM EFT Process
OAKS Pay Cycle Summary Data is created when pay cycles run
OAKS Sends the file to Bank
OAKS Pay Cycle Summary Data is Sent to OBM via e-mail.
The Banks will Contact OBM if there is a discrepancy between the amounts called in and the amount of the file
OBM Payment Issuance Manager ensures the OAKS and DAS totals match, then e-mails the totals in to the Bank.
DAS sends a copy of the payroll reconciliation to OBM with the EFT amount.
Treasurer's Letter is prepared with the EFT amount.
TOS letter and support is hand-delivered to TOS and Stamped.
TOS Initiates Transfer to the appropriate Bank
DAS and OBM log into Bank website for Reports
Agencies send a Request for Off-Cycle Manual Paycheck form to DAS
Agencies send DAS a Reversal/Return of Direct Deposit form for any reversals
OBM faxes the bank a summary of all reversal items
Cancellation Letters are Prepared
EFTs are cancelled in OAKS, and reissued as check payments.
OBM receives Monthly Bank Statement
Daily Transfers and returns are reconciled to the bank statements

The above flowchart summarizes the HCM EFT process from the time OAKS sends the payment data to OBM through the TOS transfer of funds to the designated HCM EFT bank for payment. OAKS HCM biweekly delayed and biweekly current payroll EFTs are processed through Key Bank. When a file is ready for processing, the OAKS Batch Team sends it to the Bank. The Batch Team also sends an e-mail to OBM with the pay cycle, pay date and pay end date, and the amounts contained in the file(s).

OBM receives the dollar amount of the EFT file each pay cycle from DAS and confirms the amount with the bank. The amount is compared to the amount of the file created and sent to the bank by the OAKS batch team. A copy of the Payroll Reconciliation is sent to OBM. The payroll reconciliation for each pay cycle is performed by DAS. OBM is responsible for submitting the amounts provided by DAS to TOS for transfer and e-mailing the totals to the bank, as well as the month-end reconciliation.

The Payment Issuance Manager sends an e-mail to Key Bank requesting the funds be processed from the OBM payroll account. There is no confirmation from the bank that the amounts match; however, if there are discrepancies, the bank will notify OBM immediately.

Returns / Cancellations

The KTT report is received from the bank on a daily basis and is used to create adjusting entries for HCM EFTs. EFT rejects and reversals are cancelled in OAKS and supporting documentation is provided to OBM to support the amounts returned from the bank. Each day, DAS Payroll Support obtains a "Full Activity Summary Report" (KTT report) that contains returns.

For rejects, the data from the KTT report is recorded by DAS. Each agency is notified of the errors for their agency. The agency must then send a Request for Off-Cycle Manual Paycheck form to DAS before the EFT can be cancelled and reissued. Once the notice is received, DAS Payroll Support reverses / adjusts the payment. DAS Payroll Support notes the advice number, earnings, taxes, deductions, and net pay. A manual (online) check is created with the original paycheck information, then confirmed and printed at DAS. The new check number is written on the Request for Reversal/Return of Direct Deposits form and attached to the manual check. The agency must then pick up and sign for the check. The Request for Reversal/Return of Direct Deposits form is detached and maintained at DAS.

The report of EFT rejects is saved and OAKS automatically uploads the reject information file to create an Agency Error Report that further details the EFT errors. Agencies can log on to OAKS and view the errors for their agency and make changes as necessary.

Reversals

When an agency realizes there is an error with a payroll transaction that was submitted, they may request a reversal. Examples of reasons for reversals include a closed account, overpayments, suspected account fraud, and changed account information. The agencies send a Reversal/Return of Direct Deposit form to DAS to authorize cancelling the payment. The agencies enter the employee name, ID, agency, pay period end date, pay date, and the reason for the request on the form.

DAS enters the information from the KTT Reports into a tracking spreadsheet. An ACH Services File Maintenance Request form is also completed and faxed to the bank, along with the tracking spreadsheet, to provide a summary of the payees, bank account information, and dollar amounts of the transactions that require removal from the file. The fax also contains the total amount that should be credited to the account for the reversals and rejects (from the spreadsheet). Once the bank has completed the deletions, they fax the form back to OBM with checkmarks next to the payments that were successfully deleted, and notes next to any that had problems. A confirmation e-mail is also sent to OBM stating the wire transfer is complete.

These amounts are also available through the OH_PYCNTR_Reversals query in OAKS. The total amount is used on the DAS Payroll

Each month a bank statement is received from Key Bank for the four FIN EFT accounts (Maintenance, Medicaid, Tax, and Welfare) and the HCM EFT Payroll account. The bank statements show all deposits and additions (transfers in from TOS), and debits for outgoing payments. OBM maintains a reconciliation spreadsheet for each account that is updated throughout the month with deposit and withdrawal activity, with the exception of the HCM account.

Each month, OBM prepares a reconciliation for the FIN Maintenance, Income Tax, Medicaid and Welfare accounts to help ensure all incoming and outgoing transfers and return/cancelations have been processed and documented.

OBM maintains a reconciliation spreadsheet that contains FIN TOS letters, KTT report totals, and agency reversals for each month.
When the Key Bank statement is received (approximately the 15th of the month), the reconciliation is performed. A separate reconciliation is performed by the Data Integrity Group (DIG) at OBM over FIN returns and cancelations. A spreadsheet is used to track the returns/reversals, cancelations from three locations: the Daily KTT report, a query from OAKS, and the Month-end bank statement.

The month-end reconciliation is then performed to ensure all returns, reversals and cancelations are accounted for in OAKS.

DAS did not have a month-end reconciliation process is in place to reconcile the internal records of the HCM payroll account to the bank statement. Without reconciliation, there is no assurance all incoming and outgoing transfers have been processed and documented.

USER AGENCY CONTROL CONSIDERATIONS

The OAKS application was designed with the assumption that certain controls would be implemented by user agencies. This section describes additional controls that should be in operation at the user agencies to complement the controls at OAKS. User auditors should consider whether the following controls have been placed in operation at user agencies:

General EDP Control Procedures

- Each agency should develop and adopt its own computer and Internet security policies, in accordance with the related Ohio IT policies issued by DAS/OIT, IT Policy. Users should be aware of their agency computer policies and be required to sign-off on them acknowledging their acceptance.

- Users should be aware of the confidential nature of passwords and should take precautions to ensure that passwords are not compromised. Agencies' computer security policies should provide password administration guidelines to help ensure their passwords are confidential, cannot be guessed, and easily remembered.

- State agencies should ensure all user IDs are individually assigned to each system user to improve individual accountability of user activity. State agencies should ensure user IDs and associated privileges and attributes are issued only to authorized users who need access to computer resources in order to perform their job functions.

- State agencies should ensure all requests for OAKS access are documented on a security request form and are signed and approved by an authorized agency designee. Agencies should have procedures in place for notifying the OAKS security team of the appropriate agency designee, as well as any changes to that designee.

- When user agency personnel that have access to OAKS are terminated or change job responsibilities, all access capabilities for that user should be removed or modified. Procedures should be in place at the agency level notifying OAKS and ISD of the vacancy or change and all physical access to agency buildings and logical access to the system should be revoked or modified.

- Agencies should periodically complete an access confirmation of all agency users by reviewing each agency OAKS user and their associated access and requesting any needed modifications from the OAKS security team.

- Network and communication lines, junctions, and key hardware components should be secured in an area that restricts access to only authorized IT individuals.

- Agencies should review the listing of physical access to the SOCC, make any applicable modifications, and submit to SOCC security for updating to help ensure only authorized individuals have physical access to the second floor computer room at the SOCC.

- Agencies should retain source documents for an adequate period to help ensure that data can be re-inputted in the event that data files are destroyed prior to being backed up and rotated off-site.

- State agencies should ensure that backup and off-site rotation procedures for the application files and programs are adequate for their agency objectives.

- Agencies should ensure users attend the training recommended for their individual security roles.

Financial Application Controls

OAKS_FIN

- Agencies should monitor their budgets within the system to ensure they set up as requested.
- Requisition approval paths should be created by the authorized agency users to be set up in OAKS by OBM through workflows. Workflows should provide an adequate segregation of duties and restrict users from approving their own transactions.
- Transactions should require supporting documentation with proper approval.
- Purchase orders and vouchers that fail budget check or threshold check are reported on the Budget Check Exceptions screen as well as a Reconciliation Workbench report. Agencies should check the Budget Check Exceptions screen and the Reconciliation Workbench on a regular basis to identify and correct purchase orders and vouchers that have failed budget check.
- Recorded transactions should be periodically reviewed by someone independent of the data entry process to confirm proper authorization. Key transactions should be compared with input documents to ensure transactions are valid, complete and correct.
- State agencies should ensure that vendor information entered on all expenditure transactions is accurate.
- Properly approved input documents should be maintained to provide an audit trail and backup. Maintenance periods for these documents should follow approved records retention guidelines.
- Agencies should monitor the pickup and delivery of RTA warrants from OBM to the agency to ensure all warrants are received as expected.
- Agencies should ensure that all identifying chartfields, including Fund Code, Department ID, Account, ALI, Program Code, and Project are completely and accurately populated for all transactions entered into FIN.
- State agencies should ensure invoices represent the goods or services received and are in compliance with contracts.
- For payments made for goods and services, appropriate staff should periodically determine that payments recorded accurately reflect payments made for goods and services actually received. Unmatched transactions should be researched and reclassified on the system.
- State agencies should review the Correct Posting Errors screens regularly in order to identify posting errors that need corrected.
- Recorded transactions should be reviewed by someone independent of the data entry process. Key transactions should be compared with input documents to ensure transactions are valid, complete, and correct.

- State agencies should periodically confirm that Speed Charts contain valid, active chartfield combinations to ensure transactions are coded to the proper chartfields.

- State agencies should periodically review their chartfields to ensure they are accurate and authorized.

- State agencies should review the payroll edit check and budget check reports and correct errors for each payroll timely using the OAKS job Aid: Researching and Correcting Payroll Journal Errors, and ensure that any corrections to the payroll journals balance by fund and ISTV cross reference.

- Users should be aware of the confidential nature of passwords and should take precautions to ensure that passwords are not compromised.

- State agencies should ensure user IDs and associated privileges and attributes are issued only to authorized users who need access to computer resources in order to perform their job functions.

- State agencies should ensure all user IDs are individually assigned to each system user to improve individual accountability of user activity.

OAKS_HCM

- Access to perform payroll transactions in OAKS should be restricted to only those individuals whose job responsibilities require it.

- Payroll transactions should require supporting documentation with proper user authorization (something signed by the user and their supervisor).

- Only authorized agency personnel should review and resolve errors that originate from the OAKS time and labor processing. These errors could come from the Time/Admin process, the creation of the pay sheet by DAS/HRD, etc.

- Agencies and boards should notify DAS/HRD of any changes in authorized payroll processing personnel.

- Properly approved input documents should be maintained to provide an audit trail and to support all OAKS input activity. Maintenance periods for these documents should follow approved records retention guidelines.

- All agency timekeeper specialists at each agency should review the Manage Exceptions page in OAKS and resolve all errors before final payroll processing is complete.

- All agencies should review the employee master table report to ensure the payroll data that was processed for their agency was complete and accurate.

- User agencies should have controls over the development, testing and security of agency developed COGNOS reports used for monitoring OAKS transactions. Data obtained from EPM should be periodically reconciled to expected HCM production totals to help ensure the completeness and accuracy of COGNOS reports.

- Agencies should have controls in place to ensure that when an employee has a change in status all steps in the change process are completed.

- State agencies should implement procedures to periodically verify the integrity of their payroll databases.

- Agencies should review the FIN Budget Error Report each pay period and resolve any errors that were created when the payroll data was budget checked in FIN using the OAKS Job Aid: Researching and Correcting Payroll Journal Errors. All corrections should balance by fund and ISTV cross reference.

- Agencies should review the FIN Budget Error Report each pay period and resolve any errors that were created when the payroll data was budget checked in FIN.

- Agencies should review the overtime reports available in COGNOS or SOPPS to identify excessive or unauthorized overtime worked.

- Agencies should respond to any access confirmation requests from the service organization.

Warrant Writing

- Agencies should monitor the pick-up and delivery of RTA warrants from OBM to the agency to ensure all warrants are received as expected.

The user control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user agencies. Other controls may be required at the user agencies.

SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR

This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the OAKS's internal control that may be relevant to user organization's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.

The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system, for example procedures performed at the OAKS and procedures performed at user organizations that utilize the OAKS.

For each of the control objectives listed below, only those controls which contribute to the attainment of the related control objective are described and were tested.

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Changes to Existing Applications

<table>
<tr><td colspan="2"><b>Changes to Existing Applications and Systems -</b> <i>Control Objective:</i>
<b>Change Requests</b> - Requests for application program changes or system upgrades should be appropriately considered and processed.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>OAKS has a documented formal program change request process in place for the FIN and HCM applications to ensure changes are properly processed and to help ensure proper segregation of duties.</td><td>Inspected the change management procedures.</td><td>Control operating as described.</td></tr>
<tr><td>OAKS requires an SMS ticket/CRM case initiated by the requestor through PeopleSoft Accenture Service Management Suite or CRM application for all standard FIN and HCM enhancement or modification changes. The SMS tickets and CRM cases are prioritized and assigned to the Managed Services Vendor (MSV) for completion.</td><td>Obtained a listing of SMS's from the Production Control Log. Filtered the list to only include those SMS's whose target was the production environment and excluded data updates for FIN to determine the population of FY2010 changes.
Selected all 36 FIN changes and haphazardly selected 60 of the 100 HCM changes and inspected the corresponding SMS for availability, prioritization, and assignment.</td><td>An SMS was unavailable for 3 of the FIN changes selected for testing. All three were related to a project for Shared Services.
No other exceptions noted.</td></tr>
<tr><td>OAKS modifications and enhancements must be approved by the appropriate OAKS Service Assurance teams before the program change begins.</td><td>Selected all 36 FIN changes and haphazardly selected 60 of the 100 HCM changes and inspected the corresponding design approval e-mails for evidence of approvals of the design documents from a Service Assurance team member.</td><td>Design approval from Service Assurance was not available for 8 of the FIN changes selected for testing.
No other exceptions noted.</td></tr>
<tr><td>The Production Support team meets periodically to discuss all aspects of the FIN and HCM production application changes.</td><td>Selected 25 weeks throughout the year and inspected the Managed Services Request Status - FIN Weekly Operations reports as well as the scheduled HCM/OAKS/HRD Operations - Pay Confirm Week Review Meeting and the scheduled HCM Operations Meetings to confirm SMSs are periodically reviewed.</td><td>Control operating as described.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Changes to Existing Applications and Systems -</b> <i>Control Objective:</i>
<b>Change Requests</b> - Requests for application program changes or system upgrades should be appropriately considered and processed.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>OAKS has developed guidelines for the implementation of system software.</td><td>Inspected the Upgrades and Patches section of the System Administrator Manual.</td><td colspan="2">The guidelines have not been updated for new hardware implemented in February 2010.</td></tr>
<tr><td>The software used to maintain the OAKS program code has an automated lockout feature that prohibits multiple programmers from making simultaneous changes to the same program.</td><td>Attempted to access programs that were already checked out for modifications by another programmer.</td><td colspan="2">Control operating as described.</td></tr>
<tr><td>Formal written guidelines exist to define test procedures, strategies, and requirements for maintaining documentation for OAKS program changes.</td><td>Inspected the UAT testing guidelines for the Service Assurance and the Central Agency Functional Team.</td><td colspan="2">Control operating as described.</td></tr>
<tr><td>The approval of the requestor or Service Assurance, is required on all OAKS testing before acceptance of the program change.</td><td>Obtained a listing of SMS's from the Production Control Log. Filtered the list to only include those SMS's whose target was the production environment and excluded data updates for FIN to determine the population of FY2010 changes.
Selected all 36 FIN changes and 60 of the 100 HCM changes and inspected the corresponding User Acceptance Testing (UAT) e-mail approval.</td><td colspan="2">UAT approval was not available for 4 of the FIN changes selected for testing. In addition, verbal approval only was obtained for 10 of the HCM changes selected for testing.
No other exceptions noted.</td></tr>
<tr><td>Testing documentation is maintained for all OAKS program changes.</td><td>Obtained a listing of SMS's from the Production Control Log. Filtered the list to only include those SMS's whose target was the production environment and excluded data updates for FIN to determine the population of FY2010 changes.
Selected all 36 FIN changes and 60 of the 100 HCM changes and inspected the corresponding Developer's Packet for evidence of testing documentation.</td><td colspan="2">The Developer's Packet was not available for one FIN change selected for testing.
No other exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Changes to Existing Applications and Systems -</b> <i>Control Objective:</i>
<b>Change Requests</b> - Requests for application program changes or system upgrades should be appropriately considered and processed.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>OAKS restricts access to the test environments to authorized personnel.</td><td>Inspected a listing of the FIN and HCM accounts with PeopleSoft roles which allow access to the development and testing environments as well as a listing of accounts with access to the test environments on the Unix server. Confirmed access was restricted and commensurate with job duties.</td><td colspan="2">The following exceptions were noted:
• One account was identified as no longer needing access to the HCM development environment.
• One account was identified as no longer needing access to the HCM QA/testing environment.
• Two accounts were identified as no longer needing access to the FIN QA/testing environment.
• One account was identified as no longer needing access to the UNIX development environments.
No other exceptions noted.</td></tr>
<tr><td>The FIN/HCM development lead and Service Assurance approval is required before a program is transferred into production.</td><td>Obtained a listing of SMS's from the Production Control Log. Filtered the list to only include those SMS's whose target was the production environment and excluded data updates for FIN to determine the population of FY2010 changes.
Selected all 36 FIN changes and 60 of the 100 HCM changes and inspected the corresponding Production Object Migration Request (PROD-OMR) and SA e-mail approval.</td><td colspan="2">All of the changes had at least one of the two approvals; however, the following exceptions were noted:
• Service Assurance approval was not available for 2 HCM changes selected for testing.
• Service Assurance approval was not available for one FIN change selected for testing.
• Managed Services Team Lead or their designee approval was not available for 2 FIN changes selected for testing.
No other exceptions noted.</td></tr>
</table>

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Access to the OAKS production servers is restricted through UNIX security. Programmers and developers are restricted from having access to the production environments to help ensure programs are migrated by individuals independent of the development group.	Inspected the access of all four Unix production database servers, all the users and corresponding roles who have access to update the FIN and HCM PeopleSoft security rights, and a list of users with greater than READ access to the OAKS Oracle Production Databases for FIN and HCM. Confirmed the appropriateness of the users' access with the Interim State CISO and OAKS HCM/FIN management.	Two developers/programmers were identified as having unauthorized access greater than READ to the ORACLE production databases. No other relevant exceptions noted.
When changes are implemented into production, prior versions of each Structured Query Reporter (SQR) and Structured Query Command (SQC) object are available to be restored using Mercury ITG in the event of an emergency.	Inspected screen prints of versioning for FIN and HCM SQR and SQC objects.	Control operating as described.
OAKS utilizes vendor software to monitor and track all FIN and HCM code changes to the production environments.	Inspected the software roles and definitions, options, and the Prod OMR Processing Procedures as well as an example Prod OMR for FIN and HCM.	Control operating as described.
Documentation standards are available to the OAKS development teams to follow to enhance and maintain PeopleSoft objects.	Inspected the Coding Structure and Data Standards Documents.	Control operating as described.
Program changes are documented within the program code and/or developers packets. Developers Packets are maintained by SMS number and document the affected programs, changes to source code, and testing scenarios/results.	Obtained a listing of SMS's from the Production Control Log. Filtered the list to only include those SMS's whose target was the production environment and excluded data updates for FIN to determine the population of FY2010 changes. Selected all 36 FIN changes and 60 of the 100 HCM changes and inspected the corresponding system documentation or Developer's Packet.	No exceptions noted.

Changes to Existing Applications and Systems - *Control Objective:* **Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Confidential Personal Information (CPI), as defined by Ohio Revised Code, has been masked within the development environment.	Inspected screen prints of masked data within the FIN and HCM development environments and confirmed that all CPI data has been masked.	Control operating as described.

Changes to Existing Applications and Systems - *Control Objective:* **Documentation and Training** - Users and IT staff should receive appropriate training when their responsibilities are impacted by application changes or system upgrades .		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Notification of program changes, documentation, and training are provided to affected users.	Confirmed responsibility of the functional teams to determine when changes to applications affect the users and if training and/or communication of the changes is necessary. Selected all 36 FIN changes and haphazardly selected 60 of the 100 HCM changes and inspected communication of changes via 'The Weekly.' Inspected a CAB Change Request form for evidence that user training and user communication are documented on the form.	Control operating as described.

IT Security

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>Security Management -</b> Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>OAKS has an application security policies and procedures document to outline user responsibilities for OAKS application security and access.</td><td>Inspected the OAKS application security policies and procedures document for FIN and HCM.</td><td>Control operating as described.</td></tr>
<tr><td>All employees and contractors assigned to OAKS are required to sign an acknowledgement of state IT policies related to data security as part of the initial condition of employment or assignment.</td><td>Selected 25 out of the 205 personnel assigned to OAKS as of 07/22/10 and inspected the corresponding policy acknowledgement forms.</td><td>No exceptions noted.</td></tr>
<tr><td>State agencies, commissions, and boards document and authorize all access requests before they are granted in the OAKS application.</td><td>Selected 60 out of 382 agency GAAP significant HCM PeopleSoft user access change requests made during FY10 and inspected the corresponding User Security Access Request Forms.
Selected 60 out of 1,834 agency GAAP significant FIN PeopleSoft user access change requests made as of 06/15/10 and inspected the corresponding User Security Access Request Forms.</td><td>No HCM exceptions noted.
Seven of the 60 (11.67%) FIN access requests selected for testing did not have the signature of the FIN authorized agency security designee. Four of the 60 (6.66%) FIN access requests had a signature of an individual that was not listed on the FIN authorized agency security designee list. One of the 60 (1.67%) FIN access requests contained the signature of an individual that was authorized to submit request forms, but they were not authorized to sign and authorize FIN access.</td></tr>
<tr><td>When an OAKS user is terminated, the security automation program will identify the terminated user and remove the user’s access from the application.</td><td>Obtained a query of all OAKS users who were terminated during FY10.
Compared the listing to the FIN and HCM user access listings to confirm access was removed since termination.</td><td>No exceptions noted.</td></tr>
</table>

IT Security - *Control Objective:* **Security Management -** Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A security notice/banner screen is displayed prior to logging into the FIN and HCM modules that states: "OAKS is a State of Ohio computer system, which may be accessed and used only for official state business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action."	Attempted to login to the OAKS FIN and HCM applications and inspected the security notice displayed prior to login.	Control operating as described.
Procedures are in place for requesting encrypted access to ISD secured devices. Access request forms must be completed by agencies and approved by ISD personnel.	Inspected the Request for TCP/IP Access Procedures. Obtained a list of TCP/IP Access Requests for FY10 and selected 25 of the 157 user IDs that were created during FY10 and confirmed each had a Request for TCP/IP Access form on file that contained authorization signatures of both the user's supervisor and the administrator who granted the access.	Four of the 25 (16%) applicable TCP/IP Access Request forms did not have all of the required signatures. No other exceptions noted.
FIN and HCM PeopleSoft accounts are reviewed periodically to determine appropriateness of access and to eliminate unnecessary accounts.	Inspected the FIN and HCM reconciliation tracking spreadsheets.	Control operating as described.
IT security policies are in place to guide the security and administration of the OAKS infrastructure application.	Inspected the DAS/OAKS IT Security Policies to confirm policies were in place to guide the security and administration of the OAKS infrastructure.	Control operating as described.

IT Security - *Control Objective:* **System Level Access Controls -** Access to the computer system, programs, and data should be appropriately restricted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
System sign-on parameters have been established for the OAKS Windows network.	Inspected the default sign-on parameters that were used for all Windows Domain users.	No exceptions noted.
Access to the OAKS UNIX production servers is restricted through UNIX security.	Inspected the UNIX access list of all user IDs that had access to each of the OAKS production servers and confirmed the appropriateness of the listed accounts with the Interim State CISO.	No exceptions noted.
System password controls have been established for the UNIX system on the production servers that process the OAKS programs and data.	Inspected the system sign-on/password parameters for the OAKS production servers.	Due to a script error, one of the parameters was not enforced as intended. Instead, the default parameter value was in place. No other exceptions noted.
Unauthorized network traffic for the OAKS production environment is monitored by network personnel to identify key intrusion events in a timely manner.	Inspected the IDS configuration and the activity being captured by the IDS. Also, inquired with Accenture management to confirm network traffic is monitored.	Control operating as described.
OAKS uses a firewall to aid in the protection of the entity's assets, including the OAKS production environment.	Inspected a network schematic that showed major hardware connectivity of the OAKS network and the firewall rules for evidence of a network infrastructure that included the use of firewalls that restricted unauthorized IP traffic.	Control operating as described.
Administration of firewalls and modifications to the firewall rules for the firewalls protecting the OAKS production environment are documented.	Inspected the firewall administration and modification policies and procedures and the Firewall CAB Change Log to confirm policies were in place and firewall changes were documented, tracked, and approved by Accenture.	No exceptions noted.
Logical access to the firewall rules is restricted to appropriate personnel.	Inspected the Firewall administrator's permissions within the configuration tool for the firewalls protecting the OAKS production environment. Confirmed the appropriateness of the access with an Accenture Infrastructure Manager.	No exceptions noted.

<table>
<tr><td colspan="3"><b>IT Security -</b> <i>Control Objective:</i>
<b>Application Level Access Controls -</b> Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>The OAKS application incorporates PeopleTools application security software that uses roles, permission lists, field level security, page permissions, and row-level security to prevent unauthorized access to transactions.</td><td>Inspected a list of all FIN user roles and FIN permission lists. Inspected a list of all HCM user roles and HCM permission lists.</td><td colspan="2">Controls operating as described.</td></tr>
<tr><td>Application sign-on (password) parameters have been established for the OAKS FIN and HCM modules.</td><td>Inspected the password configurations globally applied to all users for the OAKS FIN and HCM modules of the OAKS application.</td><td colspan="2">Controls operating as described.</td></tr>
<tr><td>The OAKS system automatically logs users off the system after a period of terminal inactivity.</td><td>In the OAKS production environment, logged in and left a user account inactive for a period equal to the defined inactivity threshold and then inspected the resulting warning/error message. Also, inspected the source code for the web server session timeout value.</td><td colspan="2">Control operating as described.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>IT Security -</b> <i>Control Objective:</i>
<b>System Software and Utilities Access Controls -</b> Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.</td><td><b><i>Control Objective Has Not Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Access to assign and update OAKS access security rights is restricted to only those individuals whose job responsibilities require it.</td><td>Inspected the list of users with access to the FIN and HCM roles and permission lists and confirmed the appropriateness of the listed accounts with the Interim State CISO.</td><td>Of the 3 unique combinations of HCM roles/permissions, 1 of the 3 combinations contained users with unneeded access.
Of the 14 users with the role/permission combination that enabled users to reset HCM passwords 3 did not require these security rights to perform their job responsibilities.
Of the 17 unique combinations of FIN roles/permissions, 3 of the 17 combinations contained users with unneeded access as follows:
• Of the 12 users with the role/permission combination that enabled users to update FIN workflows and redirect work to employees 2 did not require access.
• Of the 16 users with the role/permission combination that enabled users to reset FIN passwords 4 did not require access.
• Of the 8 users with the role/permission combination that enabled users to perform role maintenance on terminated employees' FIN access, 1 did not require access.</td></tr>
</table>

<table>
<tr><td colspan="3">**IT Security -** *Control Objective:*
System Software and Utilities Access Controls - Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.</td><td>***Control Objective Has Not Been Met***</td></tr>
<tr><td>*Control Procedures:*</td><td>*Test Descriptions:*</td><td colspan="2">*Test Results:*</td></tr>
<tr><td>Access to OAKS system administrator privileges, sudo commands, and the UNIX superuser account (root) is restricted to authorized personnel.</td><td>Inspected the OAKS system administrator user ID password parameters.
Inspected the OAKS UNIX server group access list. Identified the admin group users and confirmed their job duties required these admin privileges with the UNIX administrator.
Inspected the sudo user access list and allowable sudo commands and confirmed the appropriateness of the sudo access with the Interim State CISO.
Inspected the sudo logs for the months of 07/2009, 9/2009, 11/2009, 01/2010, 03/2010, and 05/2010 to confirm logs were available to monitor usage of the sudo commands.
Inspected the su logs for the months of 08/2009, 10/2009, 12/2009, 02/2010, 04/2010, and 06/2010 to confirm users were using the su command and not logging directly into the root account and that the su logs were available to monitor su command activity.
Finally, inspected the available login/logout logs for the months of 10/2009, 12/2009, 02/2010, 04/2010, and 06/2010 for all the OAKS production servers for any successful attempts to logon as root or other administrator accounts.</td><td colspan="2">Only one week of the six months of sudo logs requested for testing was available for inspection.
SU logs were not available for review from the 4th production server for the months of 08/2009, 10/2009, and 12/2009. No su logs were available for review from any of the production servers for the months of 02/2010 and 04/2010. SU logs were not available for review from the 3rd production server for the month of June 2010.
No other exceptions were noted.</td></tr>
</table>

IT Security - *Control Objective:* **System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled.		***Control Objective Has Not Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Access to the OAKS databases that house production data is restricted to authorized users.	Confirmed the appropriateness of the access of users to the OAKS production databases with the OAKS management.	Of the 83 users with access to the FIN Oracle databases 4 no longer required access. (3 had View access, 1 had View, Update, & Delete access) Two (both users had View, Update, and Delete access) of the 83 users with full access to the FIN Oracle databases had greater permissions than required for their job duties. Two (both users had View, Update, and Delete access) of the 67 users with full access to the HCM Oracle databases had greater permissions than required for their job duties.
Access to the encrypted security password file is restricted to the UNIX administrators.	Inspected the access rights to the etc/shadow file for the production UNIX servers.	Control operating as described.

IT Security - *Control Objective:* **Physical Security -** Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The computer room and data processing facilities and equipment at the SOCC are protected by environmental and physical access controls. Access cards are required for all employees to the building at all times. Environmental controls identified include: • Raised floors. • Water sensors under the floor near A/C units. • Pre-action sprinkler heads at the ceiling level. • Smoke detectors in the ceiling and floors. • Fire extinguishers. • Emergency power-off switches. • Fire hoses connections. • UPS system and backup generators. A maintenance alarm system monitors the temperature and humidity throughout the building.	Toured the 2nd floor computer room at the SOCC facility and inspected the existence of physical and environmental controls. In addition, reviewed a listing of all users with access to the 2nd floor computer room.	Of the 289 individuals with access to the 2nd floor SOCC computer room, 17 no longer required access for performance of their job responsibilities.
Monthly load tests are performed to confirm the ISD's generators, switchgear, and UPS systems are available for providing constant power for data processing.	Inspected the load test reports for the months of July 2009 through May 2010 to confirm load tests were performed monthly, test results were documented, and any problems encountered were investigated and corrected. Also, inspected documentation of preventative maintenance of the battery systems that was performed during the audit period to confirm the results were documented.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Background checks are required before access is granted to non-visitor personnel at the SOCC.	Inspected a listing of SOCC badges issued during FY2010. Selected 25 of 126 individuals from the listing and inspected the corresponding Request for Background Check forms and results.	No exceptions noted.
Visitor access to the SOCC is monitored and restricted. The “State of Ohio Computer Center Visitor Notification Form” is completed and approved in advance or at the time the visitor arrives at the SOCC by an authorized SOCC employee who has sign-in privileges. The form includes relevant information guiding and documenting visitor access.	Observed access procedures for visitors entering the SOCC building. Also, inspected the SOCC Visitor Notification forms and guest registries from 25 of the approximate 250 processing days during the audit period.	Control operating as described.
The SOCC conducts quarterly confirmations of user agency personnel with access to the SOCC second floor computer room.	Inspected documentation of the September 2009 and February 2010 SOCC OIT 2nd floor quarterly access reviews for physical access confirmations from OIT.	No exceptions noted.

IT Security - *Control Objective:* **Physical Security -** Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
The computer room and data processing facilities and equipment at the data center are protected by environmental and physical access controls. Access cards or visitor cards are required for all employees and individuals to the building at all times. Environmental controls identified include: • Water sensors under the floor. • Raised Floors. • Fire Extinguishant-25 (FE-25). • Smoke detectors in the ceiling and floors. • Fire extinguishers. • Emergency power-off switches. • UPS system and backup generators. • Video surveillance system. A notification system monitors the temperature and humidity throughout the processing facilities.	Toured the computer room at the data center facility on 08/13/2010 with Accenture and facility personnel and inspected the existence of physical and environmental controls.	No exceptions noted.
Visitor access to the data center is monitored and restricted. The data center security personnel must be notified of all planned visits by non-data center individuals by authorized data center or client personnel prior to the time the visitor arrives at the data center facility.	Observed and discussed access procedures for visitors entering the NADC facility with the Data Center Manager.	Control operating as described.

IT Operations

IT Operations - *Control Objective:* **System Administration and Maintenance** - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS management meets weekly to discuss any production issues with the OAKS applications.	Inspected the HCM and FIN production meeting agendas for 10 weeks of business processing during FY10.	Control is operating as described.
OAKS system availability/downtime is monitored and documented on the OAKS Service Level Availability spreadsheets.	Inspected OAKS Service Level Availability (SLA) reports for the months of July 2009 through June 2010.	Control is operating as described.
OAKS batch processes are documented, scheduled, and maintained with automated batch processing software and are manually documented using various forms and worksheets.	Inspected the FIN and HCM UC4 Job Plans, Production Resolution Matrices, Production Batch Schedule Worksheets, and example Production Batch Status E-mails for 25 days in FY10.	Control is operating as described.
Access to the OAKS OHBATCH ID (used to administer batch processing) is restricted to authorized state employees and contractors working on the OAKS project who share the account.	Inspected password lifetime parameters of the batch ID. Also, confirmed the appropriateness of the list of users with knowledge of the batch ID password with the OAKS batch team lead.	Control is operating as described.
Detailed OAKS incident reports are created to document, maintain, and track any OAKS infrastructure issues, including any application outage, security issue, or major batch scheduling problem that may cause a major business impact of downtime.	Inspected the incident logs and root cause analysis documentation for OAKS Severity One issues for the months of July 2009 through June 2010.	Control is operating as described.
Database administrators use tools to manage and help ensure optimum performance of the OAKS databases.	Inspected screen shots of the database tools and the centralized scripts list used by the DBAs to manage the databases. Also, inquired with the OAKS DBA regarding database management procedures and tools.	Control is operating as described.
The operational status of the OAKS databases is documented daily to verify they are operating as designed.	Inspected the Daily Morning Prod Environment Health Checklist for 25 haphazardly selected days of business processing during FY10.	No relevant exceptions noted.

IT Operations - *Control Objective:* **System Administration and Maintenance -** Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Database incident reports are created to document, maintain, and track identified OAKS database issues.	Inspected all of the database incidents logged by the DBA team from July 2009 to June 2010.	Control is operating as described.
Database space check reports are automatically generated for the OAKS DBAs to review potential OAKS database issues.	Obtained example database space check reports and the database space check schedule to confirm reports were generated daily and e-mailed to the OAKS production DBAs for review.	No relevant exceptions noted.
Database alert messages are automatically generated to notify the OAKS DBAs of OAKS database performance thresholds that are about to be and/or have been exceeded.	Inspected example database alert messages.	Control is operating as described.
The operational status of the OAKS applications and critical components is documented daily to verify the OAKS applications and components are operating as designed.	Inspected the Daily Morning Prod Environment PS Admin Health Checklists for 25 days of business processing during FY10.	No relevant exceptions noted.
PeopleSoft SYSAUDIT reports are generated on a quarterly basis to identify system integrity issues for the OAKS FIN and HCM modules and are available for review by the OAKS infrastructure team.	Inspected the SYSAUDIT reports for each quarter from July 2009 through June 2010. Confirmed the procedures for the review of the SYSAUDIT reports with the interim State CISO.	Control is operating as described.

IT Operations - *Control Objective:* **Backup -** Up-to-date backups of programs and data should be available in emergencies.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
HP Continuous Access provides asynchronous replication between the NADC HP EVA and SOCC DR HP EVA for all Window servers.	Inspected the StorageWorks Command View EVA screen print showing the Windows data replication status of backups from the NADC in Cincinnati to the SOCC in Columbus.	Control is operating as described.

<table>
<tr><td colspan="3"><b>IT Operations -</b> <i>Control Objective:</i>
<b>Backup -</b> Up-to-date backups of programs and data should be available in emergencies.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Oracle Data Guard provides automated database replication between NADC production databases and SOCC DR databases.</td><td>Inspected the Oracle Redo Logs screen prints and testing files showing the Oracle data replication from the NADC production database to the DR database.</td><td colspan="2">Control is operating as described.</td></tr>
</table>

APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

FIN / EFT

(OAKS_FIN) - *Control Objective:* **Authorization -** Information entered into the agency's computer application represents valid data approved by the agency's management.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Before a requisition can be processed into a purchase order (PO), a level 4 approval is required. A user with level 4 approval access is restricted from approving a requisition they created.	Reperformed the control by attempting to source a requisition into a PO after the level 1 approval and before the level 4 approval had been obtained. Also reperformed the control by creating a requisition and attempting to approve the requisition using the same user ID. Finally, because it was noted during prior year testing that a glitch in the system occasionally caused requisitions to be automatically approved if a user's security role changed between the creation and approval of a requisition, inspected a query from the OAKS EPM environment to identify requisitions that were submitted and approved by the same user.	No relevant exceptions noted.
Only agency users with the “Requisitioner” role can create requisitions within OAKS.	Reperformed the control by attempting to access the ‘Create Requisition’ fields using an ID that was not assigned the “Requisitioner” role.	No exceptions noted.
A purchase order must pass ‘Budget Check’ before it can be “dispatched” and used for payment processing. Budget Check validates that sufficient funds are available for the PO and, if successful, automatically encumbers the funds.	Reperformed the control by attempting to dispatch a purchase order with a budget status of “Not Chk’d.”	No exceptions noted.

(OAKS_FIN) - *Control Objective:* **Authorization -** Information entered into the agency's computer application represents valid data approved by the agency's management.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
Approved non-debit vouchers that exceed $500 require an approved purchase order. All special approval validation vouchers require an approved purchase order, regardless of the amount.	Reperformed the control by attempting to enter a non-debit voucher over $500 without an associated, approved purchase order. Additionally, reperformed the control by attempting to enter a special approval validation voucher for less than $500 without an associated, approved purchase order.	No exceptions noted.	
OAKS will not process purchase orders or vouchers in excess of the available budget. Transactions that have failed budget check can be viewed on the Budget Check Exceptions Screen.	Reperformed the control by attempting to enter a voucher in excess of the available budget. Inspected the resulting error and the updated status after the Budget Check process. Also, inspected the failed voucher on the Budget Check Exceptions Screen. Processed a purchase order in excess of the available budget, and a purchase order against a budget that did not exist. Ran Budget Check and inspected the resulting budget status on the Budget Check Exceptions Screen.	No exceptions noted.	
OAKS automatically creates a timestamp at each stage of the requisition approval process that includes the user ID, the date and time of the approval, and any notes manually entered by the approver.	Observed the requisition entry and approval process and inspected the resulting timestamps of the approvals.	No exceptions noted.	
A voucher cannot be created from a PO unless the PO has been dispatched (approved and made available to the voucher creators).	Reperformed the control by attempting to process a voucher for a purchase order before it was dispatched.	No exceptions noted.	
Vouchers are required to be approved before a payment can be processed against it.	Reperformed the control by attempting to process a payment against a voucher that had an Approval Status of ‘Pending’ and verified the payment could not be processed.	No exceptions noted.	

<table>
<tr><td colspan="3"><b>(OAKS_FIN) -</b> <i>Control Objective:</i>
<b>Authorization -</b> Information entered into the agency's computer application represents valid data approved by the agency's management.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Deposits entered by the agency must be approved by the agency AR administrator before being transferred to and approved by the Treasurer of State.</td><td>With the assistance of the AR team lead, observed the approval process for a deposit.</td><td colspan="2">No relevant exceptions noted.</td></tr>
<tr><td>Vendors in OAKS must have a status of “Approved” before a voucher and payment can be issued to the vendor.</td><td>Reperformed the control by attempting to process a voucher to a vendor with a status of “Inactive,” “Unapproved,” and “To Archive.”</td><td colspan="2">Control operating as described.</td></tr>
<tr><td>OAKS has an edit in place to prohibit the submission of an EFT voucher for a vendor without EFT information in the FIN system.</td><td>Reperformed the control in the test environment by attempting to submit a voucher with a location of “EFT” for a vendor that did not have EFT information defined in OAKS. Inspected the resulting error message and confirmed the payment could not be submitted.</td><td colspan="2">Control operating as described.</td></tr>
<tr><td>Approval paths in FIN are created at the agencies and set up by the agency security designees through workflows. The system has edits to help ensure segregation of duties and approval paths are maintained.</td><td>Reperformed the control by logging into OAKS FIN as an agency security designee and attempting the following scenarios:
• Identified a user assigned the Level 4 approver role and attempted to add a requestor role.
• Attempted to assign a user to a business unit and origin ID that belonged to another agency.
• Attempted to remove the Level 4 approver role from a user that had transactions awaiting their approval.
• Attempted to remove the Level 4 approver role prior to assigning a new Level 4 approver in the approval path.
Inspected the resulting errors.</td><td colspan="2">Control operating as described.</td></tr>
</table>

(OAKS_FIN) - *Control Objective:* **Authorization -** Information entered into the agency's computer application represents valid data approved by the agency's management.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Only authorized users with the appropriate level of access can create appropriation and allotment budgets within OAKS FIN.	Reperformed the control by logging into OAKS FIN using a user ID that was not assigned a role that allowed updating the Appropriation or Allotment budgets. Attempted to create an Appropriation and Allotment budget and inspected the resulting errors.	Control operating as described.

(OAKS_FIN) - *Control Objective:* **Completeness of Input -** All authorized transactions are input and accepted for processing by the application.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Vendors are required to have unique vendor ID and tax ID numbers within OAKS to help restrict the entry of duplicate vendors. A “Check for Duplicates” option is available when adding a new vendor that identifies existing vendors with the same tax ID.	Reperformed the control by attempting to create a vendor in FIN with a vendor ID and tax ID that already existed in the application for another vendor. Inspected the resulting errors. Additionally, reperformed the control by attempting to create a vendor by using a tax ID that already existed on the system. Clicked the “Check for Duplicates” option and inspected the resulting error message.	Controls operating as described.
Required verification fields within OAKS force the user to enter the following fields *when adding a new vendor*: Vendor ID, Vendor Short Name, Vendor Name1, Address, and Location.	Reperformed the control by attempting to enter a vendor with each of the required fields left blank. Inspected the resulting errors and verified the new vendor could not be added until the errors were resolved.	No exceptions noted.
Required verification fields within OAKS *requisition processing* force the user to enter the following fields: requestor ID, category code, item description, units of measurement, quantity, price, ship to code, fund, account, ALI, department, and program code chartfields.	Reperformed the control by attempting to enter a requisition within the FIN QAS system with each of the required fields left blank. Inspected the resulting errors.	No exceptions noted.

(OAKS_FIN) - *Control Objective:* **Completeness of Input -** All authorized transactions are input and accepted for processing by the application.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Required verification fields within OAKS *voucher processing* force the user to enter the following fields: business unit, voucher ID, invoice ID, address code, pay terms, invoice date, last receipt date, and account.	Reperformed the control by attempting to enter a requisition within the FIN QAS system with each of the required fields left blank. Inspected the resulting errors.	No exceptions noted.
OAKS does not allow for the *entry of a voucher* with a duplicate voucher ID or business unit, invoice number, and dollar amount. An online error is received and will prohibit further processing.	Reperformed the control by entering a voucher within the FIN QAS system with each of the required fields left blank. Inspected the resulting errors.	No exceptions noted.
OAKS does not allow for the *entry of a pending item* with a duplicate group ID.	Reperformed the control in the test environment by attempting to add a voucher with the same Voucher ID as an existing voucher. Also, attempted to enter a voucher with a unique voucher ID number but with the same business unit, invoice number, and dollar amount as an existing voucher. Inspected the resulting errors.	No exceptions noted.
OAKS requires a Deposit ID and Deposit Unit for each *entry of a deposit* that must be a unique number for each agency.	Reperformed the control by attempting to create a new deposit in FIN QAS leaving the deposit ID and deposit Unit fields blank, and the same deposit unit and deposit ID as a previously entered deposit ID. Inspected the resulting errors. Also, attempted to create a new deposit for agency A using an existing deposit ID from agency B.	No exceptions noted.

(OAKS_FIN) - *Control Objective:* **Completeness of Input -** All authorized transactions are input and accepted for processing by the application.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Required verification fields for a *pending item* (including an ISTV entry type) force the user to enter a group unit, group ID, group type, origin ID, format currency, count, item ID, customer, amount, business unit, entry type, and reason for an ISTV entry type before the transaction can be processed.	Reperformed the control in the test environment by attempting to enter a pending item with each of the required fields left blank. Inspected the resulting errors. Removed the Fund Code and Department ID from a pending item, and then attempted to process the pending item through the system. Inspected the resulting error that was received when Journal Generator was run.	The Fund Code and Department ID chartfields were not required for input of a pending item. An error was not received until Journal Generator was run. No other exceptions noted.
Required verification fields for a *regular deposit* force the user to enter a deposit unit, deposit ID, bank code, bank account, deposit type, count, payment ID, and accounting date before the transaction can be processed.	Reperformed the control by attempting to enter a regular deposit leaving the required fields blank. Removed the Fund Code and Department ID from a regular deposit, and then attempted to process the item through the system. Inspected the resulting error that was received when Journal Generator was run.	The Fund Code and Department ID chartfields were not required for input of a deposit. An error was not received until Journal Generator was run. No other exceptions noted.
OAKS does not allow for the entry or posting of an ISTV with a duplicate bill number, dollar amount, vendor, and item ID.	Reperformed the control by attempting to create an ISTV with the same bill number, dollar amount, vendor, and item ID as an existing ISTV and inspected the resulting error message. Attempted to post an ISTV with the same information as an existing, non-posted ISTV.	No exceptions noted.
FIN OBM receives the dollar amount of the FIN EFT files each day from OAKS and confirms the amount with the respective banks. The amount is compared to the amount of the file created and sent to the bank by the OAKS batch team.	Inspected the EFT reconciliation documentation for the 5th, 10th, and 20th of each month from July 2009 through June 2010 for Maintenance, Medicaid, and Tax. Inspected Welfare August and December 2009, and May 2010 reconciliation.	No exceptions noted.

(OAKS_FIN) - *Control Objective:* **Completeness of Input -** All authorized transactions are input and accepted for processing by the application.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
HCM OBM receives the dollar amount of the HCM EFT file each pay cycle from DAS and confirms the amount with the respective bank. The amount is compared to the amount of the file created and sent to the bank by the OAKS batch team.	Using the calendar that listed state payroll dates between July 2009 and June 2010, selected 10 payroll cycles and inspected the corresponding reconciliation documentation.	No exceptions noted.
FIN / HCM After the dollar amounts of the EFT files have been compared between the OAKS file and the bank, OBM prepares and delivers/emails a letter/report to the Treasurer of State's office requesting the funds be transferred to the appropriate accounts. The Treasurer's letter is time and date stamped at the TOS office.	Inspected the TOS letters and reconciliation documentation for the FIN EFT payments from the 5th, 10th, and 20th of each month from July 2009 through June 2010. Selected 10 payroll cycles during the audit period and inspected the corresponding TOS letters and reconciliation documentation for the HCM EFT payments. Compared the FIN and HCM letters to the reconciliation documentation.	No exceptions noted.
FIN The Key Total Treasury (KTT) report is received on a daily basis from Key Bank and is used to create adjusting entries for FIN EFTs. EFT returns are cancelled in OAKS and supporting documentation is maintained.	Inspected the KTT reports for the 5th, 10th, and 20th of each month from July 2009 through June 2010. Also, inspected the OAKS screen prints of the payment cancellations for the EFTs cancelled for the respective days.	No exceptions noted.

(OAKS_FIN) - *Control Objective:* **Completeness of Input -** All authorized transactions are input and accepted for processing by the application.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
FIN Each month, OBM prepares a reconciliation for the FIN Maintenance, Income Tax Medicaid and Welfare accounts to help ensure all incoming and outgoing transfers have been processed and documented.	For the 5th, 10th, and 20th of each month from July 2009 through June 2010 inspected the Key Bank statements for the FIN accounts and reconciliation spreadsheets. Re-performed selected steps of the reconciliation by comparing the bank statement amounts to Treasurer of State transfer letters and return item totals. For July 2009 through June 2010, inspected the monthly reconciliations for the FIN Maintenance, Income Tax, Medicaid, and Welfare accounts.	No exception noted.	
HCM EFT rejects and reversals are cancelled in OAKS and supporting documentation is provided to OBM to support the amounts returned from the bank.	Haphazardly selected a sample of 60 out of 869 EFT returns and reversals and inspected the cancellation faxes sent to the bank, and inspected OAKS screen prints of the payment cancellations for the EFTs cancelled for the respective days.	Of 60 of the applicable returns, 5 were not supported by an ACH Return Items report. Five of the 60 items were not supported by an Individual File Maintenance Request Form and were also not listed in section III of the KTT report or the KTT report could not be provided for verification. One of the 60 applicable returns was not supported by a KTT report sent from the bank No other exceptions noted.	

(OAKS_FIN) - *Control Objective:* **Accuracy of Input -** Authorized transactions are accurately recorded and in the proper period.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Online edit checks prevent or detect incorrect entry of vendor ID type and tax ID *when adding a vendor*. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved.	Reperformed the control by attempting to add a vendor ID type that was not a predefined value and inspected the resulting error. Likewise, attempted to enter a tax ID with less than nine characters and inspected the resulting error.	Controls operating as described.
Online edit checks prevent or detect incorrect entry of fund, account, ALI, department, program, grant/project, and project codes *when creating a requisition*. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved.	Reperformed the control in the test system by attempting to enter a requisition using fund, account, ALI, department, program, grant/project and project codes that were not listed in the system as valid values. Inspected the resulting errors.	Controls operating as described.
Online edit checks prevent or detect incorrect entry of fund, account, ALI, department, program, and business unit *when creating a voucher.* Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved.	Reperformed the control in the test system by attempting to enter a voucher using fund, account, ALI, department, business unit, and program that were not listed in the system as valid values. Also attempted to enter a voucher within the FIN QAS system using only an account code. Inspected the resulting errors.	No exceptions noted.
A voucher number is automatically and sequentially assigned, if not manually entered by the user, once all required payment information has been entered.	Reperformed the control in the test system by creating a new voucher using a Voucher ID of “NEXT.” Inspected the resulting automatically assigned voucher number. Created a second voucher within the FIN QAS system using a Voucher ID of “NEXT.” Inspected the resulting sequentially assigned voucher number.	Control operating as described.

(OAKS_FIN) - *Control Objective:* **Accuracy of Input -** Authorized transactions are accurately recorded and in the proper period.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Edits exist that disallow transactions that exceed the Controlling Board's threshold limit of $50,000. Agencies that have obtained a Controlling Board waiver for greater than $50,000 cannot process transactions that exceed the waiver amount.	Reperformed the control by attempting to save a purchase order for a vendor for an amount that would exceed their threshold of $50,000.00. Also reperformed the control by attempting to save a Purchase Order for a vendor that would exceed their controlling board waiver threshold amount. Inspected the resulting errors.	No exceptions noted.
Agencies must select from a predefined list of Group Types, Origin IDs, Format Currencies, Customer Numbers, Reason Codes, and Business Units *when entering a pending item in the Accounts Receivable module* to help reduce data entry time and input errors.	Reperformed the control by attempting to enter a pending item using values that were not listed as valid values in the system for the required fields. Inspected the resulting errors.	Control operating as described.
When Accounts Receivable posting errors occur, the errors are available for the agencies to view and correct within OAKS. The error provides information about any data that produced an error during posting.	Reperformed the control by creating an ISTV transaction with an error and inspected the error on the Posting Results and Correct Posting Errors screens within the Accounts Receivable module.	Control operating as described.
The OAKS application provides users with pre-populated data entry options in the key fields of *requisition creation, voucher entry, pending item entry, and deposit/payment processing* to reduce input errors. Data input that does not match one of the entry options is rejected and the user receives an error.	Identified 'prompt' buttons (drop-down menus) in OAKS used to search for valid data entry options. Reperformed the control by attempting to input invalid data in key fields. Inspected the resulting errors.	Control operating as described.

<table>
<tr><td colspan="3"><b>(OAKS_FIN) -</b> <i>Control Objective:</i>
<b>Accuracy of Input -</b> Authorized transactions are accurately recorded and in the proper period.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Combo edits exist when creating an allotment budget in FIN. Expense categories must be assigned to a valid budget period, and the allotment budget must be less than or equal to the appropriation budget.</td><td>Reperformed the control by creating an Allotment budget in the FIN QAS environment and attempting the following scenarios:
• Assigned a payroll budget line item to an annual budget period (required to be budgeted quarterly).
• Assigned a non-payroll budget line item to a quarterly budget period (required to be budgeted annually).
• Entered budget lines that caused the allotment budget to exceed the appropriation budget.
Attempted to post the entries and inspected the resulting errors.</td><td colspan="2">Control operating as described.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>(OAKS_FIN) -</b> <i>Control Objective:</i>
<b>Transaction Classification -</b> Budgetary amounts are made to the correct accounts. (In other words, the agency is assured that initial budget and any amendments are coded to the proper account classification.) Receipt and purchase transactions relate to the account posted.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Online edit checks prevent or detect incorrect entry of fund, account, ALI, department, program, grant/project, and project codes <i>when creating a requisition</i>. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved.</td><td>See the test description for this control test at the OAKS_FIN control objective; Accuracy of Input.</td><td colspan="2">See the test results for this control test at the OAKS_FIN control objective; Accuracy of Input.</td></tr>
</table>

(OAKS_FIN) - *Control Objective:* **Transaction Classification -** Budgetary amounts are made to the correct accounts. (In other words, the agency is assured that initial budget and any amendments are coded to the proper account classification.) Receipt and purchase transactions relate to the account posted.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Online edit checks prevent or detect incorrect entry of fund, account, ALI, department, and program *when creating a voucher*. Error messages are displayed for erroneous data and further processing is prohibited until the errors are resolved.	See the test description for this control test at the OAKS_FIN control objective; Accuracy of Input.	See the test results for this control test at the OAKS_FIN control objective; Accuracy of Input.
Agencies must select from a predefined list of Group Types, Origin IDs, Format Currencies, Customer Numbers, Reason Codes, and Business Units *when entering a pending item in the Accounts Receivable Module* to help reduce data entry time and input errors.	See the test description for this control test at the OAKS_FIN control objective; Accuracy of Input.	See the test results for this control test at the OAKS_FIN control objective; Accuracy of Input.

(OAKS_FIN) - *Control Objective:* **Cutoff -** Transactions are recorded in the proper period.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Requisitions and vouchers must have a date within the current or future fiscal year.	Reperformed the control in the test environment by attempting to enter a requisition and voucher with a date in the prior fiscal year. Inspected the resulting errors.	Control operating as described.
Pending items and payments must have an accounting date within the current accounting period.	Reperformed the control in the test environment by attempting to enter a pending item and payment with a date in the prior fiscal year and one in a future accounting period. Inspected the resulting errors.	Control operating as described.

(OAKS_FIN) - *Control Objective:* **Cutoff -** Transactions are recorded in the proper period.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Unreconciled (non-redeemed) warrants over 90 days old are automatically voided on a monthly basis.	Inspected the FIN batch schedule and the OHAP050 job details. Reperformed the control by inspecting an outstanding payment that was over 90 days old prior to running the monthly OHAP050 job, and after running the OHAP050 job. Additionally, inspected a query of unreconciled warrants that were 90 or more days old.	No relevant exceptions noted.
Appropriation-level budgets must be created for a one year, annual budget period.	Reperformed the control in the test environment by creating an Appropriation budget and entering a quarterly budget period for a line within the budget.	Control operating as described.

(OAKS_FIN) - *Control Objective:* **Transaction Occurrence -** Transaction amounts recorded occurred and are not fictitious Duplicate budgetary amounts are prevented.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Vouchers are required to be approved before a payment can be processed against it.	See the test description for this control test at the OAKS_FIN control objective; Authorization.	See the test results for this control test at the OAKS_FIN control objective; Authorization.
Deposits entered by the agency must be approved by the agency AR administrator before being transferred to and approved by the Treasurer of State.	See the test description for this control test at the OAKS_FIN control objective; Authorization.	See the test results for this control test at the OAKS_FIN control objective; Authorization.

(OAKS_FIN) - *Control Objective:* **Existence -** Account balances exist as of the financial statement date.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
The PO and voucher budget check processes automatically update the corresponding commitment control budget.	Reperformed the control by obtaining the beginning balance of a commitment control budget. Processed a purchase order and voucher against that commitment control budget and inspected the resulting balances after budget check was run.	No exceptions noted.	
The pending item and deposit/payment processes automatically update the corresponding commitment control budgets.	Reperformed the control by obtaining the beginning balance of a commitment control budget. Processed a pending item, deposit/payment, and direct journal against that commitment control budget and inspected the resulting balances.	No exceptions noted.	
A purchase order must pass 'Budget Check' before it can be "dispatched" and used for payment processing. Budget Check validates that sufficient funds are available for the PO and, if successful, automatically encumbers the funds.	See the test description for this control test at the OAKS_FIN control objective; Authorization.	See the test results for this control test at the OAKS_FIN control objective; Authorization.	

(OAKS_FIN) - *Control Objective:* **Integrity of Standing Data -** Changes to standing data are authorized and accurately input.			***Control Objective Has Not Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
Only authorized users can create or modify *vendor information* in OAKS.	Inspected the access of users with the ability to update the vendor table in FIN and confirmed the appropriateness of the access with DAS vendor management and OSS management.	There were 11 out of 60 users (20%) with access to update the vendor database that did not require the access for their job responsibilities. From inspection of a list of vendor changes during FY10, we did not identify any unauthorized changes made by these users during the audit period.	

(OAKS_FIN) - *Control Objective:* **Integrity of Standing Data -** Changes to standing data are authorized and accurately input.		***Control Objective Has Not Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OSS completes additions or changes to the vendor file based on documented requests submitted from the vendors.	Inspected the OSS guidance used for entering vendors into FIN. Inspected a listing of EFT and Non-EFT vendors added or modified during the audit period. Sampled 60 of 13,347 EFT vendors and 60 of 6,055 Non-EFT vendors that were added or modified and inspected the corresponding change documentation.	There were 10 of 60 Non-EFT vendor changes (17%) and 3 of 60 EFT vendor changes (5%) that were not accompanied by change request documentation. The Vendor Addresses were entered incorrectly for 4 EFT vendor changes. No other relevant exceptions noted.
Only authorized users can post *journal entries* directly to the general ledger.	Inspected the access of users with the ability to post direct general ledger entries and confirmed the appropriateness of user access with the GL team lead.	No exceptions noted.
Only authorized users can create or modify the *chart of accounts (chartfields)* in OAKS.	Inspected the access of users with the ability to create or modify chartfields and confirmed the appropriateness of the user access with the appropriations control supervisor and GL team lead.	There was one out of 15 users (6.6%) with access to create and modify chartfields that did not require the access for their job responsibilities.
OBM creates and/or modifies chartfield accounts (*department, program, grant/project, project, service location, reporting, agency use, and budget refere*nce) based on approved Chartfield Change Request forms submitted by the agencies.	Inspected chartfield signature authorization forms for all agencies. Obtained a list of changes or additions to the OAKS chartfields made during the audit period. Selected 60 of 7,051 changes and inspected the corresponding Chartfield Change Request forms for availability and approval by the authorized agency contact. Inspected each sampled chartfield in the FIN QAS environment and compared them to the supporting change documentation.	No exceptions noted.
OBM State Accounting documents and approves all changes and modifications to the *fund, account, ALI, and ISTV Xref* chartfields.	Obtained a list of changes or additions to the OAKS chartfields made during the audit period. Selected 60 of 594 changes and	No relevant exceptions noted.

(OAKS_FIN) - *Control Objective:* **Integrity of Standing Data -** Changes to standing data are authorized and accurately input.		***Control Objective Has Not Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
	inspected the corresponding Chartfield Change availability and approval by OBM state accounting. Inspected each sampled chartfield in the FIN QAS environment and compared them to the supporting change documentation.	

(OAKS_FIN) - *Control Objective:* **Completeness and Accuracy of Updating -** Updates, modifications, and/or additions to information already on the application's files or database are accurately entered.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
HCM staff manually check the GL and AP files sent to FIN for accuracy and completeness.	Inspected the procedures used for performing the check of the GL and AP file creation and transfer to FIN. Re-performed the procedures for the 4/23/10 payroll with the HCM management and inspected the reconciliation documentation for five pay periods during FY10.	Controls operating as described.
The FIN HR ACCTG_LINE table, which is used to create journal entries in FIN, is created based on HCM gross pay figures from payroll processing.	Obtained the Total Gross Payroll Cost figures from the HCM Bi-Weekly Current (BCR) and Bi-Weekly Delayed (BWD) Payroll Reconciliation Spreadsheets for the following check dates: 2/26/10, 4/18/10, and 6/18/10. Obtained the figures from the HR_ACCTG_LINE table (FIN table populated by HCM used to create journals) for: 2/26/10, 4/18/10, and 6/18/10. Compared the Total Gross Payroll Cost figures from the Payroll Reconciliation Spreadsheets to the figures from the HR_ACCTG_LINE table.	No exceptions noted.

(OAKS_FIN) - *Control Objective:*
Completeness and Accuracy of Updating - Updates, modifications, and/or additions to information already on the application's files or database are accurately entered.

Control Objective Has Been Met

Control Procedures:	*Test Descriptions:*	*Test Results:*
The PO and voucher budget check processes automatically update the corresponding commitment control budget.	See the test description for this control test at the OAKS_FIN control objective; Existence.	See the test description for this control test at the OAKS_FIN control objective; Existence.
When a voucher is processed against a PO, the PO balance is automatically reduced by the voucher amount.	Reperformed the control by processing a voucher against a Purchase Order and inspected the resulting PO balance.	Control operating as described.
FIN edit and budget check errors for payroll processing are available for review and correction by the individual agencies.	Inspected examples of the GL Journal Edit Errors Report and Budget Check Errors Report.	Control operating as described.
OAKS does not allow for the entry of a voucher with a duplicate voucher ID or business unit, invoice number, and dollar amount. An online error is received and will prohibit further processing.	See the test description for this control test at the OAKS_FIN control objective; Completeness of Input.	See the test results for this control test at the OAKS_FIN control objective; Completeness of Input.
When receipts and pending items are entered in batch, control totals must be in balance with the details of the batch before accounting entries can be created.	Reperformed the control by entering a regular deposit and a pending item and attempting to create accounting entries while the control totals were out of balance. Inspected the resulting errors.	No exceptions noted.
ARUPDATE is a process in OAKS that automatically updates financial information and creates accounting entries when pending items and receipts are entered in FIN.	Reperformed the control by creating a pending item and payment in FIN. Confirmed the accounting entries did not exist online before running ARUPDATE and then inspected the updated accounting entries after ARUPDATE was run.	No exceptions noted.
When a payment is cancelled or voided in FIN, the commitment control expenses are automatically reduced and available appropriations are automatically restored by the amount of the original payment.	Reperformed the control by inspecting the original budget, voiding a payment, and inspecting the resulting budget amounts.	No exceptions noted.
The pending item and deposit/payment processes automatically update the corresponding commitment control budgets.	See the test results for this control test at the OAKS_FIN control objective; Existence.	See the test results for this control test at the OAKS_FIN control objective; Existence.

(OAKS_FIN) - *Control Objective:* **Completeness and Accuracy of Updating -** Updates, modifications, and/or additions to information already on the application's files or database are accurately entered.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS does not allow for the entry of a pending item with a duplicate group ID.	See the test description for this control test at the OAKS_FIN control objective; Completeness of Input.	See the test results for this control test at the OAKS_FIN control objective; Completeness of Input.

(OAKS_FIN) - *Control Objective:* **Completeness and Accuracy of Accumulated Data -** The integrity of accumulated data is preserved.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Only authorized users can post journal entries directly to the general ledger.	See the test performed for this control test at the OAKS_FIN control objective; Integrity of Standing Data.	See the test results for this control test at the OAKS_FIN control objective; Integrity of Standing Data.
Only authorized users can create or modify the chart of accounts (chartfields) in OAKS.	See the test performed for this control test at the OAKS_FIN control objective; Integrity of Standing Data	See the test results for this control test at the OAKS_FIN control objective; Integrity of Standing Data.
OBM creates and/or modifies chartfield accounts (*department, program, grant/project, project, service location, reporting, agency use, and budget reference*) based on approved Chartfield Change Request forms submitted by the agencies.	See the test performed for this control test at the OAKS_FIN control objective; Integrity of Standing Data.	See the test results for this control test at the OAKS_FIN control objective; Integrity of Standing Data.
OBM State Accounting documents and approves all changes and modifications to the *fund, account, ALI, and ISTV Xref chartfields*.	See the test performed for this control test at the OAKS_FIN control objective; Integrity of Standing Data.	See the test results for this control test at the OAKS_FIN control objective; Integrity of Standing Data.
When a voucher is processed against a PO, the PO balance is automatically reduced by the voucher amount.	See the test performed for this control test at the OAKS_FIN control objective; Completeness and Accuracy of Updating.	See the test results for this control test at the OAKS_FIN control objective; Completeness and Accuracy of Updating.
OAKS requires a Deposit ID and Deposit Unit for each entry of a deposit that must be a unique number for each agency.	See the test performed for this control test at the OAKS_FIN control objective; Completeness of Input.	See the test results for this control test at the OAKS_FIN control objective; Completeness of Input.

(OAKS_FIN) - *Control Objective:* **Restricted Access to Assets -** Only authorized personnel have access to the application’s programs and data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Only agency users with the "Requisitioner" role can create requisitions within OAKS.	See the test description for this control test at the OAKS_FIN control objective; Authorization.	See the test results for this control test at the OAKS_FIN control objective; Authorization.
Only authorized users can post journal entries directly to the general ledger.	See the test description for this control test at the OAKS_FIN control objective; Integrity of Standing Data.	See the test results and level of reliance for this control test at the OAKS_FIN control objective; Integrity of Standing Data.
Only authorized users can create or modify the chart of accounts (chartfields) in OAKS.	See the test description for this control test at the OAKS_FIN control objective; Integrity of Standing Data.	See the test results and level of reliance for this control test at the OAKS_FIN control objective; Integrity of Standing Data.

HCM

<table>
<tr><td colspan="3"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Authorization:</b> Recorded payroll transactions are for performance of services and are approved.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>All permanent, non-exempt, and non-elected official agency positions and their corresponding pay rates must be approved by an OBM budget specialist prior to assigning an employee to the position. If an existing non-vacant position number is reclassified to a different category, a personnel action form must be sent to DAS for approval.</td><td>Inspected a listing from OAKS of all positions approved from July 1, 2009, to June 30, 2010. Selected 41 new or reclassified positions and inspected the corresponding position approval documentation from agencies requesting approval of positions.
Inspected the procedures used by the OBM budget analysts and agencies as a guide when approving positions.
In addition, in the OAKS test environment, confirmed that OAKS would not allow an employee to be hired into a proposed position.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Only authorized OBM budget specialists and elected agency payroll officers are assigned the roles that allow approving positions within OAKS HCM.</td><td>Inspected a list of users assigned the OH_HR_CENTRAL_OBM_SPEC and OH_HR_CENTRAL_ELECTED roles that allow the approving of agency positions and pay rates and confirmed the appropriateness of the users’ access with the OBM budget deputy director and the HCM HR configuration lead.
Attempted to approve a position in the OAKS test environment using a user ID that was not assigned one of the two OBM or agency central roles.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

(OAKS_HCM) – *Control Objective:* **Authorization:** Recorded payroll transactions are for performance of services and are approved.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS roles have uniquely defined user access levels to help prevent unauthorized changes to data. Row-level security prevents agencies from viewing or changing data from other agencies.	Reperformed the control in the OAKS test environment using a user ID with row-level security assigned to agency A by attempting the following: • Attempted to access and modify an employee's *personal* data from a different state agency C. • Attempted to access and modify an employee's *job* data from a different state agency C. • Attempted to change an employee's *position* data to a department belonging to a different state agency B. • Attempted to change an employee's *job* data to a department belonging to a different state agency B. Inspected the resulting error messages and confirmed further processing was prohibited until errors were resolved.	No exceptions noted.
Ohio row-level security, which allows access to all OAKS agency payroll data regardless of the associated agency, is restricted to authorized users.	Obtained a list of users assigned Ohio row-level security and confirmed the appropriateness of users with the DAS/HRD policy supervisor.	No relevant exceptions noted.
Payroll runs are confirmed by the DAS payroll supervisor prior to the final run.	Inspected the confirmation e-mails for five of the 26 pay periods in FY10 sent from the DAS payroll supervisor to the OAKS batch team.	Control operating as described.

(OAKS_HCM) – *Control Objective:* **Authorization:** Recorded payroll transactions are for performance of services and are approved.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
A Request for Off-Cycle Manual Paycheck form must be signed and approved by an authorized agency payroll representative and sent to DAS for all manual checks to be processed.	Inspected a listing of payroll contacts authorized to submit manual paycheck requests. Sampled 60 out of 23,043 manual checks and inspected the manual paycheck requests for authorized signatures, and confirmed the requests matched the check information from HCM.	Of the 60 forms, one was not signed at all, and two were signed by an agency representative that was not on the list of authorized contacts. No other exceptions noted.
Access to create and modify the leave plan tables is restricted to the HCM configuration team.	Inspected a list of HCM users with access to modify the leave plan tables and confirmed only authorized users were assigned the role.	No exceptions noted.

(OAKS_HCM) – *Control Objective:* **Completeness of Input:** Payroll transactions are input and accepted for processing.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Before an employee record is accepted, online edit checks require data fields on the personal information page (name, organizational relationship, address, DOB, and SSN) and the job information page (permanent / temporary indicator / title / company, classification indicator, department, job code, SSN, appointment type/bargaining unit flag, retirement plan [Empl class], officer code, paygroup, location, rate code, benefits enrollment, and compensation) to be entered.	Reperformed the control in the test environment by leaving the required fields blank in the Personal and Job Information sections and trying to process the transaction. Inspected the resulting errors/warning messages and confirmed further processing was prohibited until errors were resolved.	No exceptions noted.

(OAKS_HCM) – *Control Objective:* **Completeness of Input:** Payroll transactions are input and accepted for processing.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
HCM's Time and Labor function has edits in place to detect errors in the payroll. The Time Admin process applies business rules to reportable time submitted and determines exceptions. Agencies must review the Manage Exceptions Page and resolve all exceptions before the reportable time is converted to payable time and a pay sheet can be subsequently created	Inspected a listing of Time and Labor error messages. Selected 12 of the 129 edit errors and in the OAKS test environment, observed while the management analyst supervisor created the corresponding error scenarios in payroll. Inspected the resulting exceptions and an employee's subsequent pay sheet and paycheck to confirm the employees would not be compensated for the time submitted in error.	No exceptions noted.
For each pay cycle, DAS/OIT performs a reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing. An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed.	Observed the management analyst supervisor perform the payroll reconciliation for the bi-weekly delayed pay group pay date of 4/16/10 (10-BWD-04 pay cycle). Inspected the completed reconciliation, OAKS query, payroll summary reports, and e-mails sent to OIT printing and back from OIT printing at the completion of the warrant print job. Inspected payroll reconciliations and e-mails sent to OIT printing for four additional pay cycles (10-BWD-04, 10-BWD-08, 10-MDV-02, 10-BCR-12, and 10-MCR-01).	No exceptions noted.
Each employee may only be assigned to one pay group, which will determine the frequency and timing of payroll processing for the employee. Once a pay group has been submitted and confirmed, the group cannot be reprocessed	Inspected a listing of available pay groups in OAKS. In the OAKS test environment, reperformed the control by attempting to assign more than one pay group for an employee. Also attempted to submit a pay group for processing that had already been confirmed.	No exceptions noted.

(OAKS_HCM) – *Control Objective:* **Completeness of Input:** Payroll transactions are input and accepted for processing.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS has online edits that prohibit entering hours into a timesheet for an individual that is not an active state employee in HCM.	In the OAKS test environment, reperformed the control by attempting to submit hours for an employee with an HR status of “Inactive” in OAKS. Also submitted hours for an employee with an HR status of "active" and observed the system response.	Controls operating as described.

(OAKS_HCM) – *Control Objective:* **Accuracy of Input**: - Payroll transactions are accurately recorded.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Online edit checks help ensure employee and position data entered is accurately recorded during payroll processing. Error messages are displayed for erroneous data, and further processing is prohibited until the errors are resolved.	Reperformed the control in the test environment by entering invalid values in the date of birth, SSN, birth country, national ID country, date of death, ethnic group, effective date, and date entitled to Medicare employee data fields. Also, entered invalid values in the Effective Date, Job Code, Department, Regulatory Region, Company, Business Unit, Location, Standard Hours, Rate Code, Pay Group, Compensation Rate, Compensation Frequency, Position Number, and Benefits Program position data fields. Inspected the resulting errors/warning messages received and confirmed further processing was prohibited until errors were resolved.	There were no limits on the hourly rate field. Inspected a query of employees with hourly rates greater than $150/hour and found no relevant exceptions. There were no age limit edits on the date of birth field. Inspected a query of active employees younger than 16 or older than 85. One active employee was listed with a birth date in 1900 and two active employees were incorrectly listed with an age under 15. No other exceptions noted.

<table>
<tr><td colspan="3"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Accuracy of Input</b>: - Payroll transactions are accurately recorded.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Each employee (with SSN) is automatically assigned a unique employee ID to allow for tracking and monitoring of the employee’s status. Online edit checks are used to prevent an SSN from receiving duplicate employee IDs.</td><td>Created two new employees in the test environment and confirmed OAKS automatically generated sequential employee IDs
Also reperformed the control by attempting to create an employee ID using an SSN already used in the OAKS test environment. Inspected the resulting error message received and confirmed further processing was prohibited.</td><td colspan="2">Controls operating as described.</td></tr>
<tr><td>Each new job position is automatically assigned a unique number to allow for tracking and approval of the position.</td><td>Reperformed the control by creating two new positions in the OAKS test environment and confirmed OAKS automatically generated a unique, sequential position number.</td><td colspan="2">Control operating as described.</td></tr>
<tr><td>Each off-cycle / manual check is automatically assigned a unique check number, if the user does not manually enter a number.</td><td>Performed a walkthrough of the issuance of a manual check. Inspected the automatic generation of a check number when a number was not manually entered.
In the OAKS test environment, created a manual check using a check number that had already been used to determine whether HCM prevented duplicate check numbers.
Because the system allowed check numbers to be manually entered and reassigned, inspected a listing of manual checks with a source of “******” (indicating the manual check number had been changed) to determine how frequently the manual check numbers were changed during the audit period.
Inspected the paycheck history screen to confirm each check had a unique number.</td><td colspan="2">HCM allowed entering check numbers for manual checks that had already been used for previous checks. Because the system allowed duplicate manual check numbers to be entered, inspected the manual check listing to determine whether duplicate check numbers were issued during the audit period. There were no manual checks issued during the audit period that had duplicate check numbers.
No other exceptions noted.</td></tr>
</table>

(OAKS_HCM) – *Control Objective:* **Accuracy of Input**: - Payroll transactions are accurately recorded.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
HCM has edits in place that prevent submitting leave hours that exceed an employee's leave balance, or hours that exceed 24 hours for one day.	For the online edits (non-interfacing agencies): Reperformed the control in the OAKS test environment by attempting to enter compensatory, personal, and vacation leave hours that exceeded the available balances for an employee. Inspected the resulting error messages and confirmed further processing was prohibited. For the Time and Labor edits (interfacing and non-interfacing agencies): Reperformed the control in the OAKS test environment by attempting to submit sick leave hours that exceeded an employee's balance, and more than 24 hours of SL, VL, CT, and PL in one day for an employee. Inspected the resulting error message received after the Time Admin process was run, and confirmed further processing was prohibited. Finally, inspected an employee's paysheet (paycheck) for a pay period where a Time and Labor edit was not resolved to confirm the employee would not be compensated for the time submitted in error.	No other exceptions noted.	
Payroll journals are automatically edit checked and budget checked when the HCM data is interfaced to FIN. An error is created if the payroll journal contains invalid chartfields or the amount submitted exceeds the budget amount approved by OBM.	In the OAKS FIN test environment, inspected a payroll journal with a chartfield edit error and a payroll journal with a budget error. Corrected the payroll journal so it would pass the chartfield edit check but NOT budget check. Inspected the resulting error messages and confirmed the journal could not be posted while the budget error existed	No exceptions were noted.	

(OAKS_HCM) – *Control Objective:* **Accuracy of Input**: - Payroll transactions are accurately recorded.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
For each pay cycle, DAS/OIT performs a reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing. An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed.	See the test description for this control test at the OAKS HCM control objective; Completeness of Input.	See the test results for this control test at the OAKS_HCM control objective; Completeness of Input.	

(OAKS_HCM) – *Control Objective:* **Cutoff of Transactions -** Employee services are recorded in the proper period.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
Each position requires a valid effective date. The employee personal data effective date must be on or before the effective date the employee is hired into a position or assigned a work schedule. The system also produces a warning message if the effective hire date is more than 30 days in the past or future.	In the OAKS test environment, reperformed the control by attempting the following scenarios: • Left the effective date of a new position blank. • Entered an invalid effective date. • Hired an employee into a position using an effective date earlier than the employee's personal data effective date. • Assigned a work schedule to an employee using an effective date earlier than the employee's personal data effective date. Inspected the resulting error messages and confirmed further processing was prohibited until the errors were resolved. Additionally, attempted to hire an employee into a position using effective hire dates that were more than 30 days into the past and future and inspected the warning message.	No exceptions noted.
When a manual / off-cycle check is issued and recorded through OAKS, pay period end dates are automatically populated with the current pay period. Earnings beginning and end dates are required for all manual checks.	Confirmed manual check processing procedures with the management analyst supervisor and observed issuance of a manual check. Also, inspected a query of all manual checks issued from July 1, 2009, through June 30, 2010, and confirmed the earnings beginning, and end dates were required for all checks printed.	Controls operating as described.

<table>
<tr><td colspan="2"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Transaction Classification –</b> Employee's payroll relates to the employee's position and duties performed.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Positions must be assigned one or more combo codes (RefNos in old State Payroll system), each of which indicates the account to be charged for various payroll expenditures (earnings, deductions, taxes, etc). The combo code distribution percentage for a position must equal exactly 100%.</td><td>In the OAKS test environment, attempted to reperform the control by leaving the combo code field blank for a position. Additionally, modified the distribution percentage for a position to be less than, and then greater than 100%. Inspected the resulting error messages and confirmed further processing was prohibited until the errors were resolved.</td><td>Controls operating as described.</td></tr>
<tr><td>Row-level security prohibits agencies from using a combo code that belongs to another agency. A drop down box allows only the authorized combo codes to be available to the user.</td><td>In the OAKS test environment, logged in with row level security of OHRL_Agency A and attempted to access combo codes for agency B. Inspected the resulting error messages and confirmed further processing was prohibited until the errors were resolved.</td><td>No relevant exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Transaction Occurrence –</b> Payroll transactions recorded occurred and are not fictitious. Duplicate payroll transactions are prevented.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>For each pay cycle, DAS/OAKS performs a reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing.

An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed.</td><td>See the test description for this control test at the OAKS HCM control objective; Completeness of Input.</td><td>See the test results for this control test at the OAKS HCM control objective; Completeness of Input.</td></tr>
<tr><td>Each off-cycle / manual check is automatically assigned a unique number, if the user does not manually enter a number.</td><td>See the test description for this control test at the OAKS HCM control objective; Accuracy of Input.</td><td>See the test results for this control test at the OAKS HCM control objective; Accuracy of Input.</td></tr>
</table>

(OAKS_HCM) – *Control Objective:* **Transaction Occurrence –** Payroll transactions recorded occurred and are not fictitious. Duplicate payroll transactions are prevented.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS roles have uniquely defined user access levels to help prevent unauthorized changes to data. Row-level security prevents agencies from viewing or changing data from other agencies.	See the test description for this control test at the OAKS_HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.

(OAKS_HCM) – *Control Objective:* **Existence -** Account balances exist as of the financial statement date.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
All permanent, non-exempt, and non-elected official agency positions and their corresponding pay rates must be approved by an OBM budget specialist prior to assigning an employee to the position. If an existing non-vacant position number is reclassified to a different category, a personnel action form must be sent to DAS for approval.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.

<table>
<tr><td colspan="2"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Integrity of Standing Data -</b> Changes to standing data are authorized and accurately input.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Only authorized personnel have access to the corrections roles that allow the updating of historical data for approved positions, pay rates, and benefits in OAKS.</td><td>Confirmed the access level required to make changes to information within OAKS with OAKS security personnel.

Inspected a listing of roles available in OAKS with corrections access. Inspected a listing of users with access to Benefits, HR, Payroll, and security corrections access and confirmed the appropriateness of the access with OAKS management.

Additionally, reperformed the control by logging into the OAKS test environment using a user ID that was not assigned any of the corrections roles and attempted to modify the effective date (benefits), position number (HR), employee bank information (payroll) and security options (security) of existing records.</td><td>Controls operating as described.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Integrity of Standing Data -</b> Changes to standing data are authorized and accurately input.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>Access to modify the drop-down menu items in HCM is restricted to the payroll configuration team. All changes are documented and authorized on a CRM form.</td><td>Obtained a list of users within OAKS with access to update translate tables from the Security PM Admin.

Inspected the users with access to Benefits, HR, Payroll, and Security translate table access, and inspected the listings with the, OAKS Configuration / Benefits Lead; the DAS/OAKS Agency Support; the OAKS Configuration / Payroll / Time & Labor Team; and the Security PS Admin, respectively, to confirm the appropriateness of the access.

Additionally, obtained a listing of all updates to the translate tables from July 1, 2009 through June 30, 2010 and requested Change Request Forms for each change made to the translate tables. Inspected forms for proper authorization from a DAS supervisor.</td><td>Controls operating as described.</td></tr>
<tr><td>All permanent, non-exempt, and non-elected official agency positions and their corresponding pay rates must be approved by an OBM budget specialist prior to assigning an employee to the position. If an existing non-vacant position number is reclassified to a different category, a personnel action form must be sent to DAS for approval.</td><td>See the test description for this control test at the OAKS HCM control objective; Authorization.</td><td>See the test results for this control test at the OAKS HCM control objective; Authorization.</td></tr>
<tr><td>OAKS roles have uniquely defined user access levels to help prevent unauthorized changes to data.

Row-level security prevents agencies from viewing or changing data from other agencies.</td><td>See the test description for this control test at the OAKS HCM control objective; Authorization.</td><td>See the test results for this control test at the OAKS HCM control objective; Authorization.</td></tr>
</table>

<table>
<tr><td colspan="3">(<b>OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Completeness and Accuracy of Updating</b> – All payroll transactions input are accurately updated to the accounting system and payroll database.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>For each pay cycle, DAS/OIT performs a reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing.
An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed.</td><td>See the test description for this control test at the OAKS HCM control objective; Completeness of Input.</td><td colspan="2">See the test results for this control test at the OAKS HCM control objective; Completeness of Input.</td></tr>
</table>

<table>
<tr><td colspan="2">**(OAKS_HCM)** – *Control Objective:*
Completeness and Accuracy of Accumulated Data - The integrity of the payroll records in the payroll database and accounting system accounts, after payroll transactions have been accumulated in them, is preserved.</td><td>***Control Objective Has Been Met***</td></tr>
<tr><td>*Control Procedures:*</td><td>*Test Descriptions:*</td><td>*Test Results:*</td></tr>
<tr><td>Leave balances for each employee are accumulated according to the benefit plan contained in OAKS and are updated with any leave taken during payroll processing. A history of leave accruals and balances is available in OAKS.</td><td>Inspected an employee’s benefit (leave) plan in the OAKS test environment to determine the employee’s accrual rates.
Reperformed the control in the OAKS test environment as follows:
• Inspected an employee’s original leave balances.
• Inspected OAKS timesheets for pay periods where sick, personal, vacation and comp time earned and used were submitted.
• Recalculated the expected changes in leave balances based on the leave plan and hours submitted.
• Inspected subsequent leave balances in OAKS.
Inspected the Leave Accrual job aid to confirm agencies were provided instructions on using the leave accrual screens.
Finally, inspected an employee’s leave balances and accruals to confirm OAKS maintained a history of employee leave balances.</td><td>No relevant exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>(OAKS_HCM)</b> – <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data -</b> The integrity of the payroll records in the payroll database and accounting system accounts, after payroll transactions have been accumulated in them, is preserved.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>OAKS maintains a history of all manual and automated checks after they have been issued.</td><td>In the OAKS test environment, inspected an employee’s paycheck history on 7/8/10, after PPE 6/19/10 and before PPE 7/3/10 data was posted and available. Next, inspected the employee’s paycheck history on 7/27/10 and an example paycheck in OAKS to confirm the most recent paycheck was updated in the paycheck history. Finally, inspected an employee’s paycheck history in ePay to confirm paycheck history was available to state employees.</td><td>Control operating as described.</td></tr>
<tr><td>OAKS HCM automatically calculates an employee’s gross pay based on the employee’s hourly rate and the hours submitted.</td><td>Inspected a query containing hours worked and hourly rates for the paygroup BDQ for the pay period ending 6/5/2010. Used audit software to recalculate the expected gross pay for all employees in the paygroup and compared the recalculated gross pay to the actual gross pay from the paycheck listing.</td><td>No relevant exceptions noted.</td></tr>
<tr><td>For each pay cycle, DAS/OAKS performs a reconciliation to confirm the EFT and warrant payroll processing files and amounts balance to HCM production payroll amounts before the files are submitted for EFT processing/warrant writing.
An additional reconciliation is completed after warrant writing is completed to confirm the amounts submitted for processing were printed and distributed.</td><td>See the test description for this control test at the OAKS HCM control objective; Completeness of Input.</td><td>See the test results for this control test at the OAKS_HCM control objective; Completeness of Input.</td></tr>
</table>

(OAKS_HCM) – *Control Objective:* **Restricted Access to Assets and Records -** Only authorized personnel have access to personnel/payroll records, including standing data.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
OAKS roles have uniquely defined user access levels to help prevent unauthorized changes to data. Row-level security prevents agencies from viewing or changing data from other agencies.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.
Ohio row-level security, which allows access to all OAKS agency payroll data regardless of the associated agency, is restricted to authorized users.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.
All permanent, non-exempt, and non-elected official agency positions and their corresponding pay rates to be approved by an OBM budget specialist prior to assigning an employee to the position. If an existing non-vacant position number is reclassified to a different category, a personnel action form must be sent to DAS for approval.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.
Only authorized OBM budget specialists and elected agency payroll officers are assigned the roles that allow approving positions within OAKS HCM.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.
Access to create and modify the leave plan tables is restricted to the HCM configuration team.	See the test description for this control test at the OAKS HCM control objective; Authorization.	See the test results for this control test at the OAKS HCM control objective; Authorization.

Warrant Writing

(WARRANT WRITING) - *Control Objective:* **Completeness and Accuracy** – All disbursements are written for the proper amount and to the proper payee. All warrants are printed and issued.		***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*
DAS Mainframe Print Center management maintains formal instructions relating to check printing and documentation.	Inspected the check printing documentation and instructions, procedures for submitting OAKS production warrants to print, OAKS financials roll to roll procedures, OAKS warrant delivery procedures, procedures for void accountability, and procedures for daily checking of RTAs. Also, toured the print facility and confirmed the procedures were available to all Mainframe Print Center staff.	No exceptions noted.
Courier slips accounting for all warrants taken for mailing and distribution are completed and approved by DAS and the courier.	Obtained the OAKS Warrant Logs for FY10. Selected 30 dates from FY10 and inspected the corresponding courier pickup slips for approval.	No relevant exceptions noted.
Warrant Delivery Logs are signed and dated by both the OBM delivery representative and the OBM recipient representative confirming the integrity of the lock box security and agreement between the delivery log and actual contents of the lock box.	Observed the daily pickup routine of the RTA warrants. Inspected the OAKS Warrant Delivery Log Sheets from the 1st, 10th, and 20th of July 2009 through June 2010.	No relevant exceptions noted.

<table>
<tr><td colspan="3"><b>(WARRANT WRITING) -</b> <i>Control Objective:</i>
<b>Completeness and Accuracy</b> – All disbursements are written for the proper amount and to the proper payee. All warrants are printed and issued.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>All issued warrants are accounted for and uniquely identified during the warrant writing process.</td><td>From the calendar of FY10 payroll dates, selected 10 payroll dates and inspected the corresponding e-mails from the HCM bi-weekly delayed, bi-weekly currents, current monthly, or monthly advanced files submitted by the HCM staff to the Mainframe Print Center indicating the payroll warrant files were waiting in the print queue and the post-print e-mails sent from the Mainframe Print Center staff after printing was completed. In addition, inquired about reconciliation procedures with the Mainframe Print Center manager. Also, inspected the corresponding OAKS Check Logs for the 10 selected dates.
Selected 30 dates from FY10 OAKS Warrant Logs and inspected the corresponding OAKS Financials Report Log and OAKS Check Logs. Inspected the corresponding Fulfillment Service Job Logs for evidence of print sequence numbers for all warrants processed.
Observed the Mainframe Print Center manager submit a warrant file for printing.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

(WARRANT WRITING) - *Control Objective:* **Completeness and Accuracy** – All disbursements are written for the proper amount and to the proper payee. All warrants are printed and issued.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
OAKS check stock is compared to actual printed warrants each time OAKS warrants are printed via the updated and signed OAKS check log.	Selected 10 payroll dates from FY10 and inspected the corresponding OAKS Check Logs for reconciliation information accounting for used check stock. Selected 30 dates from FY10 from the OAKS Warrant Logs and inspected the corresponding OAKS Check Logs for reconciliation information accounting for used check stock. Observed the Mainframe Print Center manager submit a file for printing and complete the OAKS Check Log with reconciliation information.	No exceptions noted.	

(WARRANT WRITING) - *Control Objective:* **Completeness and Accuracy of Accumulated Data** – All warrants and related adjustments are recorded in the entity's financial records.			***Control Objective Has Been Met***
Control Procedures:	*Test Descriptions:*	*Test Results:*	
Control totals and other reconciling information are confirmed by print center staff to provide for completeness and accuracy prior to OAKS payroll warrant file processing.	From the calendar of FY10 state payroll days, selected 10 payroll dates and inspected the corresponding e-mails for the HCM bi-weekly delayed, bi-weekly currents, current monthly, or monthly advanced files that were submitted by the HCM support staff to the mainframe print center indicating he payroll warrant files were waiting in the print queue. Confirmed reconciliation procedures with the Mainframe Print Center manager and observed the manager submit a file for printing.	Control operating as described.	

<table>
<tr><td colspan="2"><b>(WARRANT WRITING) -</b> <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data</b> – All warrants and related adjustments are recorded in the entity's financial records.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>DAS print center management reviews the OAKS Financials Report Log prior to submitting a print job to prevent duplicate print runs.</td><td>Observed the Mainframe Print Center manager submit a job for print. Inspected the Log to confirm it was updated with the information from the print job after submitting the job for print and after the printing was complete.
In addition, inspected the OAKS Financials Report Log for FY 2010.</td><td>Control operating as described</td></tr>
<tr><td>Post printing confirmation is communicated to OAKS FIN/HCM support staff by the Office of State Printing and Mail Services to reconcile and validate the print jobs.</td><td>Selected ten payroll dates from FY10 and inspected the corresponding e-mails for the HCM bi-weekly delayed, bi-weekly currents, current monthly, or monthly advanced files that were submitted by the Mainframe Print Center Staff to the HCM Support Staff.
Inspected example post-print e-mails for the FIN cut and roll print jobs that were submitted by the Mainframe Printer Center to the FIN Support Staff.</td><td>Control operating as described.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>(WARRANT WRITING) -</b> <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data</b> – All warrants and related adjustments are recorded in the entity's financial records.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td><i>Test Results:</i></td></tr>
<tr><td>DAS Fulfillment Service Job Logs are completed and used by DAS management to account for the disposition of warrants during transport from the print section to the fulfillment area for cutting and stuffing into envelopes.</td><td>Selected 30 dates from FY10. Obtained the OAKS Warrant Logs and inspected the corresponding OAKS Check Logs (records how many warrants were printed) and OAKS Fulfillment Service Job Logs to determine they contained reconciliation information accounting for the printed checks. Fulfillment Logs record the number of checks cut and stuffed into envelopes for mailing. In addition, compared the Fulfillment Log information to the OAKS Check Logs for reconciliation.

Also, observed the Mainframe Print Center manager submit a file for printing, complete the OAKS Check Log with reconciliation information, transfer the checks to the fulfillment section, and then complete the Fulfillment Service Job Log.</td><td>No relevant exceptions noted.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>(WARRANT WRITING) -</b> <i>Control Objective:</i>
<b>Completeness and Accuracy of Accumulated Data</b> – All warrants and related adjustments are recorded in the entity's financial records.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>Voids are stamped and accounted for by the print center manager and stored in a secure location until destruction.</td><td>Selected 10 payroll dates from FY10 and inspected the corresponding OAKS Check Logs for evidence of the Mainframe Pint Center manager's signature and information relating to any voided checks created by the print job.
Obtained the OAKS Warrant Logs for FY10 containing summaries of all print jobs and selected 30 dates. Inspected the corresponding OAKS Check Logs for evidence of the Mainframe Print Center manager's signature and information relating to any voided checks created by the print job.
Observed the Mainframe Print Center manager submit a file for printing, complete the OAKS Check Log with reconciliation information, stamp any damaged or blank check stock with the "void" stamp, and then transfer the checks to the locked cage at the print facility.
Inspected the shred log for FY10 to confirm it contained a listing of all warrants to be shredded.
Observed the shred process completed by the print center manager and the OBM representative.</td><td colspan="2">Control operating as described.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>(WARRANT WRITING) -</b> <i>Control Objective:</i>
<b>Restricted Access to Assets, Records, Programs and Data</b> – Only authorized personnel have access to manual and electronic records and unissued checks.</td><td><b><i>Control Objective Has Been Met</i></b></td></tr>
<tr><td><i>Control Procedures:</i></td><td><i>Test Descriptions:</i></td><td colspan="2"><i>Test Results:</i></td></tr>
<tr><td>OAKS warrant file datasets on the OIT mainframe are protected from unauthorized access.</td><td>Obtained a list of the OAKS warrant file datasets on the OIT mainframe. Inspected the logical access rights on the corresponding RACF security reports (LISTDSDs) for each dataset and confirmed the appropriateness of the listed accounts with the Mainframe Print Center programmer specialist.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Access to the print facility where all the OAKS warrants and State checks are stored, printed, and processed, is restricted to authorized DAS Office of State Printing and Mail Services personnel.</td><td>Inspected the list of users with access to the print facility. Confirmed the appropriateness of access for the listed users with the Mainframe Print Center managers, Fulfillment supervisor, and the DAS manager of safety and security.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>Physical access to all the voided RTA warrants before they are destroyed or returned to OBM is restricted to authorized DAS mainframe print center management.</td><td>Inspected a listing of users with the combination to the locked cage and confirmed the appropriateness of the access for the listed users with the Mainframe Print Center manager.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>The blank check stock is stored in a physically and environmentally secure warehouse cage at the print facility.</td><td>Physically inspected the blank check stock inventory at the print facility.
Also, toured the cage area where the inventory was stored and observed the physical access and environmental controls.</td><td colspan="2">No exceptions noted.</td></tr>
<tr><td>The blank check stock inventory is maintained by the mainframe print center manager using an inventory listing sheet.</td><td>Inspected the Inventory Listing of the blank check stock ordered from July 2009 through June 2010.
Re-performed the control by comparing the physical check stock inventory to the inventory listing.</td><td colspan="2">No exceptions noted.</td></tr>
</table>

Mary Taylor, CPA
Auditor of State

STATE OF OHIO SAS-70
OAKS HUMAN CAPITAL MANAGEMENT (HCM) & FINANCIALS (FIN)
WARRANT WRITING AND EFT

FRANKLIN COUNTY

CLERK'S CERTIFICATION

This is a true and correct copy of the report which is required to be filed in the Office of the Auditor of State pursuant to Section 117.26, Revised Code, and which is filed in Columbus, Ohio.

Susan Babbitt

CLERK OF THE BUREAU

CERTIFIED
OCTOBER 14, 2010