The State of Colorado Governor's Office of Information Technology

Report on controls placed in operation and tests of operating effectiveness

July 1, 2009 – June 30, 2010

Ernst & Young

Quality In Everything We Do

LEGISLATIVE AUDIT COMMITTEE
2010 MEMBERS

Senator David Schultheis
Chair

Senator Lois Tochtrop
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Frank McNulty
Representative Dianne Primavera
Representative Joe Miklosi
Senator Shawn Mitchell

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan C. Trull
Legislative Audit Manager

Ernst & Young LLP
Contract Auditors

Report on controls placed in operation and tests of operating effectiveness

Statement on Auditing Standards (SAS) No. 70

Table of Contents

1 Glossary of Acronyms

Acronym	Definition
ACID	Access ID
ACS	Access Control Servers
ADS	Applicant Data System
ASEC	Agency Security Table
ATL	Automated Tape Library
C2P	The Colorado Consolidation Plan
CDHS	Colorado Department of Human Services
CDLE	Colorado Department of Labor and Employment
CDOT	Colorado Department of Transportation
CFO	Chief Financial Officer
COBOL	Common Business-Oriented Language
COFRS	Colorado Financial Reporting System
CPP	Control Processing Procedure
CPPS	Colorado Personnel Payroll System
CTO	Chief Technical Officer
DF	Data Facility
DLT	Digital Linear Tape
DOR	Department of Revenue
DPA	Department of Personnel & Administration
FDW	Financial Data Warehouse
FTE	Full-time Equivalent
GB	Gigabyte
GFS	Government Financial System
HRDW	Human Resources Data Warehouse
HSM	Hierarchical Storage System
IBM	International Business Machines
ISOC	Information Security Operations Center
JCL	Job Control Language
KVM	Keyboard, Video Mouse switch
MIPS	Million Instructions per Second
MNT	Multi-Use Network
MVS	Multiple Virtual Storage
OCS	Office of Cyber Security
OIT	Office of Information Technology
OS	Operating System
PDU	Power Distribution Unit
SAN	Storage Area Network
SAS	Statements on Auditing Standards
SMF	System Management Facility
SMS	Storage Management System
SOP	Standard Operating Procedure
STATE CIO	State Chief Information Officer
TB	Terabyte
TMU	Technology Management Unit
TSS	Top Secret Security software
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
VSAM	Virtual Sequential Access Method
VTS	Virtual Tape Subsystem

SECTION ONE: REPORT OF INDEPENDENT AUDITORS

Ernst & Young LLP
Suite 3300
370 17th Street
Denver, Colorado 80202-5663
Tel: +1 720 931 4000
Fax: +1 720 931 4444
www.ey.com

Report of Independent Auditors

Legislative Audit Committee Members
Governor's Office of Information Technology

We have examined the accompanying description of controls relative to selected services provided by the Governor's Office of Information Technology (OIT) related to processing activities as they apply to the Colorado Financial Reporting System (COFRS) and the Colorado Personnel and Payroll System (CPPS) applications and their related interfaces to the Financial Data Warehouse (FDW), Document Direct, Human Resources Data Warehouse (HRDW) and KRONOS applications. In addition, our examination procedures included general controls as they apply to the OIT server hosting and housing services. Our examination procedures did not include Information Technology (IT) general control procedures over the applications that interface with COFRS and CPPS. Our examination included procedures to obtain reasonable assurance about whether: (1) the accompanying description presents fairly, in all material respects, the aspects of OIT's controls that may be relevant to a customer organization'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 customer organizations applied the controls contemplated in the design of OIT's controls; and (3) such controls had been placed in operation as of June 30, 2010. The control objectives were specified by the management of OIT. 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 controls presents fairly, in all material respects, the relevant aspects of OIT's 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 customer organizations applied the controls contemplated in the design of OIT's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section Three, to obtain evidence about their effectiveness in meeting the related control objectives, described in Section Three, 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 Three. This information has been provided to user organizations of OIT and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

OIT states in its description of controls that it has controls in place to restrict security administrator access for the mainframe to limited authorized individuals and that logs are reviewed periodically to identify and investigate unusual items. Our tests of operating effectiveness noted that controls around restricting administrator access for the mainframe Top Secret environment and log reviews were not performed during the year in accordance with the

OIT's policy. This resulted in nonachievement of control objective 11: "Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of their systems."

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

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

The description of controls at OIT is as of June 30, 2010, and information about tests of the operating effectiveness of specific 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 OIT 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 changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

This report is intended solely for use by the Members of the State of Colorado Legislative Audit Committee and management of OIT, its customer organizations and the independent auditors of its customer organizations. This restriction is not intended to limit distribution of this report which, upon release by the Legislative Audit Committee, is a matter of public record.

Ernst & Young LLP

September 14, 2010

2 Report Summary

Authority, Purpose and Scope

The Office of the State Auditor engaged Ernst & Young LLP to conduct a Statement on Auditing Standards (SAS) No. 70 examination of the Colorado Governor's Office of Information Technology's (OIT's) Data Center controls. The examination was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct audits of all departments, institutions and agencies of state government. This examination was performed in accordance with the American Institute of Certified Public Accountants' SAS No. 70, *Service Organizations*.

We have examined the accompanying description of controls relative to selected services provided by OIT related to processing activities as they apply to the Colorado Financial Reporting System (COFRS) and the Colorado Personnel and Payroll System (CPPS) applications and interfaces. In addition, our examination procedures included general controls as they apply to the OIT server hosting and housing services. Our examination procedures did not include Information Technology (IT) general control procedures over the applications that interface with COFRS and CPPS. Our examination included procedures to obtain reasonable assurance about whether: (1) the accompanying description of controls presents fairly, in all material respects, the aspects of OIT's controls that may be relevant to a customer organization'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 customer organizations applied the controls contemplated in the design of OIT's controls; and (3) such controls had been placed in operation as of June 30, 2010. The control objectives were specified by the management of OIT.

Summary of Major Findings and Recommendations

A complete listing of our findings, recommendations and management's responses may be found in Section Three of the report. Additionally, a summary of progress in implementing prior recommendations from the Office of the State Auditor's 2008 Information Technology Audit of OIT's Data Center and the prior SAS 70 can be found in Section Four.

It should be noted that in several instances, the recommendations are the logical result of an exception noted during our testing.

The following summarizes the significant findings contained in the report:

Top Secret Logical Security. Two users maintained inappropriate administrator level access within Top Secret out of a total population of 27 administrators. We determined that these two users' access privileges are inappropriate based on our evaluation of the annual Top Secret review. Additionally, four administrators have excessive administration rights to certain profiles and facilities within Top Secret. These excessive rights were identified by the data center operations manager during her annual Top Secret user review. However the suggested access changes identified during the annual review were not implemented leading to inappropriate administrator access. Failure to restrict administrative rights to Top Secret leads to unauthorized

administrator access to the mainframe supporting COFRS and CPPS. We recommend that OIT review administrative access to Top Secret on a periodic basis and take the necessary steps to restrict administrator access on the mainframe to authorized individuals.

Top Secret Logical Security. OIT is not consistently following the established process for adding or modifying user accounts on the mainframe. Specifically, documentation for two out of a total population of three new user access requests/changes sampled was not entered in the Remedy ticket system and maintained by OIT as required. Additionally, an Agency Security Administration (ASA) form was not completed for any of the three new users added this year as required by OIT policy. Furthermore, no evidence of the required signed Statement of Compliance was found for one out of three new users added to the system. Failure to maintain documentation authorizing account creation and modification could result in a person gaining unauthorized access to systems or data. We recommend that OIT consistently follow the process established to document and maintain documentation related to the creation and modification of mainframe user accounts using the Remedy ticket system.

Top Secret Logical Security. Security profile change logs have not been reviewed in a timely manner for Fiscal Year 2010. Specifically, security log violations for Top Secret have not been reviewed since September 2009. A periodic review of the security violation logs and security profile change logs helps in identifying any attempts made by users to gain unauthorized access to Top Secret. We recommend that OIT review Top Secret log violation reports and security profile change logs on a periodic basis to identify and investigate unusual activities or violations.

Logical Access to COFRS. The OIT Controller had the ability to establish user access in the COFRS financial system as part of the new user access process until November 2009. Since the OIT Controller is an approver of access and has the ability to set up users, there is a lack of segregation of duties in the access control process. Between July 2009 and November 2009 the OIT Controller established access for two out of the three users, who were granted new access to the COFRS application during the audit period. The OIT Controller also performs an annual review of all COFRS users. Typically the person performing a review of users' access in COFRS should not have the ability to add/modify/delete users in the COFRS application. We recommend that OIT segregate responsibilities for approving, establishing and reviewing user access rights within the COFRS financial system.

Server Hosting. A System Administrator maintained the administrator password for a customer web server in clear text and within plain view at OIT's headquarters. The server name, administrative login ID and password were readily visible to other staff. Also, password security controls were not enforced for this server. Per inquiry of management, this web server was hosted by OIT on behalf of the Department of Higher Education and no confidential data exists on the server. The web pages and content on the server are public information. We recommend that OIT develop practices to enforce password security on servers hosted for customer agencies and maintain control around the confidentiality of administrator passwords.

Organization and Administration. Standard Operating Policies and Procedures were not regularly reviewed and updated for the fiscal year. Furthermore, an organizational chart describing the various functional departments and job hierarchy was not published. An updated organizational chart and policies and procedures help guide the organization in following standard operating procedures. The lack of a published organizational chart and outdated

policies reduces accountability and responsibility across the organization. We recommend that OIT improve its IT governance procedures by updating its policies, procedures and organizational chart annually.

3 Recommendation Locator

RECOMMENDATION LOCATOR

Rec No.	Page No.	Recommendation Summary	OIT Response	Implementation Date
1	75	We recommend that OIT improve the logical security over the mainframe by: a. Consistently following established controls and standard operating procedures designed to enforce logical security for Top Secret. b. Establishing a dedicated resource to perform Top Secret administration duties. c. Reviewing administrative access to Top Secret on a periodic basis and taking the necessary steps to restrict administrator access on the mainframe to authorized individuals. d. Consistently following the process to document and maintain documentation related to the creation and modification of mainframe user accounts using the Remedy ticket system. e. Reviewing Top Secret log violation reports and security profile change logs on a periodic basis to identify and investigate unusual activities or violations.	Although controls were developed and had been previously working effectively, OIT did experience an operational and transitional gap in services and systems administration from September 2009 to August 2010. The gap in essential support services and access control administration was due to the unanticipated resignation of the primary system and security administrator in September 2009 and the operational realignment of the secondary system and security administrator during a recent layoff and restructuring initiative that occurred at OIT in October 2009. On July 1, 2010, 900 employees were consolidated within OIT. As part of that restructuring, OIT has implemented an Access Control Section which in addition to other duties has the responsibility for long-term administration and access control functions for Top-Secret and the related control functions identified above. The Access Control Section consists of approximately 15 information technology professionals and this depth will provide for succession planning and program coverage. While there was a gap in this particular control for the time period noted, this is not the only control in place to prevent security violations and breaches. To prevent unauthorized access, each application in the mainframe environment has its own application security and each department has both an application security, administrator and a Top Secret security administrator. In addition, there are business side controls, such as payroll reconciliations and expenditure review and approval in each of the departments, as well as cash reconciliation within the Department of Treasury and vendor control within the Office of the State Controller. All of these controls work in conjunction to mitigate the state's risk. To ensure that these additional controls were in place during the above-noted time period, OIT reviewed compensating controls and activity logs for the period to ensure that no unauthorized access occurred.	Implemented

RECOMMENDATION LOCATOR

Rec No.	Page No.	Recommendation Summary	OIT Response	Implementation Date
2	76	We recommend that OIT develop practices to enforce password security on servers hosted for customer agencies and to maintain control around confidentiality of administrator passwords.	The OIT Office of Cyber Security has worked with the server management team to address the issue of keeping passwords written on paper and to ensure that the current server team password vault solution is being used to maintain and protect the administration credentials of State servers. In addition, the Office of Cyber Security has procured a state-wide license for the Center for Internet Security (CIS) hardening benchmarks to be used as the State security standard for operating systems, network devices and applications. The Office of Cyber Security is currently working with the OIT CTO's office on the socialization and implementation of the CIS standards across all State systems.	Implemented
3	77	We recommend that OIT improve its IT governance procedures by updating its policies, procedures and organizational charts annually.	OIT is reviewing all Standard Operating Procedures (SOP) related to data center operations and updating them to reflect the effects of consolidated staff and operations. An updated organization chart has been published to the OIT Intranet site, which is accessible by all employees.	July 2011

SECTION TWO: DESCRIPTION OF CONTROLS PROVIDED BY OIT

1 Scope of this Report

The following description is intended to provide customers, such as state agencies, and their independent auditors with information about the control activities of the OIT Data Center. The controls described include certain IT general controls that support the delivery of OIT processing activities, including a review of the general and application controls as they apply to the COFRS and CPPS applications and related interfaces. In addition, our procedures include a review of the general controls as they apply to OIT's server housing and hosting services in the Data Center in Lakewood, Colorado. This report does not encompass IT general control reviews over the applications that interface with COFRS and CPPS.

The following description is intended to provide sufficient information for such customers and their independent auditors to obtain an understanding of the controls in place over OIT's Data Center services to plan their audits. The description has been prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants' SAS No. 70, *Service Organizations*, and SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*.

2 Overview of OIT Data Center

The Data Center is vital to state operations and houses critical applications that make it possible for state agencies to provide efficient and effective services to people living and conducting business in Colorado. The Data Center supports several statewide financial applications used commonly by all state agencies, including COFRS and CPPS. For Fiscal Year 2009, the Data Center received an appropriated spending authority of approximately $54 million and 607 full-time equivalents (FTE) to provide computer services to state agencies.

The Data Center, formerly known as the General Government Computer Center, has 9,075 square feet of raised floor space containing the computer room, the server farm, office space and print distribution areas. The purpose of the Data Center is to perform services for state agencies that are its customers, including computer processing, maintaining system software, statewide telecommunications, networking, server hosting, secure housing for customer-owned server and network equipment and disaster recovery planning. The Data Center operates 24 hours per day, 7 days per week, including holidays.

3 Overview of OIT Data Center Services

Services performed for state agencies include computer processing, maintaining system software, processing of computer output, statewide telecommunications network, server hosting, secure housing for customer-owned server and network equipment and ensuring that the hardware and operating system can be recovered in case of a physical disaster at the Data Center.

Although the basic mission and objectives of the Data Center have not changed, the overall philosophy pertaining to the use of computer systems has evolved since the Data Center's creation in 1978. There has been a noticeable change in the type of services requested by Data Center customers. Traditional batch processing has predominately shifted to real-time

processing. In real-time processing, users have instant access to the computer through remote terminals connected to the Data Center's computer via telecommunications lines. This change to real-time processing places a greater demand on the Data Center's systems.

Real-time processing helps provide more timely and accurate data and also reduces costs associated with creating and maintaining computer-stored data. Errors are usually detected at the source, where those most knowledgeable about the data can make corrections promptly. Thus, the state saves the time and costs associated with making corrections. Also, in some cases, real-time processing reduces the personnel costs associated with the update and maintenance of data on the computer system. Providing real-time processing to OIT customers resulted when the Data Center installed and made available high-level programming software packages that are more adaptable and easier for non-IT personnel to use.

The change to real-time processing has also brought about a change in the types of customers using the computer system. Managers, statisticians, research analysts, accountants, clerks and others have ready access to the computer system to enter, update, change and query information.

Additionally, customers are requesting that the Data Center expand its services beyond the realm of mainframe processing. Customers expect the Data Center to coordinate and facilitate the acquisition and support of computing power regardless of whether the requirements are for mainframe or mid-range processors. Customers would like to access resources from the Data Center on an as-needed basis to provide application programming support, training and new technology expertise.

The Data Center houses the state's mainframe for traditional legacy systems. It also houses a growing number of servers for state agencies. Customers are able to utilize the secure and highly available physical infrastructure of the Data Center and manage their mid-range server platforms themselves or turn over varying levels of control and responsibility for their servers to the Data Center. The Data Center has expanded its services well beyond the realm of mainframe processing by coordinating and facilitating the acquisition and support of server-class computing resources. Data Center customers can now receive client-server infrastructure support, web-based application development assistance and new technology consulting.

Customers continue to rely heavily on the Data Center to deliver traditional database processing, online access, tape and disk storage and printing services. The Data Center is housed in a secure facility with 24 hours per day, 7 days a week on-site staffing for Operations Control Center personnel. Additionally, the Data Center is equipped with environmental controls such as fire suppression systems, uninterruptible power supply (UPS), generator backup and space for additional equipment.

4 Description of Services Provided

OIT General Services

OIT offers services to state agencies in an effort to consolidate the activities of multiple agencies into one environment. The **OIT Operating System (OS) Technical Support and Software Support teams** offer mainframe application hosting services and provide the platform where many of the statewide applications run. These teams maintain reasonable currency of the mainframe system and software and apply appropriate patches or upgrades to that environment. This is accomplished by evaluating the patches and upgrades (changes) to the operating system supplied by IBM on a regular basis. These changes may or may not be relevant to the specific configuration of the OIT OS. Therefore, it would not be reasonable for OIT to implement some of these changes even though they are available. It would be reasonable to implement changes that fix an identified problem or to effect changes that improve the efficiency of the configuration. These changes might also be delayed (and therefore not current) while implementation is coordinated with OIT customers. The same holds true for software support on the mainframe. This is common practice in the mainframe environment.

The **Computer Operations team (Computer Operations)** maintains the mainframe hardware and peripherals, prints mainframe reports, provides mainframe tape handling and monitors the mainframe system and batch processing. Some of the statewide applications run on open systems platforms that are supported by the Server Management team as part of its server hosting service. Computer Operations monitors the computer rooms' environmental health and works with the Department of Personnel & Administration's (DPA) Capitol Complex building maintenance team to maintain a computer-friendly environment for hosted and housed servers. Computer Operations is also responsible for provisioning power from the Power Distribution Unit (PDU) for use by customers wishing to house servers at the Data Center. All other aspects of the housed servers are the responsibility of the customer.

The **Server Management team** provides and maintains the hardware and operating systems for servers hosted at the OIT Data Center, while customers maintain their own applications on these hosted servers.

The **Storage Management group** provides data storage and management services to customers using the mainframe and hosted servers. Customers housing servers at the Data Center are responsible for their own storage needs.

Statewide application services are provided by OIT for those applications that are used commonly among all state agencies. These applications are COFRS; the Financial Data Warehouse (FDW), a research and reporting tool for COFRS information; KRONOS for tracking timekeeping and leave for state employees; the Applicant Data System (ADS) used to track state job applicants and the application process; CPPS; and the Human Resources Data Warehouse (HRDW) used to maintain current and historical employee information. Document Direct is supported by a software support group and provides online report viewing for customer-identified mainframe reports.

While many state departments and agencies utilize OIT services, the major customers are the Colorado Department of Human Services, the Department of Revenue, DPA and the Colorado Department of Labor and Employment (CDLE). These departments make use of all Data Center services with one exception; CDLE does not utilize OIT's server hosting or housing services.

Mainframe Application Hosting

The mainframe hardware and software provide an environment for state agencies to access statewide applications as well as some of their own individual applications. The OIT OS Technical Support and Software Support teams have managed, operated and maintained an IBM z9 BC Enterprise Server with Integrated Facility for Linux (IFL) since March 2008. The z9 BC, rated at 500 Million Instructions per Second (MIPS), runs the z/OS 1.10 operating system in one partition and VM/Linux in the other partition, and has 8 gigabytes (GB) of memory.

In addition, the IFL component provides the facility by which multiple distributed system servers can be aggregated into the architecture without acquisition of additional physical servers. Together, the IBM z9 BC and the IFL allow personnel to implement an Enterprise Server (mainframe) architecture that continues to provide support for aggregated legacy mainframe processing while supporting aggregated distributed system processing. The z9 BC Enterprise Server allows for usage-based billing from IBM. All OIT data, programs and documentation necessary to restore system files are stored off-site.

Security for the mainframe data is managed by the Information Security Operations Center (ISOC) using Top Secret Security (TSS) software. Customers are also given rights in TSS for administering access to their data for their agency personnel. Each agency has access to only its files, unless access to other files is specifically permitted by another agency's administrator.

Server Housing and Hosting

Server hosting is a service that has grown and will continue to grow as state agencies choose to contract with OIT to perform the care and maintenance of their servers in the Data Center server farm. The Server Management team has responsibility for implementing and maintaining the hardware and operating systems for servers hosted at the OIT Data Center. OIT is implementing server consolidation options through platforms such as Linux under z/VM and VMware for Intel platforms in an effort to reduce costs by utilizing shared resources for these server instances. The OS Technical Support team creates and implements virtual server instances in the Linux environment under z/VM. The Server Management team manages virtual servers on VMware. The Data Center provides a range of server support levels ranging from server housing (limited to providing floor space, power, and network connections only) to full service hosting (complete operating system, hardware and application package installation). To support its growing server hosting service, the Data Center has invested in Storage Area Network (SAN) technologies, enterprise-class backup solutions such as dedicated backup infrastructure and automated tape libraries and effective physical support features such as Keyboard Video Mouse (KVM) switches, multiple-zoned power feeds, protective racks and cabinets.

OIT leases an EMC DMX1000 SAN [4 Terabytes (TB)] and owns an EMC DX300 SAN (9.5 TB). In addition, on some Windows and Unix servers, disk storage needs are met via local disk.

Mainframe disk storage is managed using IBM's SMS/HSM software along with Computer Associates CA-1 tape library management software.

Tape storage for the mainframe is provided by the following:

- Ten – 3480 18-track cartridge drives and an inventory of 21,000 tapes
- Ten – 3590 (Magstar) drives serviced by an automated tape library (ATL) containing 2,750 tapes
- Sixty-four – Virtual tape subsystem (VTS) logical drives with 630 Magstar backstore tapes

The tape media supports archival, batch processing, disaster recovery and customer off-site data storage needs.

Mainframe tape management, including vault management, is handled by CA-1. In-house written routines invoke CA-1's expiration and scratch features to enforce locally defined policies. Server tape management is handled by a combination of manual methods for some servers and by catalog/repository for Symantec Netbackup-managed servers.

Tape storage (backup) for distributed systems is provided by a Quantum M2500 Digital Linear Tape (DLT) ATL. Numerous other servers have on-board (local) tape devices used for backup. The tape media supports disaster recovery and file restoration services.

A Quantum DX30 ATL supports distributed tape storage activities. Symantec NetBackup is used to manage open system backup tasks.

Computer Operations

Computer Operations is responsible for monitoring hardware and the Data Center environment in support of all OIT services and customers. Computer Operations ensures that individuals entering the computer rooms follow the OIT access procedures. This group also provides print and tape handling services, report distribution, and warehouses print forms for Data Center customers. Computer Operations supplies power resources to server housing customers by arranging the purchase and installation of power cables from Data Center PDUs to designated customer locations under the raised floor. The Operations Control Center within Computer Operations is the single point of contact for customers. The Operations Control Center provides an after-hours service desk, job scheduling and monitoring, and systems monitoring for OIT and its customers.

Security

The ISOC performs several security functions, including perimeter security at the Internet Gateway, mainframe security through the use of TSS software, incident response, change processing through Security Variance Requests, systems administration of security devices and monitoring of the Multi-Use Network (MNT) traffic. Perimeter security is performed at the Internet Gateway through the use of two Enterprise firewalls. The ISOC works in conjunction with a vendor to monitor the MNT 24 hours a day, 7 days a week (24x7) through the use of intrusion detection systems and firewall log files.

The ISOC utilizes an advisory procedure to alert agencies and some non-state governmental entities of suspicious traffic and incidents on the MNT and provides coordination services, forensic services and expertise for research and eradication of malicious code and traffic. Mainframe user access as well as access to datasets is controlled through TSS administration.

Desktop security for OIT is managed by OIT's Desktop Support team.

Statewide Applications

CPPS is the payroll system for the State of Colorado. This system was purchased from Integral Systems, Inc. in 1984 and has been modified to meet the rules and procedures for the state, including a benefits subsystem for reporting insurance premiums. CPPS is currently supported by OIT for system modifications and vendor-supplied software updates.

CPPS was developed in the COBOL language using Virtual Sequential Access Method (VSAM) file structures. Ad hoc reporting is accomplished using the FOCUS programming language.

COFRS is the accounting system of final record used by the State of Colorado. All state agencies except the Colorado Department of Transportation (CDOT) and higher education institutions use COFRS directly to perform their day-to-day accounting functions. CDOT and higher education institutions have implemented their own accounting systems but interface summarized accounting information to COFRS.

The original purchase of COFRS was supported by the State Auditor's Office, which needed one auditable system to replace the many different departmental systems in place at the time. COFRS was also supported by the Office of the State Controller as a single source of data for the statewide financial reports.

The application (GFS) software of COFRS is implemented on the mainframe in COBOL. It uses a VSAM file structure. The CORE software (database and file handling routines) of COFRS is implemented in a mixture of assembly language and COBOL.

5 Relevant Aspects of the Internal Control Environment

Organization

As of July 1, 2009, OIT officially became responsible for the operations of the state's Data Center, which was previously under the Department of Personnel and Administration. OIT, organizationally located within the Governor's Office, is led by the State Chief Information Officer (State CIO), who is appointed by the Governor.

OIT senior management have the primary responsibility to develop, maintain and document adequate internal controls within the Data Center environment, including compliance with state and federal laws. A formal management organizational structure exists with appropriate levels of reporting and accountability. Assignment of responsibilities is made to segregate incompatible activities. All issues and problems are escalated to the appropriate management levels based on established procedures for resolution.

OIT's Chief Technical Officer (CTO) is responsible for Data Center operations and reports both administratively and operationally to the Deputy State CIO. Day-to-day management of the Data Center is the responsibility of the Computer Operations Manager.

Data Center operations groups are separated from network monitoring, system development and security groups. Approximately 60 full-time equivalents (FTE) are directly involved with Data Center operations. These FTE work within the following Data Center work groups or teams:

- **Computer Services Operating System (OS), Technical Support and Software Support Teams.** These teams offer mainframe application hosting services and provide the platform where many of the statewide applications run. These groups maintain and manage the mainframe system and software and apply appropriate patches or upgrades to that environment.

- **Computer Operations Team.** This team maintains the mainframe hardware and peripherals, prints mainframe reports, provides mainframe tape handling, and monitors the mainframe system and batch processing. Computer Operations monitors the environmental health of the Data Center's computer room and works with Capitol Complex to maintain a computer-friendly environment. Computer Operations also provisions power from the power distribution unit for use by customers wishing to house servers at the Data Center. The Service Center, administratively located within the Computer Operations Team, is the single point of contact for the Data Center's customers. The Service Center provides service desk support, job scheduling and monitoring, and system monitoring for the Data Center and its customers.

- **Server Management Team.** This team provides and maintains the hardware and operating systems for agency-owned servers hosted at the Data Center.

- **Storage Management Group.** This group provides data storage and management services to customers using the Data Center's mainframe and hosted servers. Customers housing servers at the Data Center are responsible for their own data storage needs.

- **Technology Management Unit (TMU).** The TMU provides statewide application services for those applications used commonly among all state agencies.

- **Information Security Operations Center (ISOC).** ISOC is responsible for the overall security of the Data Center and the State Multi-Use Network mainframe security provisioning through the use of Top Secret Security (TSS) software, incident response, change processing through security variance requests, systems administration of security devices and monitoring MNT traffic.

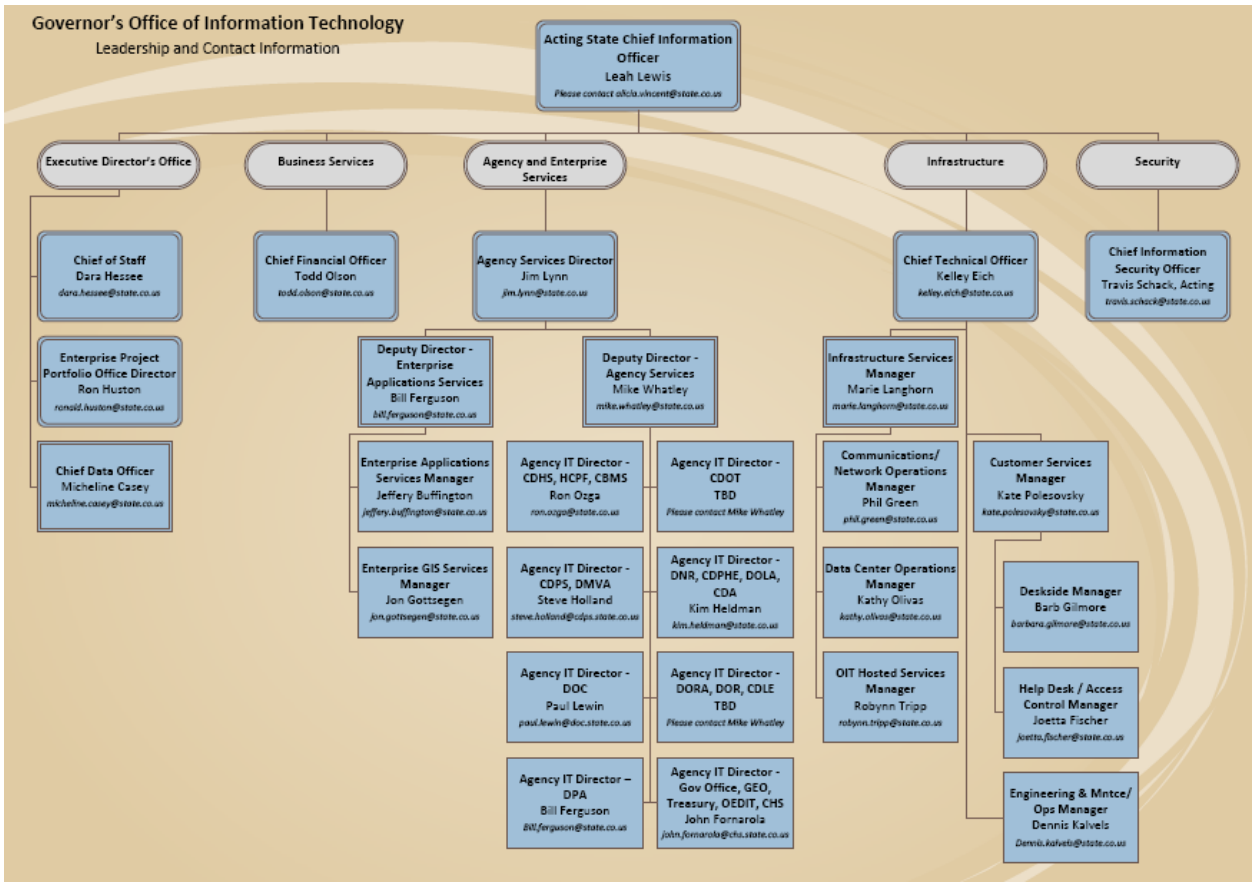
- **Business and Administrative Services Group.** This group provides business and administrative support services required to operate the Data Center. Services include budget preparation, accounting, personnel functions, word processing, and switchboard/receptionist services at the Data Center.

The Data Center is cash-funded by user agencies, which include more than 110 billable customers, such as state departments, institutions and agencies. Billable items include computer processing time, data storage space, printing charges and database support. Funds for these services are appropriated to each customer, with the Data Center receiving matching cash spending authority. For Fiscal Year 2009, the Data Center received an appropriated spending authority of approximately $54 million and 607 FTE to provide computer services to state agencies.

The Colorado Consolidation Plan (C2P) and its enabling legislation (Senate Bill 08-155) calls for a four-year consolidation and transformation of IT, led by the OIT. The effort officially started in 2008, and we are now halfway through the plan. The key achievements to date are: (1) reorganizing nearly 1,000 employees into a single chain of command; (2) implementing budget controls to ensure that purchases are managed in a coordinated fashion and are following our technology standards; and (3) implementing strict project management methodology and governance for state IT projects.

OIT Organization Chart

The following organization chart does not illustrate the entire OIT organization, but rather only those units specifically responsible for aspects of the Data Center and COFRS and CPPS applications.



Controls Related to Personnel

OIT has both classified and non-classified employees. State personnel rules and procedures are followed in all areas concerning the hiring, promotion, leave administration, annual performance management and termination of OIT employees. Additionally, orientation sessions are made available to all new employees. A checklist for new, promoted and transferred employees is utilized by the administrative staff to ensure assignment of proper user profiles for the various systems. A checklist for departing employees is utilized by the administrative staff to ensure deletion of user access for departing employees.

OIT employs a performance management program approved by DPA's Division of Human Resources (DHR) and requires semiannual reviews. Annual ratings for all employees are performed each April.

Employees are trained in accordance with job responsibilities and are informed of their respective responsibilities and duties through distribution of the organization chart and job descriptions when changes are made.

Risk Assessment

OIT management prepares strategic plans for IT that align business objectives with IT strategies by soliciting input from relevant internal and external stakeholders impacted by these plans. Management obtains feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process and monitors its progress against the strategic plan in meeting established objectives. IT plans are communicated to OIT customers and employees, and to the state's department Information Technology Directors. OIT senior management or their designees oversee the IT function and its activities and communicate its activities, challenges and risks on a regular basis to the State Chief Information Officer (State CIO), OIT's Executive Director.

OIT management identifies and analyzes risks relevant to achieving business objectives. The IT organization's risk assessment framework is used in the implementation of projects across the organization to ensure OIT's viability, reliability and ability to achieve business objectives. The IT organization's insurance and liability risk is managed at the state level by DPA.

Monitoring

OIT performs a variety of review, audit and inspection activities for quality control purposes. Management regularly reviews capacity and performance metrics. An annual TSS access review for Computing Services is completed by management each year to ensure that access to data remains appropriate for individual staff members at OIT. Annual reviews of Standard Operating Procedures (SOPs) against current operations are performed by the responsible manager and ratified by senior management. Major system outages are documented in Remedy (OIT's problem tracking system) and summarized in the Service Outage Notification Report, which is distributed to senior management on a monthly basis.

Information and Communication

OIT is responsible for managing all aspects of the system environment, ensuring that key systems and data have been inventoried and their owners identified. IT strategies and ongoing operations are formally defined and communicated to senior management and the state's department IT Directors. Formal job descriptions, called Position Description Questionnaires (PDQs), are kept for all OIT state employees. Each position and its relationships within OIT are described on an organizational chart that is kept current and made available to staff on the OIT intranet to ensure that employees understand their roles and have available to them the current organizational structure.

Significant IT events or failures such as security breaches or major system failures are reported to senior management. Contracted staff are subject to the same policies and procedures to assure the protection of OIT's and OIT's customers' information assets.

OIT holds staff meetings to communicate management goals and to provide a forum for communications between management and staff. Management communicates its activities, challenges and risks to the State CIO. OIT provides information externally to customers as appropriate.

Regularly scheduled staff meetings are used to share general project, organization, service level and service delivery information with employees.

Control Activities

Organization control, including the consistent application of entity controls, is addressed through the publication, maintenance and use of SOPs. SOPs are managed in accordance with OIT SOP #0001. SOPs are reviewed annually against current operations to ensure consistency and alignment with OIT business objectives. When SOPs are published, an email is sent to Computing Services staff notifying them of the updates.

OIT publishes OIT's Publication of Change Activities twice a week to ensure that agencies are aware of customer-affecting changes and planned outages. Customers will notify OIT if published activities need to be rescheduled or will have an unanticipated negative impact on their operations.

6 Description of IT General Controls

Physical and Environmental

The Data Center is housed in a secure facility with 24x7 on-site staffing for operations and Service Center personnel plus environmental controls, fire suppression system, Uninterruptible power supply (UPS) system, generator backup and space for additional equipment.

The Data Center computing facility is composed of three areas: the print/distribution room, the computer/server room and the telecommunications room. Trilogy locks are used to secure the print/distribution and the computer/server room areas, as well as the vault room where warrant stock is stored and managed. Unique access codes for this system are assigned to individuals who report to work in these rooms and other OIT staff who frequently enter the rooms on a daily basis in execution of their normal duties. The telecommunications room uses a Cipher lock system. When an employee terminates, they are deleted from the Trilogy lock system. Additional changes or deletions can also be made at management's discretion. Employees are entered into the Trilogy lock system for only those areas for which they are authorized.

All visitors to the Data Center must enter the building through the front entrance and pass through two secured staging areas that are controlled by building reception. All building entrances are controlled by a Hirsch scramble pad access system used only by employees. Visitors must check in with reception to pass through the staging areas and must complete the roster with their name, time in and who they are seeing. Visitors must be escorted at all times, unless granted specific permission for unsupervised admission, and are assigned badges that they must wear while in the building. Badges must be turned in before leaving the building, and visitor time out is recorded on the roster. All employees must also wear badges while in the

building. There are standard procedures for accepting and transferring materials into and out of the Data Center.

The Data Center has a generator alternate power source that is connected and operational on the Data Center's power grid. The Data Center has a UPS system to support the Data Center's raised floor equipment that ensures continuous availability of electrical power between the initial interruption of power and the standby generator coming online. The technical support and administration area is provided with power outlets (for desktop computers) that are connected to the UPS/generator backup power supply. The raised floor environment is adequately controlled with eight high-capacity air conditioning units and three humidifiers. The Data Center is equipped with an FM-200 gas fire suppression system. The FM-200 system is inspected semiannually and annual training is provided to the Computer Operations staff on the FM-200 system and on the operation of portable fire extinguishers. Smoke detectors are located above and below the Data Center's raised flooring and directly linked to the FM-200 system. Below-floor water detection devices are located throughout the raised floor area. The temperature and humidity in the Data Center are monitored by the Computer Operations staff. The Data Center staff also monitors the building cameras for unfamiliar or unusual activity after normal business hours. State Capitol Complex Facilities is the custodian for the Data Center building, located in Lakewood, Colorado. The custodian provides central maintenance of the building, including the fire alarms, UPS and generator systems and all cooling facilities. The fire alarms are monitored by the local fire department, which will respond if an alarm is activated.

Software and Technology Acquisition Management

Acquisition of new software and hardware requires business justification and manager approval. The Data Center will request funding for software products only when multicustomer interest is evident. System software is obtained through competitive bid, Request for Proposal (RFP) or formal sole source processes, assuring acquisition from a reputable software development company and proven product reliability.

Acquisition of new technology requires business justification and manager approval to ensure that platforms are appropriate to support existing or new applications. Capacity and performance of Data Center computer resources are actively tracked and recorded through the ongoing, real-time usage of the System Management Facility (SMF). Tracking options are selected to appropriately track system data to monitor the effective and efficient utilization of the computing system on behalf of the customers' application workload. SMF data are captured and retained in order to support historical analysis and reporting, as well as to generate future utilization projections. Management regularly reviews capacity and performance metrics. Certain information is put in graphical and other more readable formats and is made available to requesting customer agencies. Hardware acquisitions may include prepaid maintenance and support, or funds for renewal of maintenance and support that are encumbered prior to expiration.

Install and Test Technology Infrastructure

A formal change management system is used to control and document changes to system software. The methodology includes management assessment of the potential impact to client processing and authorization to proceed only by appropriate personnel. Once authorized to

proceed, system software modifications are thoroughly tested and approved before introduction into the production environment. Testing is accomplished through an independent test environment and test plans are used to functionally evaluate all system change modifications. There is a formal installation process for production software, which includes an implementation schedule that is published to the customers and affected clients, who are notified via email, telephone or broadcast message before a change is placed into production. Back-out procedures are written so that the system can be returned to its pre-implementation condition if necessary.

Documentation for installed system software products is available and current. During system software testing, conversion and implementation, documentation is generated, updated and archived appropriately. The installation process for system software includes a review/update of all associated documentation.

COFRS and CPPS Change Management

COFRS

Changes to COFRS go through a formal change management process, which includes documenting the change and control steps in a Remedy ticket, as well as in hard copy folders. This process consists of the following:

Upon identification of a needed change, the details of the change are entered into a Remedy ticket. The ticket is reviewed, and if authorized, the change is assigned to a developer.

In the production environment, there are libraries for source code and compiled code. Developers have read access to the production environment and upon authorization for a change, they copy the associated code objects from production to the development environment. Developers code and test the new change in the development environment. When the change is ready for review, a "last modified" date stamp and sign-off are attached to the source code object. The requestor or management reviews the change to validate that it is appropriate, and that it fixes the issue originally identified. If the change meets the end user's criteria, it is then approved for push into the production environment. The change is then assigned to the Move Coordinator for move-back into the production source code library. Once it has been moved, the source code is compiled by an analyst installing the new code in the functioning production environment.

The Development Supervisor has access to the production environment as a backup to the Move Coordinator. In order to mitigate the associated risks of a developer having access to the production environment, the Financial Systems Manager performs a monthly review of all changes made to the production environment and verifies that all changes are authorized and approved by mapping them back to approved Remedy tickets.

On a monthly basis, a release letter is sent to business and IT managers who are affected by changes to COFRS.

CPPS

Changes to CPPS go through a formal change management process, which includes documenting the change and control steps in a Remedy ticket, as well as in hard copy documentation. This process consists of the following:

> Upon identification of a needed change, the details of the change are entered into a Remedy ticket by the Manager HR/Payroll Systems. Changes are entered into the ticketing system only if they have been authorized by the Central Payroll Manager or the Manager HR/Payroll Systems. Separate development and production environments exist. Developers code and test the new change in the development environment. The change is then reviewed by the requestor for acceptance testing and approval for production. The requestor or management reviews the change to validate that it is appropriate, and that it fixes the issue originally identified. If the change meets the end user's criteria, it is then approved for push into the production environment.
>
> Production support personnel move the code into the production environment. The development manager also has the ability to move code into the CPPS production environment as a backup to the production support and maintenance teams.
>
> The Central Payroll Manager sends out notices for major changes to the agencies if the changes will impact them.

Mainframe Logical Security

Mainframe user access as well as access to datasets is controlled through TSS administration. The ISOC uses the Remedy ticketing system for all TSS changes. The System Security and Use SOP #8808 provides clear guidance regarding the responsibilities of TSS security administrators and the issuance of access permissions. The SOP requires that users be granted access only to those resources necessary and appropriate to each user's job duties. All Data Center, Technology Management Unit and Information Technology Unit employees receiving logical access to the mainframe are required to sign a compliance statement, referencing and acknowledging the computer usage and data security policy. Computer security information is also included in the SOP, which each employee is given to retain for personal reference. Security administrators are required to sign an additional statement of compliance referencing and acknowledging their responsibilities relative to TSS security administration. Agency security administrators are responsible for granting and revoking agency users' rights to the COFRS application.

The Service Center provides new personnel with access to mainframe software and datasets. New personnel receive a unique access identification (Access ID), temporary common password and minimum permission rights as directed by their supervisor based on their particular job level and responsibilities. Employees must change the initial password on their first login attempt or their account will be suspended. Future permission changes/enhancements require an email from the user's supervisor to the Service Center explaining the reason for the permission change. A checklist for departing employees is utilized by the administrative staff to ensure deletion of user access for departing employees. A checklist for new, promoted and

transferred employees is utilized by the administrative staff to ensure assignment of proper user profiles for the various systems.

TSS software is used to control access to all mainframe software and datasets. Permissions are defined by the user and controlled through login and password. TSS is configured to enforce adequate password controls, including minimum length, alpha and numeric character requirements, defined password expiration, minimum re-use of password generation and account suspension/lockout after minimum failed login attempts. Passwords are not displayed as they are input and are encrypted as they are stored.

TSS will disable an account if it is not used within six months and will automatically disconnect a login session if no activity occurs within a defined period. The Service Center can unlock and reset an account only after verifying a user's identity from INSTADATA (additional private information a user provides to the security administrator on account startup as a means to verify his or her identity). Security violations are logged and reviewed, and action is taken to investigate violations. Security profile changes are also logged and periodically reviewed, and any unusual items are investigated.

Logical Perimeter Security

Logical perimeter security is performed at the Internet Gateway through the use of two Enterprise firewalls. Changes to these firewalls are made by following an ISOC procedure that identifies change windows and approval for security variance and emergency changes. The ISOC administers the OIT/DPA Virtual Private Network (VPN) Concentrator and the OIT/DPA Access Control Servers (ACS), as well as the Internet firewalls. The firewall change request process is used to make any changes to the Internet firewalls or Data Center firewalls. This process includes data owner signatory authorities, risk assessment and ISOC signatory authority.

The ISOC works in conjunction with a vendor, GB Protect, to monitor the MNT through the use of Intrusion Detection Systems and firewall log files. The MNT is monitored 24x7 by the vendor, with on-call support from the ISOC. An advisory procedure is employed to alert agencies and non-state governmental entities of suspicious traffic and incidents on the MNT within their respective organization. The ISOC utilizes the Chief Information Security Officer's Incident Response Plan/Policy as a guideline for all incident response activities.

OIT IT components, as they relate to security, processing and availability, are well protected, prevent any unauthorized changes, and assist in the verification and recording of the current configuration. Only authorized software is permitted for use by employees utilizing OIT IT assets. System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, are properly configured to prevent unauthorized access.

IT management has implemented antivirus and antispam protection across OIT to protect information systems and technology from computer viruses. A biannual assessment is performed to confirm that the software and network infrastructures are appropriately configured. Additionally, key network and all security device configurations are monitored daily for any unauthorized changes via automated tools.

CPPS and COFRS Logical Security

CPPS

Access control for CPPS is largely managed by the Central Payroll Manager. In order to access CPPS, a user must have a valid Access ID as well as having been set up in CPPS itself. CPPS password settings are set to require at least one alphabetic character and one numeric character.

When a new user requires access to the system, he or she fills out a user request form, which must be approved by the user's manager. The form is then reviewed by the Central Payroll Manager prior to access being granted. Within OIT, the OIT Controller authorizes access requests prior to sending the request to the Central Payroll Manager. In the event of a termination, Human Resources notifies OIT of the separation, after which the CPPS administrators remove the user from the system. On a quarterly basis, the Central Payroll Manager sends out a listing of all users in the system to each agency for review. The OIT Controller reviews the list of users for OIT and verifies that they are all authorized for access to the system and notifies the Central Payroll Manager if any changes in access need to be made. Security administrative access in CPPS is defined as those who have been assigned the query ID of ALLUUU. Such access is restricted to authorized individuals.

COFRS

Access control for COFRS is managed in a distributed fashion by each agency. A security administrator is assigned in each agency and is responsible for setting up user access for his or her respective agency. In order to access COFRS, a user must have a valid Access ID, as well as having been set up in COFRS itself. Password configuration settings for COFRS are based on the mainframe.

Within OIT, when a new user requires access to the system, he or she fills out a user request form which must be approved by the user's manager. The form is then reviewed by the OIT Controller, who reviews and sets up access in the system based on the detailed access levels in the request. In the event of a termination, Human Resources notifies the relevant OIT unit or group of the separation, after which the COFRS administrators remove the user from the system. On an annual basis, a comprehensive review of access in COFRS is performed by the OIT Controller. Administrative access to COFRS is defined as those who have been assigned the following security groups: SECA, STAB, COFRS, or DPTS. Such access is restricted to authorized individuals.

Job Scheduling

Computer Associates scheduling software (CA7) is utilized to schedule the processing of batch jobs. TSS is used to restrict access to CA7 to appropriately authorized personnel only. Access to scheduling files is restricted to Service Center scheduling personnel (schedulers); customers have access to the scheduling software to schedule jobs for their agency only. Exceptions to normal operations are reported by schedulers and are published for management review via maintenance requests and Remedy tickets. The automated scheduling system ensures that batch jobs are run on a predetermined schedule and are tracked automatically. Where jobs are

irregularly scheduled, schedulers verify that jobs have completed and follow up with any further instructions. Batch jobs that do not run correctly are automatically entered into the system log and resolved by following the Control Processing Procedure (CPP). Internal jobs that have on-call personnel are entered into the problem management system (Remedy). Remedy helps to ensure that problems are recorded and tracked to appropriate resolution. External jobs that have on-call personnel have a maintenance request form that is completed by the schedulers and sent to the programmer; no Remedy ticket is opened.

Computer operators are restricted from discretionary use of the computer system, as schedulers control the scheduling and submission of computer application jobs; actions required from an operator during application processing are therefore minimized. All operator activities are recorded on the console log, and system processing is recorded on the System Management Facility (SMF).

Data Control within Computer Operations is responsible for report distribution. Reports are logged prior to distribution to users.

Problem and Incident Management

Incidents and problems are managed in accordance with SOP #8802. An incident/problem management system (Remedy) is used to record, track and resolve identified incidents and problems. Customers or OIT employees may report incidents or problems. Incidents or problems identified are immediately entered into Remedy; the details are described in the ticket, and the ticket is assigned to the appropriate technical work group. Individual assignment of tickets is made within the work group and corrective procedures are undertaken. Once corrective actions are verified as successful, the ticket is placed in "Resolved" status.

Customers do not have access to Remedy, but can inquire about the status of a ticket by contacting the Service Center. Unplanned outages related to incidents are managed in accordance with SOPs to ensure proper response, investigation and resolution. Service Outage Notification Reports are provided to management, and short- and long-term resolutions are reviewed.

Backup and Recovery

Several SOPs provide guidance regarding the processes and responsibilities for data storage and management. Data allocation of all z/OS/MVS disk datasets is controlled by IBM's Storage Management Subsystem (SMS) and assigned to a generalized pool of Direct Access Storage Device (DASD) volumes. All backup, archive and retention operations are governed by SMS parameters. All datasets are kept until they are either deleted from the catalog or expired. Exceptions are noted in SOP #8814. All datasets that are migrated to tape by SMS will be kept on-site until they are deleted from the catalog.

Dataset backup, archiving and space management is handled with the IBM software packages for DF/SMS/HSM [Data Facility (DF), Storage Management Subsystem (SMS) and Hierarchical Storage Management (HSM)]. The backed-up and archived datasets are recoverable at the disaster recovery site. Customers are responsible for their own application data backups, and for their own off-site disaster recovery.

Off-site tapes are transported and stored by Iron Mountain. The transport trucks and the facility where the tapes are physically stored are unmarked. The tapes are secured in locked metal boxes, and access is restricted to authorized personnel.

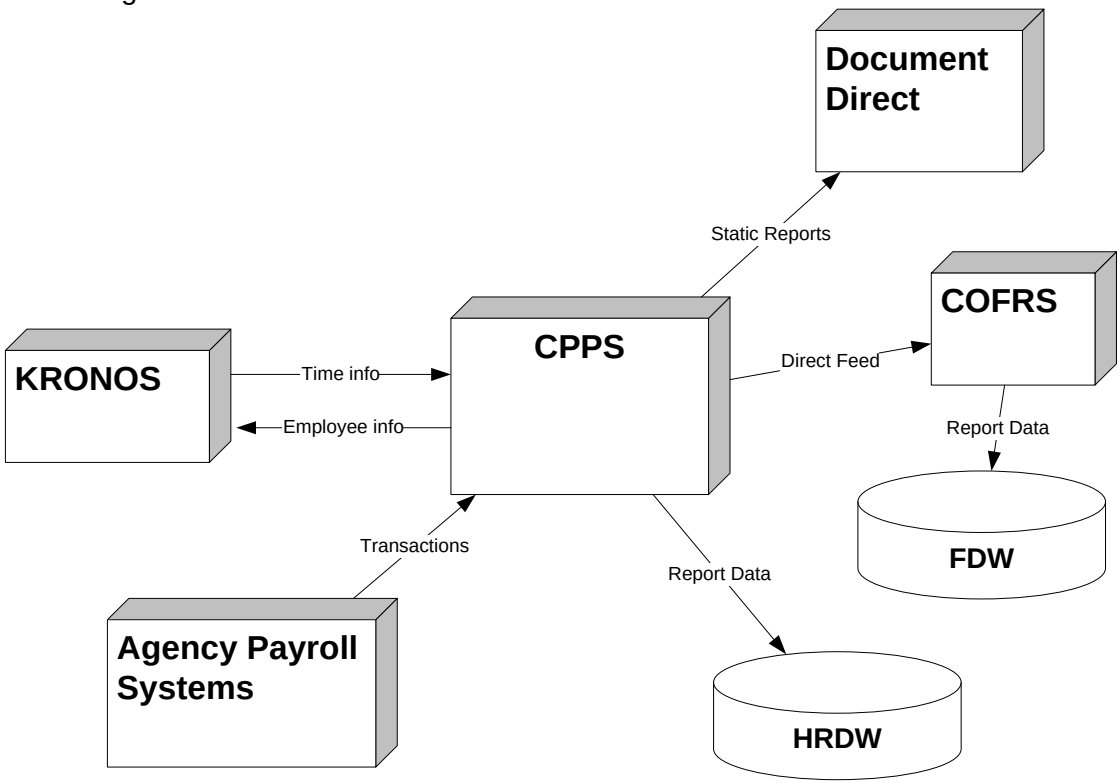
Management of Third-Party Services

Procurement and monitoring of third-party services are managed in accordance with OIT SOP #0606. OIT defines these services as those provided for the benefit of OIT and/or its customers by a person or entity other than at state agency or its employees. In general, such work would be done on-site, and the services would be paid for out of the personal services budget category. Services of short duration that can only be provided at the vendor site, such as a training class, are excluded from this process.

Responsibilities are defined for the hiring manager, the project manager and the financial administrative manager. A Third-Party Services Performance Report is completed as part of this process.

CPPS Interface

CPPS interfaces with several other systems in the IT environment, including various agency payroll systems, COFRS, Document Direct, HRDW and KRONOS. These interfaces are shown in the diagram below:

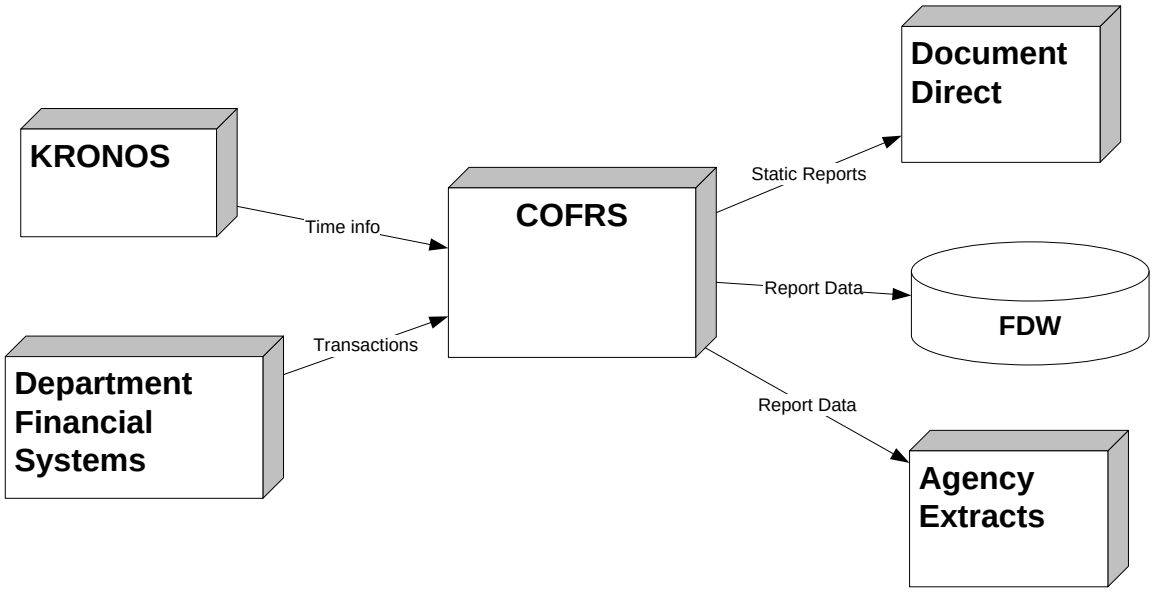


CPPS receives direct transactions from each agency's payroll system. All new interfaces for incoming transactions must be approved by the State Controller's Office prior to being allowed in the system. These incoming transactions cannot be processed unless they are free of errors. CPPS alerts users if there are errors in input forms.

During the payroll processing process, a series of batch jobs generates files for the output interfaces to HRDW, FDW and Document Direct. These output files are reviewed manually by analysts and reconciled to the payroll information in CPPS to verify that they are correct prior to payroll processing. Additionally, COFRS generates an error report for incoming transactions and posts it to Document Direct. This error report is also reviewed manually to verify that payroll processing is free of errors.

COFRS Interface

COFRS interfaces with several other systems in the IT environment, including various department financial systems, KRONOS, Document Direct and FDW. Additionally, agencies have custom extracts that are pulled for reporting. These interfaces are shown in the diagram below:



COFRS receives direct transactions from each department's financial systems. All new interfaces for incoming transactions must be approved by the State Controller's Office prior to being allowed in the system. These incoming transactions cannot be processed unless they are free of errors. All transactions must have a unique ID. COFRS alerts users if there are errors in input forms.

Additionally, the system requires that all transactions are approved prior to acceptance in COFRS as defined by the approval levels set for each transaction type.

If transaction counts or total amounts in the batches do not match proof totals, then batches are rejected. Additionally, in the rare case that a transaction is clearly erroneous and prevents balancing of the ledgers, statewide application services staff will manually modify the ledger record. The statewide application services staff maintains an electronic log detailing all such changes. A representative of the State Controller's Office authorizes all changes to the ledgers in writing.

All critical programs in the nightly cycle automatically issue termination codes identifying any processing errors detected by the program. Condition code checking in the Job Control Language (JCL) and CA7 prevents further processing after serious errors have occurred. In the event of an abnormal termination, the on-call programmer is notified, and is then responsible for resolution of the problem.

Each morning system analysts review system assurance reports that compare balances and other reports that will indicate whether transactions were processed completely and accurately.

Server Housing and Hosting

OIT provides both server housing and hosting services. Server housing consists of providing a rack location, power and network connectivity for an organization's server. Server hosting involves configuring, installing, managing and maintaining a server on behalf of an organization in addition to housing it in OIT's Data Center.

A repeatable process via documentation is used to build and configure a hosted server for customer requests. All deployed servers are reviewed with the customer during initial project/task meetings to determine the business needs of the requested server. Also defined within the business needs are hardware requirements, backup requirements, recovery expectations, remote access needs, contact information, security needs, procurement needs and change management expectations. With the business needs defined, a task/project is added to the Server Team Project List, where it is updated weekly via Server Management team status meetings.

If the server requirements identify that the system can be virtual, the server is built and configured on the VMware platform and Storage Area Network (SAN). If the server requirements identify that it needs to be a physical system, the server is acquired via OIT's approved procurement process. Upon receiving and/or identifying the required hardware, the server is physically installed on a rack in the Computer Room server "hosting" racks. The server is then placed within the identified Virtual Logical Area Network (VLAN) and behind a firewall. The necessary firewall communication rules are requested and configured, the OS is installed, supporting infrastructure is configured and the server is finally tested to make sure that it meets the identified needs of the customer and Server Management team build documentation. The server is added to the network monitoring software, added to the inventory database and labeled in the cabinet. Upon review of the server configuration to make sure that it the project/task requirements, server access is given to the customer to install its application.

The customer works with the Server Management team to install and configure its application. If the customer requested a test platform, all initial testing of the application would be performed on that system first. Upon successful completion of the test, the server is identified to the Service Center as a new test and/or production system on the network.

Changes and updates to the system are initiated via the customer or the Server Management team through the Remedy application. The Server Management team is required to notify and seek approval from the customer before any change is made to the system. OS updates are published by the OS manufacturer monthly and provide background of the updates or patches posted. Since all applications on "hosted" servers are managed by the customer, updates and changes to the application are handled through notification via the Service Center or Server Management team manager. Customers will work with the Server Management team to accomplish the desired application change.

If a server encounters an unexpected problem that is reflected in the network monitoring tool (Netman), the Service Center calls the Server Management team to notify it of the problem and opens a Remedy ticket. Initial troubleshooting is performed, and the outcome of that troubleshooting process is shared with the customer and updated in the Remedy ticket. If a change is required to fix the problem, it is also noted in the ticket and approval is sought from the customer.

Computer Operations is responsible for provisioning power from the power distribution units (PDUs) for use by customers wishing to house servers at the Data Center. Computer Operations monitors the computer rooms' environmental health and works with DPA's Capitol Complex building maintenance team to maintain a computer-friendly environment for hosted and housed servers. The Telecommunications team works with customers to provide network connectivity. All other aspects of the housed servers are the responsibility of the customer.

7 User Control Considerations

OIT's processes and controls have been designed with the assumption that certain controls would be implemented by user organizations (i.e., agencies). The application of such controls by user organizations is necessary to achieve certain control objectives included in this report. Data Center clients generally retain the functions of providing policy governance, investigation and vendor relationship management practices. There may be additional control objectives and related controls that would be appropriate to the processing of user transactions that are not identified in this report.

It is an assumption and an expectation of OIT that state agencies maintain an environment that also gives reasonable assurance that their own controls are placed in operation.

This section describes other control activities that should be in operation at user organizations to complement the control activities and processes at OIT. User auditors should consider whether the following controls are functioning effectively at user organizations.

General

- Agencies are responsible for evaluating and monitoring OIT's delivery of service to ensure conformity with contractual obligations.
- Agencies should designate their own internal client representative to ensure adequate maintenance of controls over services provided by OIT.
- Agencies should ensure that proper segregation of duties exists at their facilities.

Physical and Environmental

- Agencies should establish procedures to ensure that physical access to computer workstations and terminals is limited to authorized personnel.
- Agencies are responsible for ensuring that their employees who are given access to the Data Center are authorized by their management, and for notifying OIT when the employee's access to the Data Center should be removed.

CPPS and COFRS Change Management

- Agencies are responsible for ensuring that their requested changes to CPPS and COFRS have been authorized by the appropriate agency personnel.

Mainframe Logical Security

- Agencies should establish procedures and documentation for authorizing user access to terminals and application functions. Periodically, access granted to users should be reviewed to confirm that such access remains appropriate based on users' job functions.
- Agencies administering access security have the responsibility for ensuring adequacy of logical security over their environments.
- Agencies should establish procedures to ensure that additions, changes and deletions in agencies' personnel and their associated job responsibilities are authorized and communicated to OIT in a timely manner.
- Agencies should establish procedures to prohibit the use of shared user IDs or user IDs whose passwords are not changed on a regular basis.
- Agencies should regularly advise employees of the importance of security and of reporting suspicious personnel and/or transactions.
- Agencies should confirm that a TSS Security Violations Report is produced and reviewed by the agency security administrator on a regular basis. Agencies are responsible for investigating and correcting errors found on this report.

- Agencies should confirm that a TSS User Profile Change Log is produced and reviewed by the agency security administrator on a regular basis. Agencies are responsible for investigating and correcting errors found in this log.

CPPS and COFRS Security

- Agencies are responsible for appointing an Agency Security Administrator for COFRS who will have update rights to the Agency Security Table (ASEC) for his or her agency. This administrator is responsible for managing the access to COFRS for the employees in his or her agency.

- Agencies are responsible for managing new user access requests in COFRS, verifying that such requests are approved, and that access that is set up in the system matches what was requested.

- Agencies are responsible for ensuring that access requests for CPPS have been approved prior to being sent to the Payroll Manager for final review and approval.

- Agencies are responsible for removing terminated employees from the COFRS application on a timely basis.

- Agencies are responsible for notifying the Central Payroll Manager of terminated employees who have access to CPPS in a timely manner so that they can be removed from the system.

- Agencies are responsible for reviewing access to COFRS and CPPS for their employees on a periodic basis.

Perimeter Security

- Agencies should provide appropriate network filtering through the use of firewalls and other appropriate network defense strategies such as demilitarized zones (DMZs) and service gateways such as web proxies. The agencies should not rely on the basic filtering offered by the MNT because it is not specialized for the requirements of each individual agency. Agencies should create the appropriate policies, procedures and training plans to use the network devices and perimeter security strategies effectively.

CPPS and COFRS Interfaces

- Agencies should develop controls to ensure that input data and transactions are authorized, complete, accurate and valid.

  Input Controls – The OIT Data Center has implemented procedures to ensure control over agency transactions and data that have been submitted for processing on the Data Center's mainframe computer system. However, it is the agency's responsibility to initiate transactions and control data and to submit both to the Data Center. Agencies are responsible for ensuring that data and transactions are authorized, accurate and promptly

submitted to the Data Center for processing. When reviewing input controls at the user agency, auditors should:

- Confirm that input documents are authorized and reviewed by an appropriate level of management.
- Ensure that control totals are used to verify that all transactions are entered.
- Confirm that management reviews remote job entry documents before they are released for batch processing and that all remote job entry input documents or listings are canceled to prevent duplicate entries.

Output Controls – The Data Center's control procedures ensure that agency output is generated and distributed according to agency instructions. However, it is the agency's responsibility to ensure that output is accurate or that corrections are made promptly. When reviewing output controls at the agency, the auditor should:

- Confirm that exception reports are reviewed promptly and that any necessary corrections are made in a timely manner.
- Look for evidence of management's review of output reports for accuracy, completeness, reasonableness and mathematical accuracy.
- Review agency procedures for ensuring that output is distributed only to appropriate personnel.

Server Housing and Hosting

- Agencies have the responsibility for ensuring adequacy of logical security over their housing and hosted environments.
- Agencies have the responsibility for maintaining the applications installed on housing and hosted environments.
- Agencies have the responsibility for specifying the data to be backed up on housing and hosted environments.

SECTION THREE: INFORMATION PROVIDED BY THE INDEPENDENT AUDITOR

Overview of Control Objectives, Related Controls and Tests of Operating Effectiveness

1 Overview

This report on the controls placed in operation and tests of their operating effectiveness provides interested parties with sufficient information to understand the controls relative to selected services provided by OIT related to processing activities as they apply to the COFRS and CPPS applications and interfaces. In addition, our examination procedures included general controls as they apply to the server hosting and housing services provided by OIT. Our examination procedures did not include IT general control procedures over the applications that interface with COFRS and CPPS.

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specified controls. We considered the results of our tests over OIT's control environment, risk assessment and monitoring processes in determining the nature, timing and extent of our tests of operating effectiveness of the specific control activities for OIT's control objectives. Control environment objectives encompass the following areas:

- Strategic planning
- Information and communication
- Risk assessment and monitoring

IT general controls affect applications processed on the systems managed by OIT and encompass controls in the following areas:

- Physical and environmental
- Software and technology acquisition
- Infrastructure testing and installation
- CPPS and COFRS change management
- Mainframe logical security
- Perimeter security
- CPPS and COFRS logical security
- Job scheduling
- Problem and incident management
- Backup and recovery
- CPPS and COFRS interfaces
- Server housing and hosting

Our examination was performed in accordance with SAS No. 70, *Service Organizations*.

Our tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from July 1, 2009 to June 30, 2010. Our tests of the operational effectiveness of the controls were designed to cover a representative number of

events throughout the period. In selecting particular tests of operational effectiveness of controls, we considered the:

- Nature of the items being tested
- Types of available evidential matter
- Nature of the objectives to be achieved
- Assessed level of control risk
- Expected efficiency and effectiveness of the test

2 Control Objectives, Control Activities, Testing Procedures and Results of Tests

The following table describes the tests of operating effectiveness that were performed. OIT management specified the control objectives and the related control activities.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Strategic Planning		
Control objective 1: Controls provide reasonable assurance that the strategic planning process is in place to provide the direction and mandate for helping the business achieve its objectives.		
1.1 Management prepares strategic plans for IT that align business objectives with IT strategies. The planning approach includes mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans.	*Inspected* IT strategic plans to determine whether management aligns business objectives with IT strategies. *Inquired* of OIT to determine whether mechanisms are in place to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans.	No relevant exceptions noted.
1.2 An IT planning or steering committee exists to oversee the IT function and its activities. Committee membership includes representatives from senior management and the IT function.	*Inspected* a sample of IT steering committee meeting minutes to determine whether the committee exists to oversee IT activities and that committee membership includes representatives from senior management and IT.	No relevant exceptions noted.
1.3 OIT ensures that IT plans are communicated to business process owners and other relevant parties across the organization.	*Observed* whether IT plans are communicated to business process owners and other relevant parties across the organization.	No relevant exceptions noted.
1.4 OIT monitors its progress against the strategic plan and reacts accordingly to meet established objectives.	*Inspected* whether procedures are in place to monitor progress against the strategic plan and whether the IT organization reacts accordingly.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Information and Communication		
Control objective 2: Controls provide reasonable assurance that the IT organization is managing all aspects of the system environment and that policies and procedures have been developed and are maintained that define required acquisition and maintenance processes.		
2.1 Key systems and data have been inventoried and their owners identified.	*Observed* whether key systems and data have been inventoried and owners have been identified.	No relevant exceptions noted.
2.2 Contracted staff and other contract personnel are subject to policies and procedures created to control their activities by the IT function to assure the protection of the organization's information assets.	*Inspected* policies and procedures related to contract personnel to determine whether contractors are subject to procedures to protect OIT information assets.	No relevant exceptions noted.
2.3 IT strategies and ongoing operations are formally defined and communicated to senior management and customer CIOs.	*Observed* whether mechanisms are in place to communicate IT strategies to senior management and CIOs.	No relevant exceptions noted.
2.4 Significant IT events or failures (e.g., security breaches, major system failures or regulatory failures) are reported to senior management.	*Inquired* of OIT whether significant IT events are reported to senior management. *Inspected* a sample of incidents/problems to determine whether problems were identified and immediately entered into Remedy, whether corrective procedures were undertaken and whether the incident was reported to senior management.	No relevant exceptions noted.
2.5 Formal job descriptions exist and are kept current.	*Inspected* a sample of job descriptions to determine whether descriptions exist and are kept current.	No relevant exceptions noted.
2.6 An organizational chart is published and kept current.	*Inspected* OIT organizational chart to determine whether it is kept current.	No organizational chart was published for this fiscal year due to the consolidation of multiple state agencies. However, there is an executive management organizational chart available. See recommendation No. 3 on page 77.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Information and Communication		
Control objective 2: Controls provide reasonable assurance that the IT organization is managing all aspects of the system environment and that policies and procedures have been developed and are maintained that define required acquisition and maintenance processes.		
2.7 IT management has formulated, developed and documented policies and procedures governing the IT organization's activities.	*Inspected* policies and procedures to determine whether activities governing the IT organization have been documented.	No relevant exceptions noted.
2.8 IT management periodically reviews its policies, procedures and standards to reflect changing business conditions.	*Inspected* IT policies and procedures to determine whether management periodically performs reviews and updates to reflect changes to the environment.	Standard Operating Policies and Procedures were not regularly reviewed and updated for this fiscal year due to the consolidation of multiple state agencies. See recommendation No. 3 on page 77.
2.9 IT management has communicated policies and procedures governing the IT organization's activities.	*Inquired* of OIT whether IT policies and procedures are communicated to employees.	No relevant exceptions noted.
2.10 SOP manuals exist and are used by Data Center and statewide application systems personnel.	*Inspected* OIT SOPs to determine whether manuals exist and are used by Data Center and statewide application systems personnel.	No relevant exceptions noted.
Management Response: At the time of the 2010 SAS 70 examination the Office of Information Technology Executive Leadership team was in the process of formalizing the departmental organizational chart in support of IT consolidation efforts. At the time of this request, only the senior and executive management tiers of the organizational chart had been adopted operationally. OIT believes that the distribution of the entire organizational chart prior to the publication to all OIT employees and executive management approval would have been premature operationally. However, on June 25, 2010, the formal organizational chart, containing line authorities and supervisory reporting structures, was published to all OIT employees and delivered to the SAS 70 auditors as requested. The existing policies and procedures were followed during the course of the year without modification during the transition period leading up to the OIT employee consolidation and finalization of the resulting organizational structure. The organizational structure will be finalized in the first quarter of Fiscal Year 2011. Once this is complete, policies and procedures will be addressed to incorporate these organizational changes.		

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Human Resources		
Control objective 3: Controls provide reasonable assurance that hiring, training, performance evaluation, job responsibilities and termination practices are in accordance with established policy and that such policies are adequately communicated to personnel.		
3.1 State personnel rules and procedures are followed in all hiring, training, performance evaluation, job responsibilities and termination practices.	*Inspected* state personnel rules to determine whether procedures are followed in hiring, training, performance evaluation, job responsibilities and termination practices.	No relevant exceptions noted.
3.2 A checklist is used for all departing employees to ensure that separation/ termination activities are conducted according to policy.	*Inspected* a sample of departing employees to determine whether separation/termination activities were conducted according to policy.	No relevant exceptions noted.
3.3 New employees attend departmental and divisional orientation sessions.	*Inspected* a sample of newly hired employees to determine whether new employees attend departmental and divisional orientation sessions by reviewing evidence related to new hire orientation from the new hire checklist.	No relevant exceptions noted.
3.4 New employees sign a Statement of Compliance indicating that they have received and agree to the computer usage and data security policy.	*Inspected* a sample of newly hired employees to determine whether new employees sign a Statement of Compliance indicating that they have received and agree to the computer usage and data security policy.	No relevant exceptions noted.
3.5 A performance appraisal system is in place. Semiannual reviews are required and annual ratings are performed.	*Observed* whether performance appraisal system is in place requiring semiannual performance reviews and that annual ratings are performed in April.	No relevant exceptions noted.
3.6 Employees are trained in accordance with job responsibilities.	*Inspected* training programs to determine whether employees are trained in accordance with their job responsibilities.	No relevant exceptions noted.
3.7 Newly hired employees are required to pass a background check prior to employment.	*Selected* a sample of newly hired employees to determine whether background checks had been performed prior to employment.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Risk Assessment and Monitoring		
Control objective 4: Controls provide reasonable assurance that the IT organization has an entity- and activity-level risk assessment framework, which is used periodically to assess risk to achieving business objectives, and quality programs that address both general and project-specific quality assurance activities.		
4.1 Project risk assessment is addressed as new projects are proposed to the Project Review Board.	*Inquired* of OIT whether project risk assessments are addressed as new projects are proposed to the Project Review Board. *Inspected* a sample of Project Proposals to determine whether risk assessments are considered.	No relevant exceptions noted.
4.2 Risk assessment is documented in the Project Proposal Form.	*Inspected* a sample of Project Proposals to determine whether risk assessments are documented in the Project proposal Form.	No relevant exceptions noted.
4.3 Management obtains feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process.	*Inquired* of OIT whether management obtains feedback from business process owners and users regarding the quality and usefulness of IT plans for use in the ongoing risk assessment process.	No relevant exceptions noted.
4.4 The Service Level Manager researches all known major system outages, completes an outage notification and distributes it to senior management.	*Selected* a sample of major system outages to determine whether an outage notification was completed and distributed to senior management.	No relevant exceptions noted.
4.5 Management receives and reviews unplanned outage notification forms monthly.	*Inspected* a sample of monthly unplanned outage notification forms to determine whether they were sent for management review.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Risk Assessment and Monitoring		
Control objective 4: Controls provide reasonable assurance that the IT organization has an entity- and activity-level risk assessment framework, which is used periodically to assess risk to achieving business objectives, and quality programs that address both general and project-specific quality assurance activities.		
4.6 An annual TSS access review for Computing Services is completed.	*Inspected* the annual TSS access review to determine whether it was completed.	Access changes identified as a result of the annual Top Secret access review were not implemented. Two users with inappropriate administrator access identified as a result of the review were not removed. See recommendation No. 1 on page 75.
4.7 Project review sessions (Lessons Learned) are held at the end of projects to determine areas of success and areas for improvement.	*Inquired* of management and inspected a sample of session notes to determine whether project review sessions were held at the end of projects.	No relevant exceptions noted.
4.8 Standard Operating Policies (SOPs) are reviewed against current operations annually.	*Inquired* of OIT whether SOPs are reviewed against current operations on an annual basis.	SOPs were not regularly reviewed and updated for this fiscal year due to the consolidation of multiple state agencies. See recommendation No. 3 on page 77.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Risk Assessment and Monitoring		
Control objective 4: Controls provide reasonable assurance that the IT organization has an entity- and activity-level risk assessment framework, which is used periodically to assess risk to achieving business objectives, and quality programs that address both general and project-specific quality assurance activities.		
Management Response: OIT acknowledges and agrees with the findings identified in the SAS 70 examination. Although the controls are in place for those items identified above, OIT did experience an operational and transitional gap in services and systems administration from September 2009 to present day. The gap in essential support services and access control administration was due to the unanticipated resignation of the primary system and security administrator in September 2009 and the operational realignment of the secondary system and security administrator during a recent layoff and restructuring initiative that occurred at OIT in October 2009. During this same time period, the OIT Executive Leadership team was in the process of formulating the staff realignment and restructuring phase of the OIT consolidation efforts. This effort identified and placed over 850 information technology staff into operational banding units within OIT. The reorganization of these state IT personnel into the newly defined OIT organizational structure went into effect on July 1, 2010, and interim staff realignments to mitigate this operational gap could not occur prior to this date. In addition, within the newly adopted organizational structure, OIT has created and implemented the Office of the Chief Technical Officer and a subordinate Access Control Section, respectively. The Access Control Section, under this new organizational structure, has been identified as the responsible entity for long-term administration and access control functions for TopSecret and those control functions identified above. The Access Control Section consists of a Level 4 Senior IT Manager with 2 direct reports and 12-15 technical information technology staff. Beginning July 1, 2010, the Access Control Section began to identify a primary and secondary administrator to support the mainframe and TopSecret access control functions and validate and revise those control items essential to the long-term support and security requirements needed for the secure management of the system.		

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Physical and Environmental		
Control objective 5: Controls provide reasonable assurance that physical security and environmental controls help the service organization maintain the security and availability of their systems.		
5.1 All visitors must enter the OIT Data Center through the front entrance and pass through two secured staging areas which are controlled by building reception. All other building entrances are controlled by scramble pad lock combinations and are for use by employees.	*Observed* whether all visitors must enter the OIT Data Center through the front entrance and pass through two secured staging areas. *Observed* whether building entrances are controlled by scramble pad lock combinations.	No relevant exceptions noted.
5.2 Employees and visitors must wear badges at all times while in the building.	*Observed* whether employees and visitors are wearing badges while in the building.	No relevant exceptions noted.
5.3 Visitors must check in with reception and complete the roster with their name, time in and who they are seeing. Visitors are provided a visitor identification badge. Visitor time out is recorded on the roster at departure.	*Observed* whether visitors check in with the receptionist and complete a roster with their name, time and who they are seeing. *Observed* whether employees and visitors are wearing badges while in the building.	No relevant exceptions noted.
5.4 Visitors must be escorted at all times unless granted specific permission in person.	*Observed* whether visitors are escorted, unless granted specific permission in person.	No relevant exceptions noted.
5.5 The Data Center computing facility is comprised of two areas: The Telecommunications Room and the Computer Room. A Trilogy lock system secures each area.	*Observed* whether the Data Center computing facility is protected by a Trilogy lock system.	No relevant exceptions noted.
5.6 The Data Center has 24x7 operations and someone is on-site at all times.	*Inquired* of Data Center personnel and inspected operator's schedule to determine whether operations are manned 24x7.	No relevant exceptions noted.
5.7 Data Center staff monitor the building cameras for unfamiliar or unusual activity after normal business hours.	*Observed* whether the Data Center staff monitors the building cameras for unfamiliar or unusual activity after normal business hours.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Physical and Environmental		
Control objective 5: Controls provide reasonable assurance that physical security and environmental controls help the service organization maintain the security and availability of their systems.		
5.8 Departing employees' individual Trilogy lock system codes are disabled upon termination.	*Selected* a sample of terminated employees to determine whether their Trilogy code was disabled.	No relevant exceptions noted.
5.9 Employees receive new Trilogy combinations for only those areas for which they are authorized.	*Selected* a sample of OIT employees to determine whether Data Center access is restricted to authorized employees based on job responsibility.	No relevant exceptions noted.
5.10 There are standard procedures for accepting and transferring materials (data products or common deliveries) in and out of the Data Center.	*Inspected* standard operating procedure for accepting and transferring materials in and out of the Data Center.	No relevant exceptions noted.
5.11 The computing facility is equipped with smoke detectors located above and below the raised flooring and directly linked to the fire suppression system. Water detection sensors are located under the floor.	*Observed* whether the computing facility is equipped with smoke detectors located above and below the raised floor and directly linked to the FM-200 system. *Observed* whether water detection sensors are located under the floor.	No relevant exceptions noted.
5.12 The computing facility is equipped with a FM-200 gas fire suppression system.	*Observed* whether the OIT Data Center is equipped with a FM-200 gas fire suppression system.	No relevant exceptions noted.
5.13 The FM-200 system is inspected annually by a third-party service and has an automated monitoring system that is checked regularly by Data Center personnel.	*Inspected* whether the FM-200 system is inspected annually. *Observed* whether an automated monitoring system for the FM-200 system is checked regularly by Data Center personnel.	No relevant exceptions noted.
5.14 Temperature and humidity are monitored by the Computer Operations staff in the Data Center.	*Observed* whether temperature and humidity are monitored by the Computer Operations staff in the Data Center.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Physical and Environmental		
Control objective 5: Controls provide reasonable assurance that physical security and environmental controls help the service organization maintain the security and availability of their systems.		
5.15 The Data Center is equipped with a combination of a UPS system and a generator to provide continuous power in the event of a power outage.	*Observed* whether the Data Center is equipped with a combination of a UPS system and a generator to provide continuous power.	No relevant exceptions noted.
5.16 Central monitoring of the building fire alarms is provided by building facility management, which will notify the fire department if an alarm is activated.	*Inquired* of OIT whether central monitoring of the building fire alarms is provided by the local fire department, which will respond if an alarm is activated.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Software and Technology Acquisition		
Control objective 6: Controls provide reasonable assurance that the acquisition of, and maintenance and changes to, system software and hardware are appropriately initiated and authorized.		
6.1 Documented procedures have been developed and are followed in the requisition, bidding and purchase of new utilities software and hardware.	*Inspected* procedures for requisition, bidding and purchasing of new utilities software and hardware purchases to determine whether they are developed and followed.	No relevant exceptions noted.
6.2 Appropriate justification and management approval is required before the acquisition of new utilities software and hardware.	*Inspected* a sample of new software utilities and hardware purchased to determine whether appropriate justification and management approval was obtained.	No relevant exceptions noted.
6.3 Software acquisitions include annual support or funds for renewal are encumbered annually prior to expiration.	*Inspected* a sample of new software utilities purchased to determine whether an account code was encumbered and approved and whether support funds were included.	No relevant exceptions noted.
6.4 Hardware acquisitions include annual maintenance and support or funds for renewal are encumbered prior to expiration.	*Inspected* a sample of new hardware purchased to determine whether an account code was included on the approval and whether support funds were included.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Software and Technology Acquisition		
Control objective 7: Controls provide reasonable assurance that system capacity and performance are actively monitored in order to help define requirements for acquisitions, maintenance and changes to system software and hardware.		
7.1 Service Management Facility (SMF) recording options are appropriate to capture and monitor capacity and performance.	*Inspected* SMF recording options to determine whether they are configured to capture and monitor capacity and performance.	No relevant exceptions noted.
7.2 Data Center personnel review SMF information on a regular basis to monitor system performance and usage and ensure that infrastructure is appropriate to need.	*Inquired* of OIT whether Data Center personnel review SMF information on a regular basis to monitor system performance and usage of infrastructure.	No relevant exceptions noted.
7.3 SMF data capture is retained and presented in graphical format for management review.	*Observed* whether SMF data capture is retained and presented in graphical format for management review.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Infrastructure Testing and Installation		
Control objective 8: Controls provide reasonable assurance that the maintenance and changes to system software and hardware are tested in accordance with documented requirements and authorized for implementation.		
8.1 A formal change management system is used to control and document changes to system software.	*Observed* whether OIT uses a change management system to control and document changes to system software.	No relevant exceptions noted.
8.2 Prior to the modification of system software, the modifications are authorized by appropriate personnel.	*Inquired* of OIT whether modifications are authorized in workgroups prior to development. *Inspected* a sample of system software modifications to determine whether modifications were approved prior to introduction into the production environment.	No relevant exceptions noted.
8.3 System software modifications and additions are thoroughly tested and approved before introduction into the production environment.	*Inspected* a sample of system software modifications to determine whether modifications were tested and approved prior to introduction into the production environment.	No relevant exceptions noted.
8.4 Separate test and production environment exist.	*Observed* whether separate test and production environments exist.	No relevant exceptions noted.
8.5 Documentation for system software products is available and current.	*Observed* whether documentation for system software products is available and current.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Infrastructure Testing and Installation		
Control objective 9: Controls provide reasonable assurance that changes to system software and hardware are approved prior to implementation into production and that all approved changes are properly implemented.		
9.1 An implementation schedule is published to the customers.	*Inspected* a sample of modifications to determine whether an implementation schedule is published to the customer.	No relevant exceptions noted.
9.2 Affected clients are notified via email, telephone or broadcast message prior to placing a modification into production.	*Inspected* a sample of customer notifications to validate that customers were notified following system modifications.	No relevant exceptions noted.
9.3 Prior to implementation, management assesses the impact of system software modifications on client processing.	*Inspected* a sample of modifications to determine whether OIT assesses the impact of the system software modifications on client processing.	No relevant exceptions noted.
9.4 Back-out procedures are written to return the system's configuration to its pre-implementation condition.	*Inspected* a sample of modifications to determine whether back-out plans exist.	No relevant exceptions noted.
9.5 The installation process for system software includes a review/update of associated documentation.	*Inquired* of OIT whether the installation process for system software includes a review/update of associated documentation.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
CPPS and COFRS Change Management		
Control objective 10: Controls provide reasonable assurance that changes to the CPPS and COFRS applications are appropriately initiated and authorized, tested and approved and properly implemented.		
10.1 A formal change management methodology is used to control and document changes to application software for CPPS and COFRS.	*Inspected* change management methodology to determine whether a process is in place to control and document changes to the CPPS and COFRS applications.	No relevant exceptions noted.
10.2 Proposed changes to software are reviewed and approved prior to development for COFRS and CPPS.	*Inspected* a sample of CPPS and COFRS changes to determine whether changes were reviewed and approved by the authorized manager prior to migration to the production environment.	No relevant exceptions noted.
10.3 Upon completion of software changes, software modifications are tested and formal acceptance is granted.	*Inspected* a sample of CPPS and COFRS changes to determine whether changes were authorized, tested and approved by the authorized manager prior to migration to the production environment.	No relevant exceptions noted.
10.4 Managerial or requestor review of functionality, unit testing and acceptance testing is performed prior to implementation.	*Inspected* a sample of CPPS and COFRS changes to determine whether changes were authorized, tested and approved by the authorized manager prior to migration to the production environment.	No relevant exceptions noted.
10.5 Manual controls are used to ensure that the correct version of software is being modified and later implemented into production.	*Inspected* whether separate development, test and production libraries are used when making modifications to the CPPS and COFRS applications.	No relevant exceptions noted.
10.6 For COFRS, the Financial Systems Manager performs a monthly review of all changes made to the production environment and verifies that all changes are authorized and approved by mapping them back to approved Remedy tickets.	*Inspected* a sample of monthly reviews to determine whether all changes are reviewed and mapped to authorized change requests.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
CPPS and COFRS Change Management		
Control objective 10: Controls provide reasonable assurance that changes to the CPPS and COFRS applications are appropriately initiated and authorized, tested and approved and properly implemented.		
10.7 Clients are notified of changes to the application if the changes will impact the clients' interaction with the application.	*Inspected* a sample of CPPS and COFRS notices to determine whether customers are notified of the impact of any changes.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Mainframe Logical Security		
Control Objective 11: Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems.		
11.1 Computer operators are prohibited from making changes to systems and data.	*Inspected* mainframe Computer Operator access levels to determine whether operators are prohibited from making changes to systems and data.	No relevant exceptions noted.
11.2 Application programmers are not permitted access to operating system files and data.	*Inspected* mainframe application programmers' access levels to determine whether programmers are denied access to operating system files and data.	No relevant exceptions noted.
11.3 Access to security administration functions is appropriately limited to authorized individuals.	*Inspected* mainframe administrative access to systems and resources to determine whether access is limited to specific employees and groups whose job responsibilities require such access.	We noted that two users maintained inappropriate administrator-level (SCA group) access within TSS. See recommendation No. 1 on page 75.
11.4 TSS is used to restrict access to system software to appropriate individuals.	*Observed* that TSS is configured to restrict access to production software.	No relevant exceptions noted.
11.5 TSS is used to restrict access to those system programs that allow bypassing of normal system or application controls (e.g., Super Zap).	*Inspected* system programs that allow bypassing of normal system or application controls to determine whether TSS is used to restrict access.	No relevant exceptions noted.
11.6 The System Security and Use SOP #8808 provides clear guidance regarding the responsibilities of TSS security administrators and the issuance of access permissions.	*Inspected* the System Security and Use SOP to determine whether it provides clear guidance regarding the responsibilities of TSS security administrators and the issuance of access permissions.	No relevant exceptions noted.
11.7 Employees receiving logical access to the mainframe are required to sign a Compliance Statement, referencing and acknowledging the computer usage and data security policy.	*Inspected* a sample of new mainframe accounts to determine whether employees receiving logical access to the mainframe have signed a Compliance Statement acknowledging the computer usage and data security policy.	No evidence of the required signed Statement of Compliance was found for one out of three new users added to the system since July 1, 2009. See recommendation No. 1 on page 75.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Mainframe Logical Security		
Control Objective 11: Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems.		
11.8 Security administrators are required to sign an additional Statement of Compliance referencing and acknowledging responsibilities relative to TSS security administration.	*Inspected* a sample of new OIT security administrators to determine whether the additional Statement of Compliance referencing and acknowledging responsibilities relative to TSS security administration was completed.	No evidence of the required signed Agency Security Administration (ASA) form was found for all security administrators added since July 1, 2009. See recommendation No. 1 on page 75.
11.9 SOPs require that users have access to only those resources necessary and appropriate to their job duties.	*Inspected* SOPs to determine whether users are required to have access to only those resources necessary and appropriate to the users' job responsibilities. *Inspected* a sample of new Data Center personnel and mainframe account modifications to determine whether access to mainframe and datasets was properly authorized and access rights were set up appropriately.	No relevant exceptions noted.
11.10 Supervisor/manager sends requests through the Help Desk to arrange logical access to mainframe and datasets for new Data Center personnel. The employee's supervisor defines the initial access to be granted and minimum permission rights based on their position.	*Inspected* a sample of new Data Center personnel to determine whether access to mainframe and datasets was properly authorized and whether access rights were set up appropriately.	Two of the three new mainframe users selected for testing had no Remedy ticket documenting that their access was requested and authorized. See recommendation No. 1 on page 75.
11.11 New personnel receive a unique Access ID and temporary password. The password must be changed on their first login attempt or their account will be suspended (locked out).	*Observed* the mainframe new account administration process to determine whether new personnel receive a unique Access ID and a temporary password that must be changed upon first login.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Mainframe Logical Security		
Control Objective 11: Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems.		
11.12 TSS is configured to enforce password controls including minimum length, defined password expiration, minimum re-use of password generation and account suspension/lockout after minimum failed login attempts.	*Inspected* certain key mainframe logical security configuration parameters to determine whether the following is configured: a minimum password length, defined password expiration period, minimum re-use of password generation and account suspension/lockout after a minimum number of failed login attempts.	No relevant exceptions noted.
11.13 The Help Desk unlocks accounts only after verifying a user's identity using additional private information from INSTADATA.	*Observed* whether the Help Desk unlocks accounts only after verifying a user's identity using additional private information stored in INSTADATA.	No relevant exceptions noted.
11.14 Future access permission changes/enhancements require an email or other written communication from the user's supervisor to the Help Desk explaining the reason for the permission change request.	*Inspected* a sample of new Data Center personnel and mainframe account access modifications to determine whether such access to the mainframe and datasets was properly authorized and whether access rights were set up appropriately.	No relevant exceptions noted.
11.15 The system automatically disconnects a Time Sharing Option (TSO) session if inactive for 15 minutes.	*Inspected* mainframe configurations to determine whether the system automatically disconnects a TSO session if inactive for 15 minutes.	No relevant exceptions noted.
11.16 TSS is operating in fail mode, meaning that unauthorized attempts to access datasets are aborted.	*Inspected* mainframe configurations to determine whether TSS is operating in fail mode.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Mainframe Logical Security		
Control Objective 11: Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems.		
11.17 TSS logs security violations; logs are reviewed weekly, and action is taken to investigate violations.	*Inspected* mainframe configurations to determine whether security violations are logged. *Observed* whether the TSS security violation logs are reviewed and signed-off on a weekly basis and whether actions are taken to investigate when necessary.	Security log violations were not reviewed after September 2009. See recommendation No. 1 on page 75.
11.18 TSS logs security profile changes; logs are reviewed monthly, and unusual items are identified and investigated.	*Inspected* a sample of the monthly security profile log reviews to determine whether the report is reviewed on a monthly basis and whether unusual items are identified and investigated.	Security profile change logs have not been reviewed since July 1, 2009. See recommendation No. 1 on page 75.
11.19 The administrative staff utilizes a departing employee checklist to ensure that the departing personnel's user mainframe account is deleted in a timely manner.	*Selected* a sample of terminated employees to determine whether the departing employees' user mainframe accounts were deleted in a timely manner.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Mainframe Logical Security		
Control Objective 11: Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems.		
Management Response: OIT acknowledges and agrees with the findings identified in the SAS 70 examination. Although the controls are in place for those items identified above, OIT did experience an operational and transitional gap in services and systems administration from September 2009 to present day. The gap in essential support services and access control administration was due to the unanticipated resignation of the primary system and security administrator in September 2009 and the operational realignment of the secondary system and security administrator during a recent layoff and restructuring initiative that occurred at OIT in October 2009. During this same time period, the OIT Executive Leadership team was in the process of formulating the staff realignment and restructuring phase of the OIT consolidation efforts. This effort identified and placed over 850 information technology staff into operational banding units within OIT. The reorganization of these state IT personnel into the newly defined OIT organizational structure went into effect on July 1, 2010, and interim staff realignments to mitigate this operational gap could not occur prior to this date. In addition, within the newly adopted organizational structure, OIT has created and implemented the Office of the Chief Technical Officer and a subordinate Access Control Section, respectively. The Access Control Section, under this new organizational structure, has been identified as the responsible entity for long-term administration and access control functions for TopSecret and those control functions identified above. The Access Control Section consists of a Level 4 Senior IT Manager with 2 direct reports and 12-15 technical information technology staff. Beginning July 1, 2010, the Access Control Section began to identify a primary and secondary administrator to support the mainframe and TopSecret access control functions and validate and revise those control items essential to the long-term support and security requirements needed for the secure management of the system.		

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Perimeter Security		
Control objective 12: Controls provide reasonable assurance that perimeter security devices are properly configured and installed to prevent access unless specifically allowed, and that the ability to make changes to the firewall is restricted to authorized individuals.		
12.1 System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	*Inspected* OIT's network diagram to determine whether firewalls and routers are strategically placed to control and filter traffic between segments of the network. *Inspected* documentation of firewall configurations and monitoring standards to determine the appropriateness of design based on the documented risks. *Inspected* system reports to determine whether firewalls are configured and monitored in accordance with OIT standards.	No relevant exceptions noted.
12.2 IT management has implemented antivirus and antispam protection across the organization to protect information systems and technology from computer viruses.	*Observed* whether OIT has implemented antivirus and antispam protection across the organization to protect information systems and technology from computer viruses.	No relevant exceptions noted.
12.3 Access Control Server is used to monitor changes to critical network equipment.	*Observed* whether RANCID is used to monitor changes to critical network equipment.	No relevant exceptions noted.
12.4 Update access to the firewalls is restricted to authorized personnel through assignment of user IDs that require passwords to authenticate.	*Inspected* accounts with the ability to update firewall rulesets to determine whether access is restricted to authorized individuals based on job responsibility. *Observed* whether firewall administrators are required to authenticate to the firewall server.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Perimeter Security		
Control objective 12: Controls provide reasonable assurance that perimeter security devices are properly configured and installed to prevent access unless specifically allowed, and that the ability to make changes to the firewall is restricted to authorized individuals.		
12.5 Changes to access control lists on perimeter security devices are authorized through a security variance process. The security variance form must be signed and the approval of changes must be done in conjunction with a risk assessment on the impact of the change.	*Inspected* a sample of firewall changes to determine whether the security variance process was followed.	No relevant exceptions noted.
12.6 Changes to perimeter security devices are authorized by the Security Manager and are performed in a time window and documented for troubleshooting purposes.	*Inspected* a sample of firewall changes to determine whether the security variance process was followed.	No relevant exceptions noted.
12.7 Changes made to security devices such as firewalls, VPN Concentrator, and ACS are done in accordance with the security variance process.	*Inspected* a sample of firewall changes to determine whether the security variance process was followed.	No relevant exceptions noted.
12.8 The ISOC uses advisories and alerts to notify parties affected by malicious traffic/code. Reports are generated by the vendor contractor and posted to a portal accessible by the ISOC.	*Observed* the use of alerts and notifications on the security portal.	No relevant exceptions noted.
12.9 Penetration testing is performed periodically by a third party.	*Inspected* a copy of a recent vulnerability scan report.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
CPPS and COFRS Logical Security		
Control Objective 13: Controls provide reasonable assurance that logical access controls are in place for the CPPS and COFRS application systems.		
13.1 A user ID and password are required to enter or modify transactions in the COFRS and CPPS applications.	*Observed* a user log in to the COFRS and CPPS applications, and noted that each of the systems requires a user ID and password.	No relevant exceptions noted.
13.2 Access to the ASEC table in COFRS in the IT department (security administrators) is restricted to authorized administrators. Access to security administration functions in CPPS is restricted to authorized administrators.	*Inspected* a system listing of users who have access to the ASEC table in COFRS and validated whether they were appropriate. Inspected a listing of users with administrative functions in CPPS and validated whether they were appropriate.	We noted that the approver/reviewer of access for COFRS was also the primary security administrator and had the ability to provision access in the system from July 2009 to November 2009. We performed testing of the new user access process, the review of access process in COFRS and the termination process. We noted no exceptions or inappropriate access. Additionally, we noted that a user must be set up with a TSS ID in order to gain access, which is outside the sphere of responsibility of the OIT Controller. See disposition of prior examination recommendations and resolution No. 2 on page 79.
13.3 Access is granted to the COFRS and CPPS systems only upon approval by the user's manager. Requests for access to CPPS must be approved by the Central Payroll Manager prior to access being granted. Requests for access to COFRS must be approved by the OIT Controller prior to access being granted.	*Selected* a sample of new users to determine whether request and approval documentation is appropriate for the access that was granted in the system.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
CPPS and COFRS Logical Security		
Control Objective 13: Controls provide reasonable assurance that logical access controls are in place for the CPPS and COFRS application systems.		
13.4 Access of terminated IT department administrators to COFRS and CPPS is revoked on a timely basis.	*Inspected* the listing of terminated employees, the listing of users from COFRS and the listing of users from CPPS to determine whether terminated employees retain access to the systems.	No relevant exceptions noted.
13.5 On a periodic basis, access to COFRS is reviewed to ensure that access is appropriate.	*Inspected* a sample of user access reviews to determine whether they were performed on a timely basis throughout the audit period.	No relevant exceptions noted.
13.6 Access to CPPS is reviewed on a periodic basis to ensure that access is appropriate.	*Inspected* a sample of user access reviews to determine whether they were performed on a timely basis throughout the audit period.	No relevant exceptions noted.
13.7 Password configuration settings for COFRS and CPPS are established to prevent account compromise.	*Inspected* the CPPS and COFRS applications to verify whether strong password configuration settings are enabled.	No relevant exceptions noted.
Management Response: In mid-November 2009, logical COFRS access was modified such that the OIT Controller can no longer set up or grant access to the COFRS system or modify user account privileges. Access was modified to move into compliance on this item based on the prior-year SAS 70 examination findings. OIT believes that this item and the requirement for separation of duties for COFRS account management was achieved within the time frame identified during the 2009 SAS 70 examination period and this examination period.		

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Job Scheduling		
Control objective 14: Controls provide reasonable assurance that authorized programs are executed as planned and that deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.		
14.1 Top Secret is used to restrict access to scheduling software (CA7) to appropriate personnel.	*Inspected* a listing of mainframe accounts with access to scheduling software (CA7) to determine whether access is restricted to appropriate personnel based on job responsibility.	No relevant exceptions noted.
14.2 Automated operation of scheduling software is used.	*Observed* whether the mainframe scheduling software CA7 is used to schedule mainframe jobs.	No relevant exceptions noted.
14.3 Operator activities are recorded on the console log.	*Observed* whether mainframe operator activities are recorded on the console log.	No relevant exceptions noted.
14.4 Batch jobs that do not run correctly are automatically entered into the system log and resolved by the Control Processing Procedures.	*Observed* whether mainframe failed batch jobs are automatically entered into the system log and resolved using Control Processing Procedures.	No relevant exceptions noted.
14.5 Batch jobs are run on a predetermined schedule and are tracked automatically.	*Observed* whether mainframe batch jobs are run on a predetermined schedule and tracked automatically.	No relevant exceptions noted.
14.6 The Data Center has documented Control Processing Procedures that provide detailed guidance to address processing problems, including who to contact for system and application-specific troubleshooting information.	*Inspected* Data Center Control Processing Procedures to determine whether procedures include detailed guidance to address processing problems, contact information and troubleshooting information.	No relevant exceptions noted.
14.7 Problems identified are immediately entered into Remedy, defining the problem and corrective procedures undertaken.	*Inspected* a sample of incidents/problems to determine whether problems are identified and immediately entered into Remedy and whether corrective procedures are undertaken.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Job Scheduling		
Control objective 14: Controls provide reasonable assurance that authorized programs are executed as planned and that deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.		
14.8 Exceptions to normal operations as they relate to processing and tracking of problems are reported for management review via Remedy tickets.	*Observed* whether problems are identified and immediately entered into Remedy and whether management is included on the ticket.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Problem and Incident Management		
Control objective 15: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.		
15.1 A problem management system (Remedy) is used to record, track and resolve identified incidents/problems.	*Observed* whether the problem management system (Remedy) is used to track and resolve identified incidents/problems.	No relevant exceptions noted.
15.2 Incidents or problems identified are immediately entered into a Remedy ticket.	*Inspected* a sample of incidents/problems to determine whether problems are identified and immediately entered into Remedy and whether corrective procedures are undertaken.	No relevant exceptions noted.
15.3 Customers are notified of outages.	*Selected* a sample of unplanned outages to determine whether customers were notified.	No relevant exceptions noted.
15.4 Unplanned outages related to incidents are managed in accordance with SOPs to ensure proper response, investigation and resolution.	*Selected* a sample of unplanned outages to determine whether outages were managed in accordance with SOPs, including customer investigation, resolution, customer notification and management review.	No relevant exceptions noted.
15.5 Outage notifications are documented.	*Selected* a sample of unplanned outages to determine whether outages were managed in accordance with SOPs, including customer investigation, resolution, customer notification and management review.	No relevant exceptions noted.
15.6 Short- and long-term outage notification resolutions are reviewed by management.	*Selected* a sample of unplanned outages to determine whether outages were managed in accordance with SOPs, including customer investigation, resolution, customer notification and management review.	No relevant exceptions noted.
15.7 Service Outage Notification Reports are provided to management.	*Selected* a sample of unplanned outages to determine whether outages were managed in accordance with SOPs, including customer investigation, resolution, customer notification and management review.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Backup and Recovery		
Control objective 16: Controls provide reasonable assurance that mainframe programs and data files are routinely backed up and archived in a secure location and that measures have been taken to minimize the risk of a business interruption.		
16.1 The following are backed up on a defined schedule: critical disk packs, system datasets and catalogs and source program libraries.	*Inspected* the job schedules for critical disk packs, system datasets and catalogs and source program libraries to determine whether they were backed up on a defined schedule.	No relevant exceptions noted.
16.2 Initial storage of data on disk is managed by SMS.	*Observed* SMS and CA7 (tape management software) parameters to determine whether backup, archive and retention were configured.	No relevant exceptions noted.
16.3 Backup, archive, and retention operations are governed by SMS parameters and CA7.	*Observed* SMS and CA7 (tape management software) parameters to determine whether backup, archive and retention were configured.	No relevant exceptions noted.
16.4 All backup datasets are kept until they are deleted from the catalog or expired.	*Inspected* a sample of backup datasets and validated that they were appropriately archived and maintained for a year.	No relevant exceptions noted.
16.5 Backup media is stored off-site.	*Inspected* a sample of tapes for one day to determine whether they were sent off-site.	No relevant exceptions noted.
16.6 Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	*Inspected* disaster recovery test report to examine summary of tests performed, results and issues encountered.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
CPPS Interfaces		
Control objective 17: Controls provide reasonable assurance that CPPS transactions (and interfaces) are complete and accurate and that any errors in processing are followed up on and corrected.		
17.1 All interfaced transactions by agencies to HR/Payroll require advance authorization from the State Controller's Office.	*Inspected* a sample of new transaction interfaces to determine whether advance authorization from the State Controller's Office was obtained.	We confirmed through corroborative evidence with the HR/Systems Manager and the State Controller's Office that no new CPPS transaction interfaces were created in the system during the period under review.
17.2 Errors detected in CPPS input cannot be processed until the user corrects them online.	*Observed* the Central Payroll Manager attempt to process an input form with errors, and noted the resulting error screen.	No relevant exceptions noted.
17.3 All critical programs in the nightly cycle issue termination codes identifying any processing errors detected by the program. Condition code checking in the Job Control Language (JCL) and CA7 prevents further processing after serious errors have occurred. In the event of an abnormal termination, an on-call programmer is notified who is then responsible for resolution.	*Inspected* an incident ticket to determine whether processing errors are detected and resolved.	No relevant exceptions noted.
17.4 Prior to running the payroll, batch jobs generate files for each output interface, and CPPS generates an error report. These files and error reports are reviewed and a manual reconciliation is performed to verify that the payroll is free of errors.	*Inspected* a payroll reconciliation to determine whether the reconciliation was performed and whether error reports were reviewed in sufficient detail to detect errors.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
COFRS Interfaces		
Control objective 18: Controls provide reasonable assurance that COFRS transactions (and interfaces) are complete and accurate and any errors in processing are followed up on and corrected.		
18.1 All interfaced transactions by agencies to COFRS require advance authorization from the State Controller's Office.	*Inspected* a sample of new transaction interfaces to determine whether advance authorization from the State Controller's Office was obtained.	No relevant exceptions noted.
18.2 Errors detected in COFRS and KRONOS input cannot be processed until the user corrects them online.	*Observed* an attempt to process an input form with errors, and noted the resulting error screen.	No relevant exceptions noted.
18.3 Batches are rejected in COFRS if the transaction count and total amount of the batch do not match the proof totals.	*Observed* an attempt to submit a batch with a transaction count and total amount that did not match with the proof totals, and the resulting system error screen.	No relevant exceptions noted.
18.4 The CORE supervisory routines enforce approval requirements for transactions as defined in the FDOC table for each transaction type. Approvals can only be given by users who have the matching Security Group and Approval Level defined in the ASEC table.	*Inspected* an approved transaction, and verified whether the Security Group and Approval Level defined by the system matched those assigned to the approver.	No relevant exceptions noted.
18.5 In the rare case that a transaction is clearly erroneous and prevents balancing of the ledgers, statewide application services staff will manually modify the ledger record. The statewide application services group maintains an electronic log detailing all such changes. A representative of the State Controller's Office authorizes all changes to the ledgers in writing.	*Inspected* the electronic log for cases where a transaction required manual modification and validated that signature authorization is provided for changes to the ledger.	No relevant exceptions noted.
18.6 Transactions have a unique ID and users are not able to enter two transactions with the same transaction ID within the same accounting period.	*Observed* an attempt to create a transaction with a duplicate transaction ID, and the resulting system error.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
COFRS Interfaces		
Control objective 18: Controls provide reasonable assurance that COFRS transactions (and interfaces) are complete and accurate and any errors in processing are followed up on and corrected.		
18.7 All critical programs in the nightly cycle issue termination codes identifying any processing errors detected by the program. Condition code checking in the JCL and CA7 prevents further processing after serious errors have occurred. In the event of an abnormal termination, an on-call programmer is notified who is then responsible for resolution.	*Inspected* a sample incident ticket to determine whether processing errors are detected and resolved.	No relevant exceptions noted.
18.8 Each morning, system analysts review system assurance reports that compare balance, and other reports that will indicate that transactions were processed completely and accurately.	*Inquired and observed* evidence of daily review of the system assurance reports.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Server Housing and Hosting		
Control objective 19: Controls provide reasonable assurance that server deployment and management processes are common and repeatable to successfully support hosted test and production servers.		
19.1 Project planning documents are used to appropriately configure hosted server resources.	*Observed* whether the Project Planning document is used to identify application requirements.	No relevant exceptions noted.
19.2 Weekly Server management Team meetings help track and assess progress of ongoing projects.	*Inspected* a sample of weeks to determine whether Server Management team meetings were held and whether staff tracked and assessed the progress of ongoing projects.	No relevant exceptions noted.
19.3 Servers are acquired via the OIT procurement approval process, which uses a Purchase Request Form identifying details of the merchandise to be purchased.	*Inspected* a sample of new software utilities and hardware purchases to determine whether appropriate justification and management approval was obtained.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Server Housing and Hosting		
Control objective 19: Controls provide reasonable assurance that server deployment and management processes are common and repeatable to successfully support hosted test and production servers.		
19.4 Server Management team members use a server build document to guide them through the process of deploying the server and assisting the customer through the install of their application.	*Inspected* a sample of server build documents to determine whether they were used in deploying and configuring servers.	A customer web server hosted by OIT did not have any password security enabled. Password weaknesses included: – No history for passwords – No minimum password length (blank allowed) – No password complexity enforced – No account lockout settings implemented A System Administrator maintained the administrator password for this customer web server in clear text and within plain site of other staff at OIT headquarters. The server name, administrative login ID and password were clearly visible to other staff. Per inquiry with management, this web server was hosted by OIT on behalf of the Department of Higher Education and no confidential data exists on the server. The web pages and content on the server are public information. See recommendation No. 2 on page 76.
19.5 A Remedy ticket is created to identify the necessary approval and action requirements needed to properly initiate a change on the server.	*Inspected* a sample of Remedy tickets relating to server builds to determine whether changes to servers are approved and documented.	No relevant exceptions noted.

Controls specified by OIT	*Testing performed by Ernst & Young*	*Results of tests by Ernst & Young*
Server Housing and Hosting		
Control objective 19: Controls provide reasonable assurance that server deployment and management processes are common and repeatable to successfully support hosted test and production servers.		
19.6 All changes are approved by the customer and Server Management team prior to the installation and are sent out as notices five business days prior to the change via the Customer Change Notification email and document.	*Inquired* of OIT to determine whether customers were notified five business days prior to a change to their server. *Inspected* a sample of Remedy tickets relating to server builds to determine whether changes to servers were approved and documented.	No relevant exceptions noted.
19.7 A Netman server (SNMP Manager) monitors NT, UNIX and the mainframe for availability. If a system is unavailable, Service Center personnel notify the network support group, which uses Event Viewer (log viewing program) to access server logs to further troubleshoot the problem.	*Observed* that Netman is used to monitor servers.	No relevant exceptions noted.
Management Response: We have addressed this issue with the administrator and added the password to the central encrypted password file for OIT-hosted servers. Staff have been reminded of security practices. Documented guidelines and policies need to be developed to reflect required access controls and uniqueness. This check and balance will be added to the server build template.		

SECTION FOUR: FINDINGS AND RECOMMENDATIONS

1 Findings and Recommendations

While performing our procedures, we identified certain areas where the control activities and processes could be enhanced or improved. Our findings and recommendations resulting from our procedures are listed below.

Logical Security – Top Secret

Top Secret is the software used by OIT to control logical access to the state mainframe. Properly controlling access to the mainframe's operating system, programs, utilities and libraries is critical to ensuring the confidentiality, integrity and availability of the data maintained in and processed by COFRS and CPPS. Our tests of operating effectiveness noted that controls around the logical security for the mainframe Top Secret environment were not performed during the year, in accordance with the OIT's policy and industry best practices. This resulted in nonachievement of control objective 11: "Mainframe Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of its systems." The specific exceptions that resulted in nonachievement of control objective 11 included OIT's failure to properly restrict high-level access within Top Secret to the appropriate staff and the lack of periodic review of critical Top Secret log files. We discuss these specific exceptions in more detail below.

Two users maintained inappropriate administrative-level access within Top Secret out of a total population of 27 administrators. We determined that these two users' access privileges are inappropriate based on our evaluation of the annual Top Secret review. Additionally, four administrators have excessive administration rights to certain profiles and facilities within Top Secret. These excessive rights were identified by the Data Center operations manager during her annual Top Secret user review. However, the changes identified during the annual review were not implemented, leading to inappropriate administrator access. Failure to restrict administrative rights to Top Secret leads to unauthorized administrator access to the mainframe supporting COFRS and CPPS.

OIT is not consistently following the established process for adding or modifying user accounts on the mainframe. Specifically, documentation for two of a total population of three new user access requests/changes sampled were not documented in the Remedy ticket system and maintained by OIT as required. See "Disposition of prior examination recommendations and resolution" section recommendation No. 1 from the 2009 SAS 70 report. Additionally, an Agency Security Administration (ASA) form was not completed for any of the three new users added this year. Furthermore, no evidence of the required signed Statement of Compliance was found for one out of three new users added to the system. Failure to maintain documentation authorizing account creation and modification could result in a person gaining unauthorized access to systems or data.

Security profile change logs have not been reviewed during Fiscal Year 2010. Additionally, we noted that security log violations for Top Secret were not reviewed after September 2009. A periodic review of the security profile change logs and security violation logs helps in identifying any users with unauthorized access to Top Secret.

Recommendation No. 1:

We recommend that OIT improve the logical security over the mainframe by:

a. Consistently following established controls and standard operating procedures designed to enforce logical security for Top Secret.

b. Establishing a dedicated resource to perform Top Secret administration duties.

c. Reviewing administrative access to Top Secret on a periodic basis and taking the necessary steps to restrict administrator access on the mainframe to authorized individuals.

d. Consistently following the process to document and maintain documentation related to the creation and modification of mainframe user accounts using the Remedy ticket system.

e. Reviewing Top Secret log violation reports and security profile change logs on a periodic basis to identify and investigate unusual activities or violations.

OIT response

Agree: Although controls were developed and had been previously working effectively, OIT did experience an operational and transitional gap in services and systems administration from September 2009 to August 2010. The gap in essential support services and access control administration was due to the unanticipated resignation of the primary system and security administrator in September 2009 and the operational realignment of the secondary system and security administrator during a recent layoff and restructuring initiative that occurred at OIT in October 2009.

On July 1, 2010, 900 employees were consolidated within OIT. As part of that restructuring, OIT has implemented an Access Control Section, which in addition to other duties has the responsibility for long-term administration and access control functions for TopSecret and the related control functions identified above. The Access Control Section consists of approximately 15 information technology professionals, and this depth will provide for succession planning and program coverage.

While there was a gap in this particular control for the time period noted, this is not the only control in place to prevent security violations and breaches. To prevent unauthorized access, each application in the mainframe environment has its own application security, and each department has both an application security administrator and a Top Secret security administrator. In addition, there are business side controls, such as payroll reconciliations and expenditure review and approval in each of the departments, as well as cash reconciliation within the Department of Treasury and vendor control within the Office of the State Controller. All of these controls work in conjunction to mitigate the state's risk. To ensure these additional controls were in place during the above-noted time period, OIT reviewed compensating controls and activity logs for the period to ensure that no unauthorized access occurred.

Implementation Date: Implemented

Server Hosting

A System Administrator maintained the administrator password for a customer web server in clear text and within plain sight of other staff at OIT headquarters. The server name, administrative login ID and password were clearly visible to other staff. Further password security was not enforced for this server.

Recommendation No. 2:

We recommend that OIT develop practices to enforce password security on servers hosted for customer agencies and maintain control around confidentiality of administrator passwords.

OIT response

Agree: The OIT Office of Cyber Security has worked with the Server Management team to address the issue of keeping passwords written on paper and ensure that the current server team password vault solution is being used to maintain and protect the administration credentials of state servers.

In addition, the Office of Cyber Security has procured a state wide license for the Center for Internet Security (CIS) hardening benchmarks to be used as the state security standard for operating systems, network devices and applications. The Office of Cyber Security is currently working with the OIT CTO's office on the socialization and implementation of the CIS standards across all state systems.

Implementation Date: Implemented

Organization and Administration

Standard Operating Policies and Procedures were not regularly reviewed and updated during the fiscal year. Further, an organizational chart describing the various functional departments and job hierarchy was not published. An updated organizational chart, policies and procedures help guide the organization in following standard operating procedures. The lack of a published organizational chart and outdated policies reduce accountability and responsibility across the organization.

Recommendation No. 3:

We recommend that OIT improve its IT governance procedures by updating its policies, procedures and organizational charts annually.

OIT response

Agree: OIT is reviewing all Standard Operating Procedures (SOP) related to Data Center operations and updating them to reflect the effects of consolidated staff and operations. An updated organization chart has been published to the OIT intranet site, which is accessible by all employees.

Implementation Date: *July 2011*

2 Disposition of prior examination recommendations and resolution

2009 SAS 70 Report

No.	2009 recommendation	OIT update response	Status June 2010 (Ernst & Young)
1	Follow the user access process to document and maintain documentation related to the creation and modification of mainframe user accounts using the Remedy ticket system.	Although the controls are in place for those items identified, OIT did experience an operational and transitional gap in services and systems administration from September 2009 to present day. The gap in essential support services and access control administration was due to the unanticipated resignation of the primary system and security administrator in September 2009 and the operational realignment of the secondary system and security administrator during a recent layoff and restructuring initiative that occurred at OIT in October 2009. During this same time period, the OIT Executive Leadership team was in the process of formulating the staff realignment and restructuring phase of the OIT consolidation efforts. This effort identified and placed over 850 Information Technology staff into operational banding units within OIT. The reorganization of these state IT personnel into the newly defined OIT organizational structure was effective on July 1, 2010, and interim staff realignments to mitigate this operational gap could not occur prior to this date. In addition, within the newly adopted organizational structure, OIT has created and implemented the Office of the Chief Technical Officer and a subordinate Access Control Section, respectively. The Access Control Section, under this new organizational structure, has been identified as the responsible entity for long-term administration and access control	Not implemented.

No.	2009 recommendation	OIT update response	Status June 2010 (Ernst & Young)
		functions for TopSecret and those controls functions identified above. The Access Control Section consists of a Level 4 Senior IT Manager with 2 direct reports and 12-15 technical information technology staff. Beginning July 1, 2010, the Access Control Section will begin to identify a primary and secondary administrator to support the mainframe and TopSecret access control functions and validate and revise those control items essential to the long term support and security requirements needed for the secure management of the system.	
2	We recommend that OIT segregate responsibilities for approving, establishing and reviewing user access rights within the COFRS financial system.	OIT will implement segregation of duties for adding or making changes to COFRS access.	Implemented November 2009

Office of the State Auditor's 2008 Information Technology Audit of the OIT Data Center

No.	2008 recommendation	OIT update response	Status June 2010 (Ernst & Young)
1	Implement additional controls to ensure that Top Secret Security Access Identifications (Access IDs) belonging to terminated and transferred employees are identified and suspended by: (a) developing formal procedures agency TSS administrators must follow when setting up new TSS Access IDs and for handling TSS Access IDs belonging to terminated employees and transfers; (b) working with the Department of Personnel & Administration to add state employee ID numbers (EIDs) to each TSS Access ID user profile; (c) developing an automated program to match the CPPS listings of terminated and transferred employees to the names and EIDs associated with active TSS Access IDs and generating and distributing reports containing the names and TSS Access IDs of terminated and transferred employees; and (d) utilizing the reports of terminated and transferred employees with TSS Access IDs to verify that agency TSS administrators have taken appropriate action and follow up as appropriate.	Partially Implemented. OIT recently started a project to strengthen TSS administration. The project will focus on the recommendations from this examination as well as recommendations regarding TSS from the Fiscal Year 08 Statewide Financial and Compliance audit. To date, OIT has completed a project plan and charter, drafted TSS procedures, developed an automated report to identify terminated and transferred individuals, worked with agencies in obtaining and utilizing this report for TSS maintenance and started inputting EIDs into the Access ID data.	Not implemented.

No.	2008 recommendation	OIT update response	Status June 2010 (Ernst & Young)
2	Develop written Service Level Agreements (SLAs) for all customers identifying the agreed-upon services to be provided, the time requirements for those services, and performance measures the Data Center should meet. Provide a list of critical services with agreed-upon response times to operations personnel so customer requests can be prioritized appropriately.	Not implemented. OIT continues to review and update its existing SLAs. Some of the SLAs currently being worked on include Department of Personnel & Administration (DPA), Treasury, and Department of Natural Resources (DNR)-Parks. Additionally, OIT created a governance committee to develop service management MOUs, which will eventually replace SLAs. The service management MOUs will contain expectations/responsibilities regarding staff consolidation under SB08-155 as well as level-of-service requirements based on the services procured by each agency.	Not implemented.
3	Establish a written document retention policy and communicate this policy to all staff.	Partially implemented. In progress. A draft SOP has been developed and is being reviewed by management. OIT expects this SOP to be formally established by January 2011.	Partially implemented.

2007 SAS 70 Report

No.	2007 recommendation	OIT update response	Status June 2010 (Ernst & Young)
1	Consider the use of version control software, including additional resources as required, for application changes, including COFRS.	Not implemented. Funding and FTE do not exist to implement this recommendation.	Not implemented.
2	Review and address the re-engineering of power and signal cable ducts to provide separation and safety in light of current state Data Center consolidation planning.	Not implemented. Complete re-engineering of power and signal cables is a very expensive endeavor. As a result, OIT has implemented other control and testing procedures to ensure proper performance. As server racks are moved in the future, under floor wiring will be addressed.	Not implemented.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 2105

Report Control Number 2105