Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit

Report on Controls Placed in Operation and Tests of Operating Effectiveness

Period from July 1, 2006 through June 30, 2007

LEGISLATIVE AUDIT COMMITTEE
2007 MEMBERS

Senator Stephanie Takis
Chair

Representative James Kerr
Vice-Chair

Representative Dorothy Butcher
Senator Jim Isgar
Representative Rosemary Marshall
Representative Victor Mitchell
Senator Nancy Spence
Senator Jack Taylor

Office of the State Auditor Staff

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Kevin Sear
Legislative Auditor

BKD, LLP

Rob MaCoy
Rodney Walsh

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007

Contents

Section

This Page Intentionally Left Blank

Section I
Independent Service Auditors' Report

Independent Service Auditors' Report

To Members of the State of Colorado Legislative Audit Committee:

We have examined the accompanying description of controls provided by Division of Information Technologies (DoIT) Data Center and Technology Management Unit (DC/TMU) relative to selected services provided to system users by DC/TMU, including users of the COFRS (Colorado Financial Reporting System) and CPPS (Colorado Personnel Payroll System) applications, related EMPL / HRDW and Document Direct interfaces, and Data Center Housing and Hosting Activities. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of DoIT's controls that may be relevant to a user 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 user organizations applied the controls contemplated in the design of DoIT's controls; and (3) such controls had been placed in operation as of June 30, 2007. The control objectives were specified by the management of DoIT. Our examination was performed in accordance with the 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 DoIT controls presents fairly, in all material respects, the relevant aspects of DoIT's controls that had been placed in operation as of June 30, 2007. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of DoIT'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 V of this report, to obtain evidence about their effectiveness in meeting the related control objectives, described in the Control Objectives Matrices of Section V, during the period from July 1, 2006 through June 30, 2007. The specific controls and the nature, timing, extent and results of the tests are listed in the Control Objective Matrices of Section V. This information has been provided to user organizations of DoIT and to their auditors to be taken into consideration, along with the information about the internal control of user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in the Control Objective Matrices of Section V, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the Control Objective Matrices of Section V were achieved during the period from July 1, 2006 through June 30, 2007. However, the scope of our engagement did not include tests to determine whether control objectives not listed in the Control Objective Matrices of Section V were achieved; accordingly, we express no opinion on the achievement of control objectives not included in the Control Objective Matrices of Section V.

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

The description of controls at DoIT is as of June 30, 2007, and information about tests of the operating effectiveness of specific controls covers from July 1, 2006 through June 30, 2007. Any projection of such information to the future is subject to the risk that, because of changes, the description may no longer portray the system in existence. The potential effectiveness of specified controls at DoIT is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

The information included in Section VII is presented by DoIT to provide additional information to user organizations and is not a part of DoIT's description of controls that may be relevant to user organizations' internal control as it relates to an audit of financial statements. The information in Section VII has not been subjected to the procedures applied in the examination of the description of the controls related to DoIT, and accordingly, we express no opinion on it.

The information included in Section V and described severally as "Department of Personnel & Administration's Response" is presented by DoIT to provide additional information to user organizations and is not a part of DoIT's description of controls that may be relevant to user organizations' internal control as it relates to an audit of financial statements. The information in Section V and described severally as "Department of Personnel & Administration's Response" has not been subject to the procedures applied in the examination of the description of the controls related to DoIT, and, accordingly, we express no opinion on it.

This report is intended solely for use by the Members of the State of Colorado State Legislative Audit Committee and management of DoIT, the user organizations, and the independent auditors of the user 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.

/s/ **BKD, LLP**

Kansas City, Missouri
September 6, 2007

This Page Intentionally Left Blank

Section II
Report Summary

Authority, Standards and Purpose/Scope of Examination

This examination of the general controls at the Division of Information Technologies (DoIT) Data Center and Technology Management Unit (DC/TMU) was conducted under the authority of Section 2-3-103, CRS, which authorizes the Office of the State Auditor to conduct audits of all departments, institutions and agencies of state government. (Please refer to Section IV for a description of the DoIT and DC/TMU organization.) This examination was conducted in accordance with standards established by the American Institute of Certified Public Accountants (AICPA). The period under review was July 1, 2006 through June 30, 2007.

SAS 70 Overview

The SAS 70 (Statement on Auditing Standards No. 70, *Service Organizations*) is an auditing standard developed by AICPA. The SAS 70 provides guidance that allows a service organization such as DC/TMU to disclose its control activities and processes to its customers (user organization) and its customer's auditors (user auditor). The service organization employs an independent accounting and auditing firm (service auditor) to examine its control objectives and control activities. The service auditor issues a Service Auditor's Report to the service organization at the end of the examination that includes the auditor's opinion.

Objectives of the Examination

This report on examination of controls placed in operation is intended to provide interested parties with information sufficient to understand the basic structure of controls within DC/TMU. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding transactions processed through the reviewed systems.

Our examination was restricted to selected services provided to system users by DC/TMU, including users of the COFRS (Colorado Financial Reporting System) and CPPS (Colorado Personnel Payroll System) applications, and related EMPL / HRDW and Document Direct interfaces, and, accordingly, did not extend to controls in effect at user locations. It is each interested party's responsibility to evaluate this information in relation to controls in place at each user location in order to assess the total system of internal control. The user and DC/TMU portions of the system must be evaluated together. If effective user controls are not in place, DC/TMU controls may not compensate for weaknesses.

Auditors using this report as part of their review of a user's system of internal controls may conclude that DC/TMU's description of controls provides a basis for reliance thereon and for restricting the extent of their substantive tests. Alternatively, user auditors may elect not to rely on controls within DC/TMU's system. In that event, they should accomplish their audit objectives by other means.

The objectives of data processing controls are to provide reasonable, but not absolute, assurance about such things as the following:

- Protection of data files, programs and equipment against loss or destruction
- Prevention of unauthorized use of data records, programs and equipment
- Proper handling of input and output data records
- Reliable processing of data records

The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits derived and, additionally, that evaluation of internal control necessarily requires estimates and judgments by management.

Summary of Major Audit Comments

A complete listing of our recommendations from this year's examination and management's responses may be found in Section III – Recommendation Locator. Additional details regarding the following recommendations, plus additional recommendations of lesser significance, may be found in Section V – Information Provided by the Service Auditor.

It should be noted that in several instances, the recommendations are the logical result of an exception noted during the examination. However, a number of recommendations refer to control objectives and activities that did not exhibit an exception during the examination. This is a result of the Division of Information Technologies successfully meeting the objective, but a best practice recommendation is being made to offer improvements to current established controls.

The following summarizes the more significant findings contained in this report:

- While reviewing the list of terminated employees against valid Top Secret Security Access Identification (TSS ACIDs), we noted there was not a clear procedure for employees who have had a change in status. During our audit, it was particularly noted that contractors that had a change in their status from contractor to employee showed on the terminations listing, although they had actually had a status change resulting in their access account remaining active. This results in confusion when reviewing the terminated employee listing. We recommend implementing an additional formal process with regard to terminated employees to validate that their ACIDs should be either suspended or marked as not being recycled for a determined time period, or remain active due to a status change. We recommend creating an exception report that shows terminated employees and also identifies individuals that were not actually terminated but had a change in their employment status (for instance, a contractor that changed from temporary to a full time employee, etc.).

- Although servers are protected with anti-virus software, we observed that the scan parameter is disabled on servers because of performance issues. We also observed that Linux servers are not utilizing any form of antivirus (AV) software. It is commonly felt that properly configured Linux systems are more resistant to attack because most Linux applications are owned by the Root account (administrator), and most users have a non-privileged account. We recommend that DoIT purchase and install anti-virus software for the Linux servers and that all servers be set to periodically scan for virus infections.

- Data Center personnel review System Management Facility (SMF) information on a regular basis to monitor system performance and usage and ensure infrastructure is appropriate to need. During our testing, it was noted that the technical support staff reviews the information, usually on a daily basis. However, there is no documentation of the review process supporting that a review was performed. We recommend that DoIT implement a procedure to document the review of SMF information.

- During our audit, it was noted that some of the supporting documents were not retained for the entire audit period. To form a proper conclusion as to the operating effectiveness of a control activity, it is crucial to have adequate data to test from throughout the audit period. We recommend DoIT review its document retention policies and require that documents demonstrating performance of control activities be retained for at least one year.

Summary of Progress in Implementing Prior Audit Recommendations

The Division of Information Technologies Data Center and Technology Management Unit have made significant progress in implementing the recommendations from prior audits and reports covering the period from April 2000 through June 30, 2005. A complete discussion of the status of implementation is provided in Section VI – Status of Implementation of Prior Recommendations.

Section III
Recommendation Locator

Recommendation Locator

No.	Figure Reference(s)*	Recommendation	Agency Response	Implementation Date
1	13.18, 13.19	We recommend that DoIT implement a standard procedure for documenting both the weekly and monthly reviews of the security violations logs and the security profile changes logs within Top Secret.	Agree.	11/30/07
2	13.1, 13.4	We recommend that DoIT implement an additional formal process to validate that terminated employee's Access Identification should be either suspended or marked as not being recycled for a determined time period, or remain active due to a status change.	Agree.	12/31/07
3	21.all	We recommend that DoIT ensure that current signed Service Level Agreements are on file and tracked for all DoIT server housing and hosting customers. SLAs should clearly define services to be provided by DoIT, responsibilities of the user and performance measures that DoIT should meet.	Agree.	9/30/08
4	3.3, 12.1	We recommend that DoIT establish a review process to ensure that new hire checklists are properly filed and vendor performance reports are completed in a timely manner.	Agree.	12/31/07
5	6.3	We recommend that DoIT implement a process to designate responsibility to the employee host to ensure all visitors successfully follow all visitor control procedures, including the return of badges and signing out of the visitor log after hours.	Agree.	12/31/07
6	14.2	We recommend that DoIT purchase and install anti-virus software for the Linux servers and that all servers be set to periodically scan for virus infections.	Agree.	3/1/08
7	21.4	We recommend that DoIT implement a Server Build configuration check off sheet to be completed by the DoIT hosted server staff. The check off sheet should be maintained in DoIT customer files for each system added.	Agree.	3/1/08

*Figure References refer to Section V Control Matrices of the 2007 SAS 70 report.

No.	Figure Reference(s)*	Recommendation	Agency Response	Implementation Date
8	2.4	We recommend that DoIT re-emphasize the outage reporting process and ensure that all outages are reported.	Agree.	3/1/08
9	9.2	We recommend that DoIT implement a procedure to document the review of System Management Facility (SMF) information. Also, DoIT should consider training another employee as a backup to ensure that review is performed on a timely basis in case the regular reviewer is not available.	Agree.	3/1/08
10	General	We recommend that DoIT conduct a periodic meeting (at least on a quarterly basis) of the members of management to ensure that control documentation is updated on a regular basis to reflect the actual controls and procedures in place, to evaluate the effectiveness of current or proposed controls, and to review prior year audit suggestions/recommendations to ascertain they are being implemented on a consistent basis during the year.	Agree.	12/1/07
11	General	We recommend DoIT review its document retention policies and require that documents demonstrating performance of control activities be retained for at least one year.	Agree.	12/1/07
12	Section VI: Prior Recommen-dations	We recommend DoIT consider the use of version control software for application changes.	Partially Agree.	Not Determined
13	Section VI: Prior Recommen-dations	We recommend DoIT review and address the separation of power and signal cable ducts in light of current State data center consolidation planning.	Partially Agree.	Not Determined

*Figure References refer to the Section V Control Matrices of the previously noted 2007 SAS 70 report.

Section IV
Description Provided by the Division of Information Technologies Data Center and Technology Management Unit

Division of Information Technologies Overview

Background

The Division of Information Technologies (DoIT) Data Center, formerly the Colorado Information Technology Services Data Center, was originally established as a division in the Department of Administration on July 1, 1978, as a service organization to deliver data processing services to various governmental entities. Today, the Data Center is the result of the consolidation of several data centers over the last 29 years.

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 the hardware and operating system can be recovered in case of a physical disaster to 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 Division'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 DoIT 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. They suggest the Data Center 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, seven days a week on-site staffing for operations and Service Center personnel plus environmental controls, fire suppression system, uninterruptible power supply (UPS), generator backup and space for additional equipment.

Data Center customers continue to move to new technologies and the Division of Information Technologies is partnering with them to deliver state-of-the-art IT solutions. In particular, the Data Center is helping customers expand their distributed systems by developing more capability in the area of "virtual servers" and "web enablement" technologies. The total number of servers residing at the Data Center grew from a total of 128 in fiscal year 2001–2002 to 367 in fiscal year 2006–2007. Today a server can be implemented on one individual, physical piece of equipment (a server) with its own resources (like storage and memory) or multiple servers, called virtual server instances, can be created on one physical piece of equipment with shared resources. The use of virtual servers allows the conservation of resources and physical space in the data center. They are also more rapidly implemented since the time it takes for the purchase of equipment for each server is eliminated. Included in today's server farm numbers noted above are 100 virtual server instances residing on six physical servers.

The Data Center has 9,075 square feet of raised floor space containing the computer room, server farm, office space, Service Center and print and distribution areas. Power from Xcel Energy is obtained through one power grid, which the Data Center manages with five power distribution units (PDU) and two extension units. Fail-over power is available through a standby generator located adjacent to the Facility. This generator currently operates at approximately 75% of capacity allowing room for Data Center expansion.

The Data Center is supported by a UPS system to ensure continuous availability of electrical power between the initial interruption of power and the standby generator coming on line. The UPS system operates at approximately 60% of capacity, leaving adequate room for Data Center expansion. The state's Capitol Complex maintenance staff manages both the generator and the UPS.

The raised floor environment is adequately controlled with six high-capacity air conditioning units and three humidifiers. The Data Center is protected by a fire suppression system using the ozone-friendly FM-200 extinguishing agent.

Organization and Management

DoIT, ITU and the Technology Management Unit (TMU) reside under the Department of Personnel and Administration (DPA), which is part of the Executive Branch of the State of Colorado government. Through March of 2007, the Director of the Division of Information

Technologies fully reported to the Executive Director of DPA who in turn reported to the Governor of the State of Colorado. In March of 2007, the DoIT Director started reporting to the State CIO operationally and continues to report to the DPA Executive Director for administrative functions such as Human Resources and Purchasing. The State CIO and the DPA Executive Director both report to Colorado's Governor.

The Data Center is a cash-funded agency with more than 90 billable customers in more than 30 state departments, institutions and agencies. Billable items include computer processing time, data storage space, printing charges and database support. Funds for these items are appropriated to each department, with the Data Center receiving matching cash spending authority. The money in the cash fund is subject to annual appropriation. During fiscal year 2007, the Data Center received an appropriated spending authority of approximately $12 million to provide computer services to state agencies.

The TMU is responsible for acquiring, implementing, operating and maintaining statewide information systems for the State of Colorado.

The Data Center operates 24 hours per day, seven days a week, including holidays. Approximately 60 of the DoIT 175 full-time equivalents (FTE) are directly involved with the Data Center. These FTEs include the following:

- **Management:** The DoIT Division Director spends approximately 50% of his time in the management of the Data Center; the Computing Services Manager is engaged full-time in Data Center management.

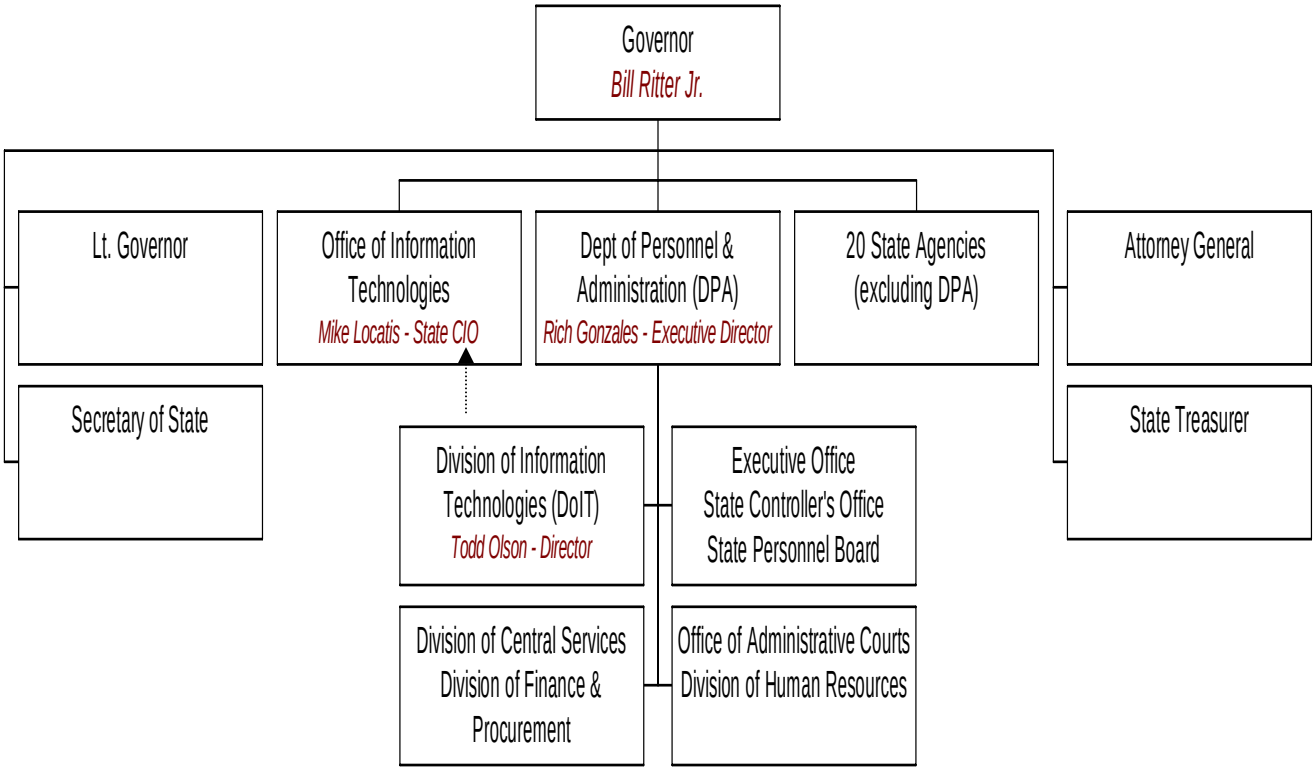
- **Business and Administrative Services:** These are support services required to operate the Data Center. Services including budget preparation, control and monitoring. Also included are internal accounting, personnel functions, word processing and switchboard/receptionist services at the Data Center.

- **Customer Support Services:** These are the direct customer support services personnel. Responsibilities include change management, security and handling customer service requests for informational reports extracted from system files in a short time period. The disaster recovery function within this area is responsible for developing, implementing, coordinating and monitoring the Data Center's disaster recovery plan.

- **Technical Services:** These services include the installation, implementation and maintenance of all computer systems software at the Data Center. Technical Services also provides support for all shared databases and support activities. Technical Services staff perform hardware and software evaluations and provide technical training and documentation for Data Center customers. Server and local area network equipment directly operated by DoIT is supported within this functional group as well.

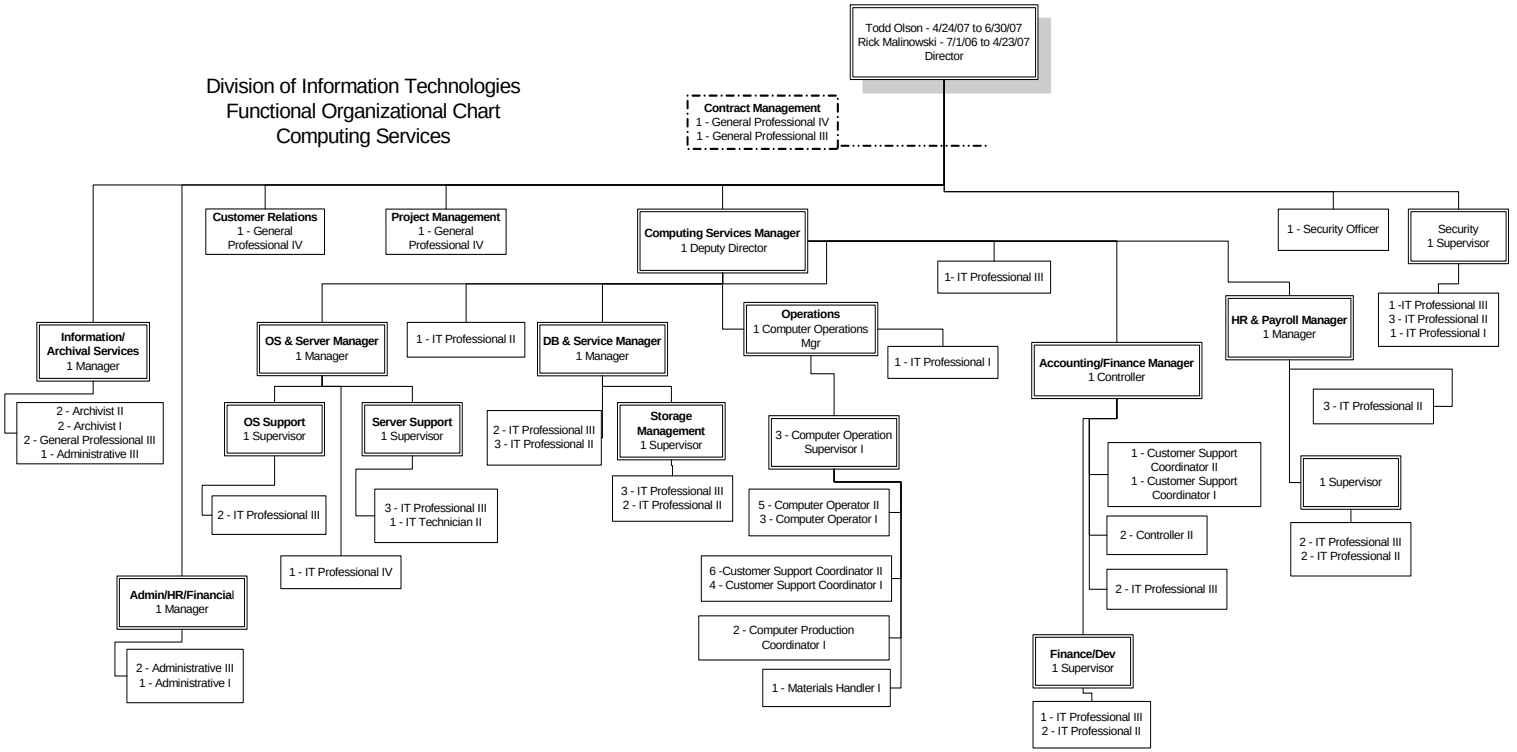
- **Computer Operations:** These services include installing and operating computer and printing equipment, maintaining disk and tape systems hardware and the control and distribution of computer output. The Service Center is a functional area within Computer Operations providing job scheduling and monitoring, console management and service desk support. The Service Center is the central point of contact for DoIT customers for handling customer service requests.

Organizational Charts

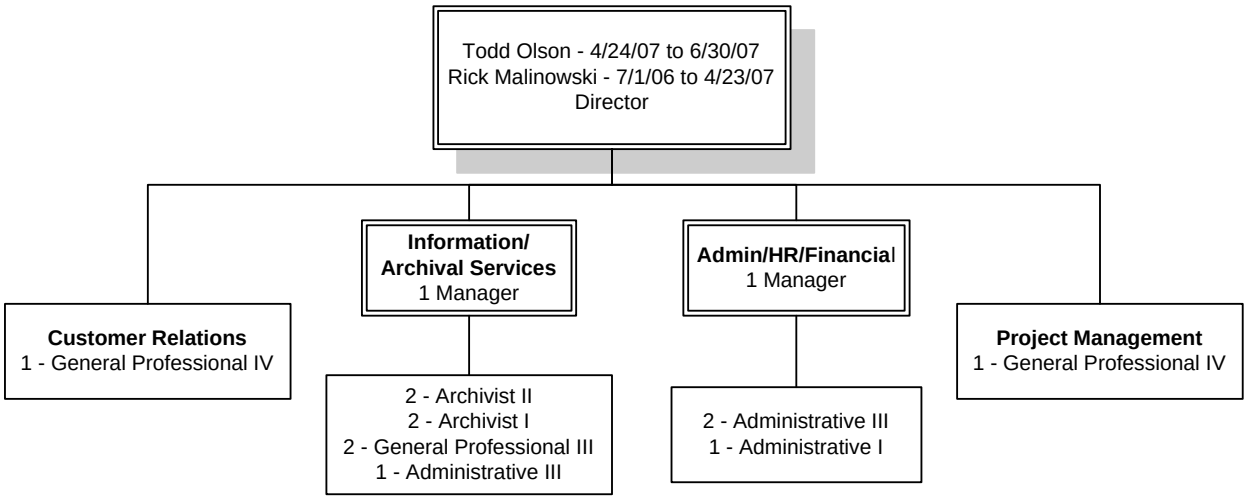


Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit

Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007

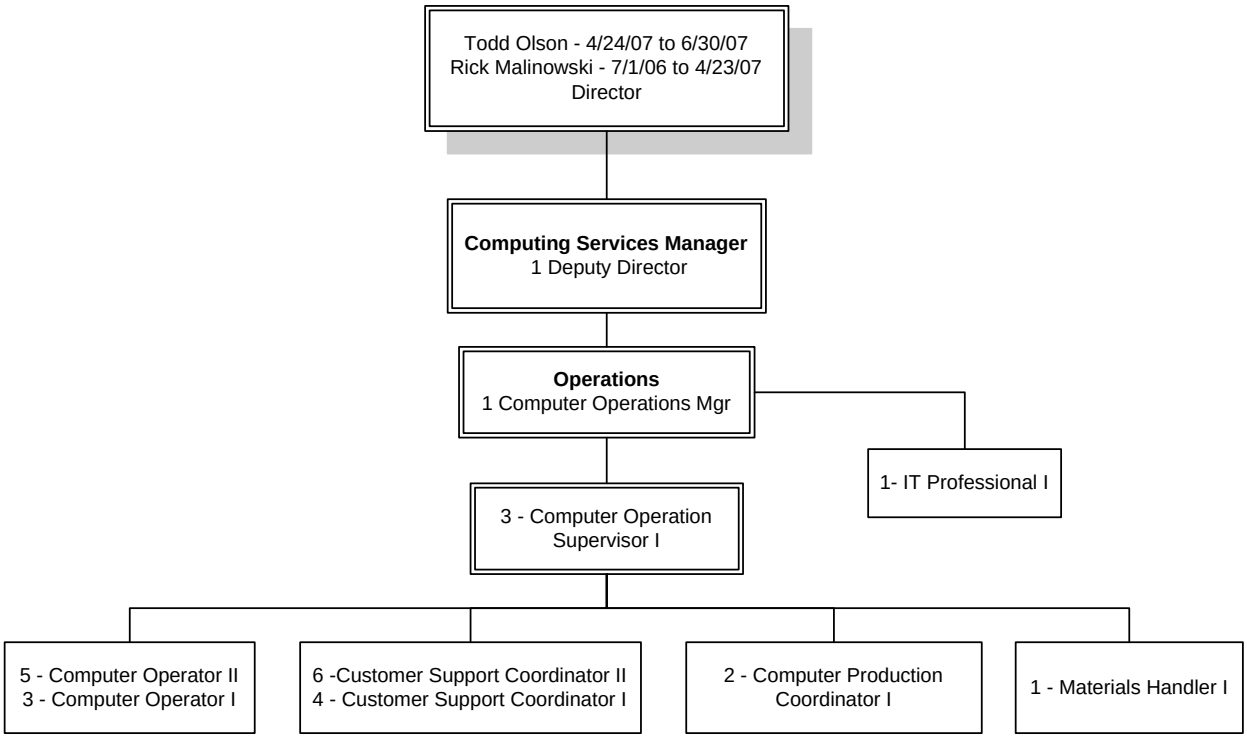


Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007



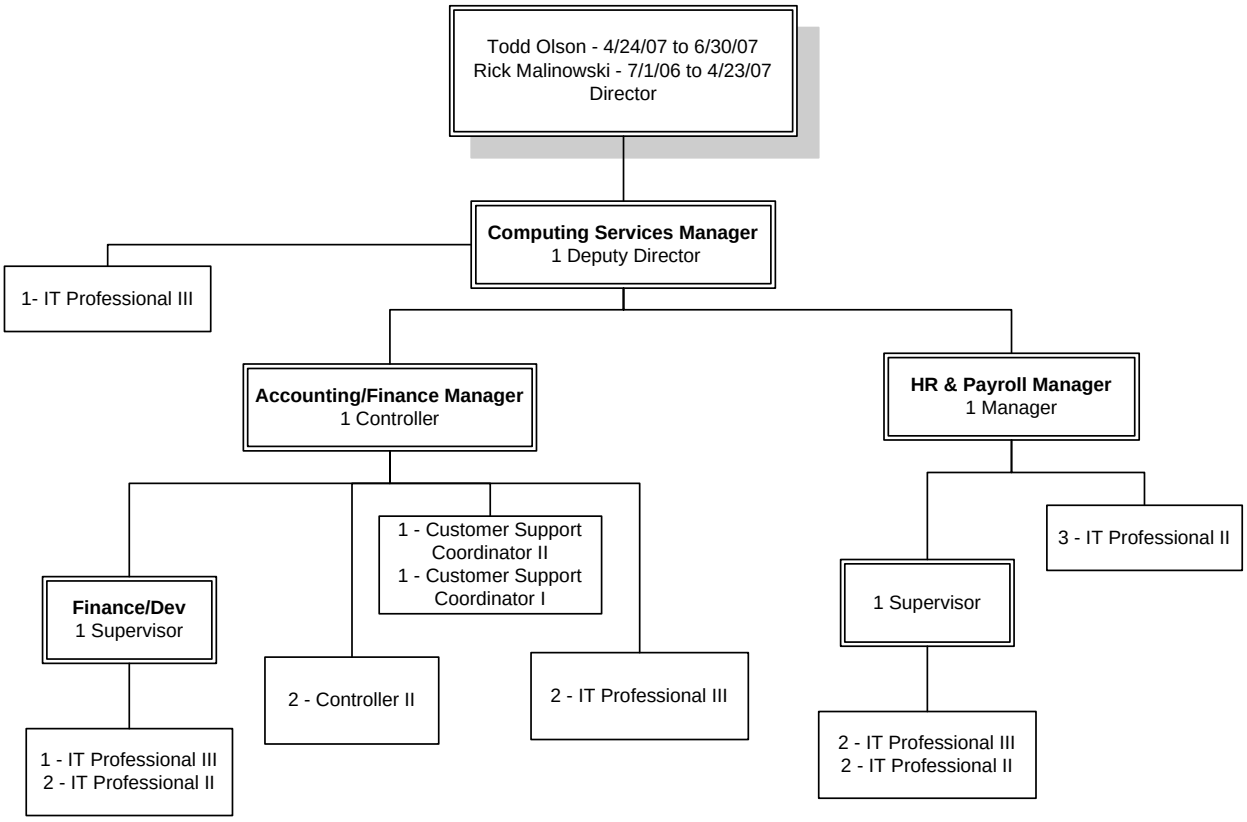
Archives/Admin

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007

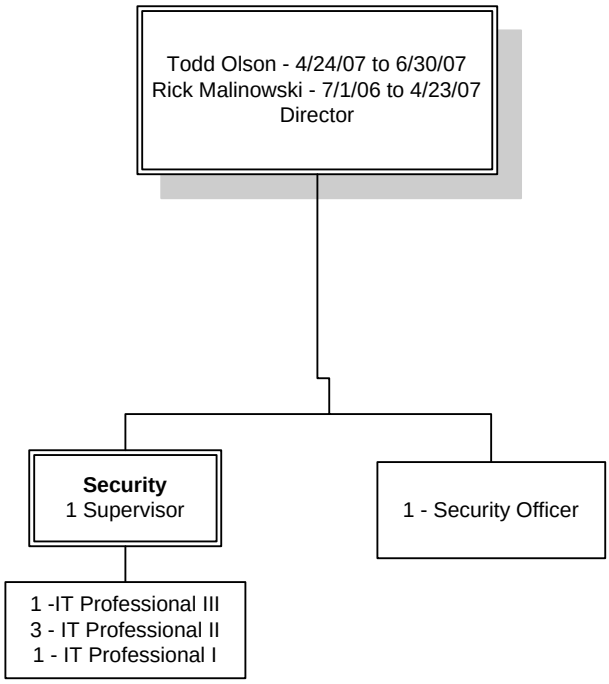


Operations

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007

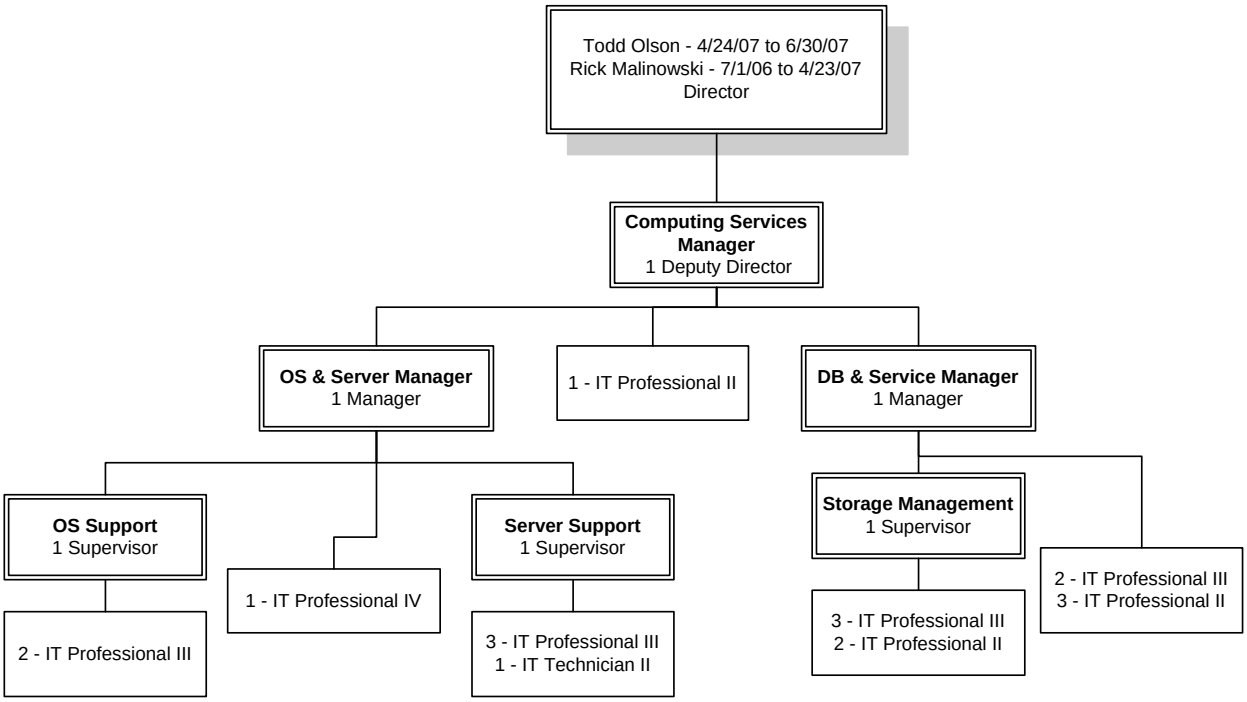


Application Services


Todd Olson - 4/24/07 to 6/30/07
Rick Malinowski - 7/1/06 to 4/23/07
Director
Security
1 Supervisor
1 - Security Officer
1 -IT Professional III
3 - IT Professional II
1 - IT Professional I

Security

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2006 through June 30, 2007



IT Support

DoIT General Services

DoIT offers services to state agencies in an effort to consolidate efforts of multiple agencies into one environment. The Computing Services Operating System (OS) Technical Support and Software Support teams within DoIT offer Mainframe Application Hosting services and provide the platform where many of the statewide applications run. These groups 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 DoIT system. Therefore it would not be reasonable for DoIT 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 DoIT customers. The same holds true for Software Support on the mainframe. This is common practice in the mainframe environment.

The Computer Operations team (outlined on page 13) 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.

The Server Management team provides and maintains the hardware and operating systems for servers hosted at the DoIT Data Center, while their customers maintain their own applications on these hosted servers. 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. 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 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 TMU for those applications that are used commonly among all state agencies. These applications are the Colorado Financial Reporting System (COFRS) the accounting system for Colorado government, 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, the Colorado Personnel and Payroll System (CPPS) the state employee payroll system 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 DoIT services, the major customers are the Colorado Department of Human Services (CDHS), the Department of Revenue (DOR), DPA and the Colorado Department of Labor and Employment (CDLE). These departments make use of all of the services identified with the one exception; CDLE does not utilize DoIT's Server Housing or Hosting services.

DoIT General Services Descriptions

- Mainframe Application Hosting
- Server Hosting and Housing
- Data Storage and Management
- Computer Operations
- Security
- Statewide Applications

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 DoIT Computing Services OS Tech Support and Software Support teams have managed, operated and maintained an IBM z890 Enterprise Server with Integrated Facility for Linux (IFL) since September of 2005. The z890, rated at 500 Million Instructions per Second (MIPS), runs the z/OS 1.7 operating system in one partition and VM/Linux in the other partition, and has 8 GB of memory.

In addition, the IFL component provides the facility the means by which multiple distributed system servers can be aggregated into the architecture without acquisition of additional physical servers. Together, the IBM z890 and the IFL allow personnel to work in compliance with the Colorado Statewide IT Plan by implementing an Enterprise Server (mainframe) architecture that continues to provide support for aggregated legacy mainframe processing while supporting aggregated distributed system processing. The z890 Enterprise Server allows for usage-based billing from IBM.

All DoIT 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 only has access to their files, unless access to other files is specifically permitted by another agency's administrator.

Server Hosting and Housing

Server hosting is a service that has grown and will continue to grow as state agencies choose to contract with the Division of Information Technologies 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 DoIT Data Center. The Division of Information Technologies is implementing server consolidation options through such platforms 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 Tech 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 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 services, the Data Center has invested in SAN (Storage Area Network) 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.

Data Storage and Management

DoIT leases an EMC DMX1000 SAN (4 Terabytes (TB)) and owns an EMC DX300 (9.5 TB) SAN. 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:

- Two – 3420 (round reel) tape drives (read only)
- 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 back store tapes

The tape media supports archival, batch processing, disaster recovery and customer offsite 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 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 automated tape library supports distributed tape storage activities. Symantec NetBackup is used to manage open systems backup tasks.

Computer Operations

Computer Operations is responsible for monitoring of hardware and the Data Center environment in support of all DoIT services and customers. Computer Operations ensures that individuals entering the computer rooms follow the DoIT access procedures. This group also provides print services and tape handling services, report distribution and warehouses print forms inventories for stock provided by 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 Service Center within Computer Operations is the single point of contact for customers. The Service Center provides service desk, job scheduling and monitoring, and systems monitoring for DoIT and its customers.

Security

The ISOC performs several security functions that include the following: perimeter security at the Internet Gateway, mainframe security through the use of Top Secret Security (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 data sets is controlled through Top Secret Security administration.

Desktop security for DoIT is managed by DPA's Information Technology Unit (ITU). (ITU is the IT organization specifically assigned to meet DPA IT needs, including desktop support for DPA employees, application support for DPA-specific applications, and server support for DPA-specific servers).

Statewide Applications

TMU Human Resources and Payroll Applications

The **Applicant Data System (ADS)** is the applicant tracking system for the State of Colorado. This system tracks job applicants, employment tests and test schedules and monitors the applicant selection process for the State. Developed by State employees in 1992, the system allows personnel administrators to monitor the status of applicants throughout the application and testing process. The ADS system is used for tracking all state jobs, including the judicial branch and higher education positions.

In 1998, a separate job announcement system for posting job announcements on the Internet was developed and implemented. In 2003, the system was enhanced to allow applicants to complete job applications over the Internet.

The ADS system is developed utilizing the ADABAS database management system with Natural coding language. The Job Announcement system was developed with Lotus Notes. The job application is a Java-based system utilizing TN3270 emulation to interact directly with the ADABAS system.

The **Colorado Personnel Payroll System (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 sub-system for reporting insurance premiums. The CPPS system is currently supported by TMU for system modifications and vendor supplied software updates.

The CPPS system is developed in the COBOL language using VSAM file structures. Ad hoc reporting is accomplished using the FOCUS programming language.

The **Employee Data Base (EMPL)** system was the State of Colorado Human Resource system of record. The EMPL system was responsible for maintaining current and historical information on all employees, positions and job classifications. The EMPL system was developed by State employees in 1981 for use by all State agencies, certain higher education institutions and the judicial branch of government. Since initial implementation, the software has been heavily modified as State personnel policies have been updated. The EMPL system was developed using the ADABAS database management system with Natural and COBOL coding languages. The

EMPL system was retired in fiscal year 2007 and pertinent data stored in the Human Resources Data Warehouse.

The **Human Resources Data Warehouse (HRDW)** is responsible for maintaining current and historical information on all employees, positions and job classifications. The HRDW system was developed by State employees in 2005 for use by all State agencies, certain higher education institutions and the judicial branch of government. The HRDW system is developed using a Web-FOCUS Application Server for web access and is supported by a MySQL database.

TMU Financial Applications

The **Colorado Financial Reporting System (COFRS)** is the accounting system of final record used by the State of Colorado. All state agencies except 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 State licensed two software applications, (1) CORE and (2) the Government Financial System (GFS) from American Management Systems (AMS) in 1989. The State has extensively customized the software and neither the CORE nor the GFS software is maintained by the vendor. The GFS software is maintained by TMU and has been significantly modified and enhanced to meet the specific needs of the State. These modifications preclude upgrading to new versions of GFS.

The original purchase of COFRS was supported by the State Auditor's Office who needed one auditable system to replace the many different departmental systems in place. 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 (Virtual Sequential Access Method) file structure. The CORE software (database and file handling routines) of COFRS is implemented in a mixture of Assembly language and COBOL.

The **Financial Data Warehouse (FDW)** is a research and reporting tool for selected COFRS tables and all COFRS accounting, budget and grant transactions. This system was developed in 1999 and went live in January 2000. The system allows users to see summary information by year-to-date, accounting period or daily amounts and then, if needed, the users can drill down into the detail transactions that make up the balance.

FDW uses the Information Builders, Inc. (IBI) WebFocus reporting tool. The database is Microsoft SQL Server 2000 and the web pages were built using active server pages. The database is loaded daily with COFRS transactions and tables.

KRONOS – is a vendor-provided timekeeping/leave tracking system. The KRONOS system was implemented in July 2001 as a result of a New Century Colorado (NCC) recommendation that the State of Colorado implement a statewide system to centralize labor force timekeeping and seek consistent standards and compliance in performance, accuracy and accountability.

The Department of Public Health and Environment and the Department of Natural Resources implemented the statewide version of KRONOS in July 2001. The Department of Labor and Employment joined the statewide system in April 2004; the Department of Personnel &

Administration implemented it in July 2004 and Secretary of State in July 2006. In December 2006, the system was upgraded to the most current version of KRONOS and was converted from an Oracle environment to a SQL server environment.

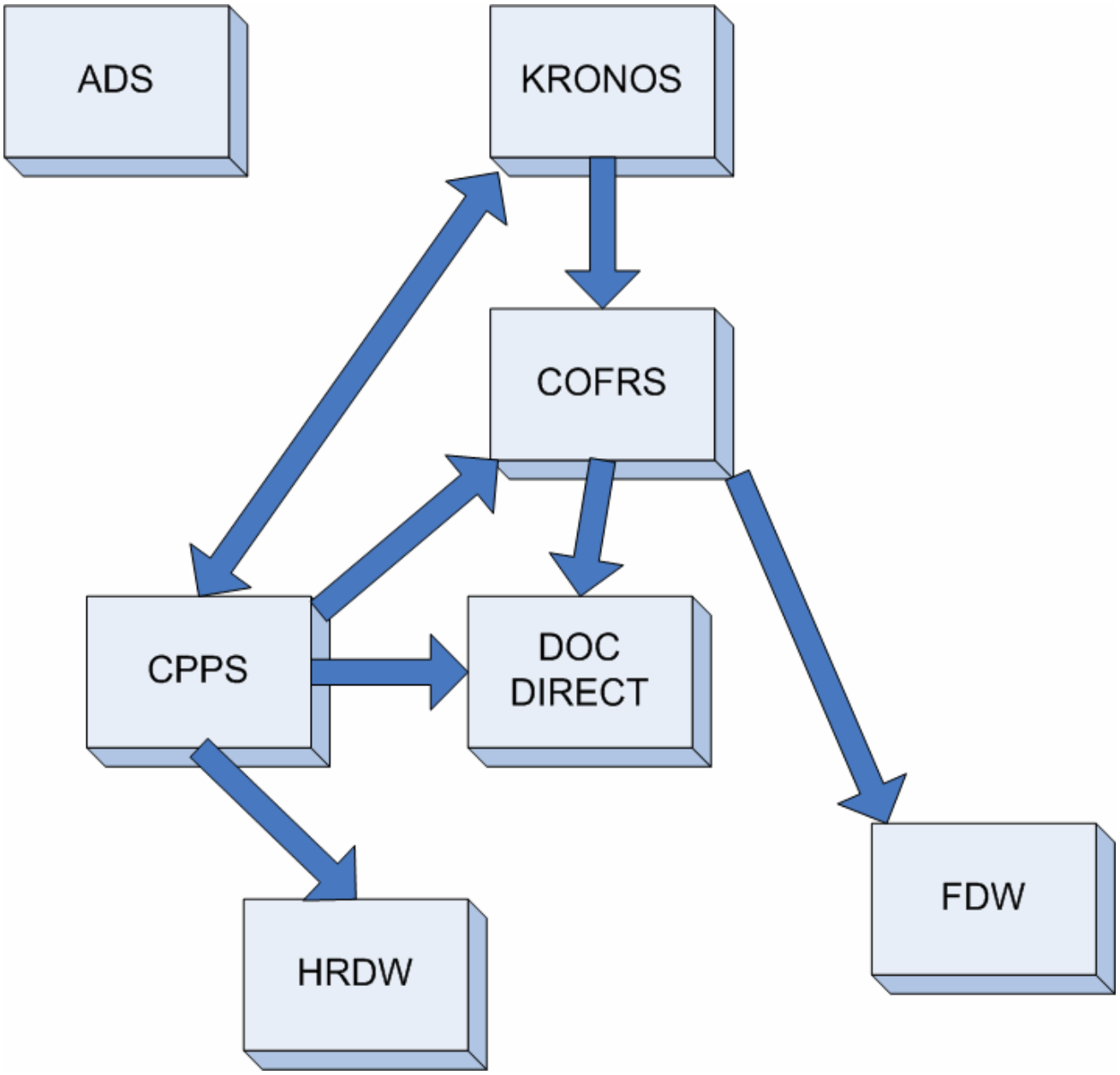
Data Storage Application

Document Direct - Document Direct for the Internet (DDRInt) provides Internet viewing access to reports that have been produced on the mainframe and is managed by software support staff at DoIT. DDRInt works in conjunction with another Mobius software product, ViewDirect, which collects the reports produced on the mainframe and stores each report version in a VSAM file. The primary reports currently accessible are COFRS accounting reports and payroll/personnel and billing reports.

DDRInt and ViewDirect were purchased to replace the Report Distribution Management system, which was part of the original COFRS software. The choice of the Mobius products came after researching many other similar products that provided online report viewing. The feature that swayed the decision in favor of Mobius was the ability to view reports that had been archived to tape directly from the tape without having to restore the report back to disk.

Relationships between Supported Systems

These systems are interrelated through interfaces and extracts as shown below.



Descriptions of Controls

Description of Controls – Strategic Planning

DoIT management prepares strategic plans for Information Technology (IT) that aligns 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 to meet established objectives. IT plans are communicated to DoIT customers and employees, and to the State's department CIOs. DoIT senior management or their designees oversee the IT function and its activities and communicates its activities, challenges and risks on a regular basis with DoIT's Executive Director.

Description of Controls – Organization and Relationships

DoIT is responsible for managing all aspects of the system environment ensuring 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 CIOs. Formal job descriptions, called Position Description Questionnaires (PDQ) are kept for all DoIT state employees. Each position and its relationships within DoIT are described on an organizational chart that is kept current and made available to staff on the DoIT 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 and other contract personnel are subject to policies and procedures to assure the protection of the DoIT's and DoIT's customers' information assets.

Description of Controls – Human Resource Management

State personnel rules and procedures are followed in all areas concerning the hiring, promotion, leave administration, annual performance management and termination of DoIT employees. Additionally, Department and Division 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.

DoIT employs the DPA performance appraisal system 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.

Description of Controls – Communication

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

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

Consistency and control are addressed through the publication, maintenance and use of standard operating procedures (SOPs). Standard Operating Procedures are managed in accordance with DoIT SOP #0001. SOPs are reviewed annually against current operations to ensure consistency and alignment with DoIT business objectives. When SOPs are published, an email is sent to Computing Services staff notifying them of the updates.

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

Description of Controls – Risk Assessment

DoIT 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 DoIT's viability, reliability and ability to achieve business objectives. The IT organization's insurance and liability risk is managed at the State level by the DPA Division of Human Resources (DHR).

Description of Controls – Facility Management

All visitors to DoIT 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 complete the roster with their name, time in and whom 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.

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 an uninterruptible power supply (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 on-line. 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. In the fall of 2003, the Data Center's halon fire suppression system was replaced to accommodate the ozone-friendly FM-200 extinguishing agent used today. The Data Center FM-200 fire suppression system is inspected semi-annually and annual training is provided to the Computer Operations staff

on the FM200 system and operation of portable fire extinguishers. Smoke detectors are located above and below the Data Center's raised flooring and directly linked to the fire suppression system. Below-floor water detection devices are located throughout the raised floor area. State Capitol Complex Facilities is the custodian for the Data Center building at 690 Kipling Street, 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 state patrol who will call the fire department if an alarm is activated.

Description of Controls – Quality Management

DoIT performs a variety of review, audit and inspection activities for quality control purposes. Management regularly reviews capacity and performance metrics. DoIT also posts a monthly executive dashboard on the DoIT intranet site. An annual Top Secret access review for Computing Services is completed by management each year to ensure that access to data remains appropriate for individual staff members at DoIT. Annual reviews of SOPs against current operations are performed by the responsible manager and ratified by additional management personnel. Major system outages are documented in the Remedy problem tracking system and summarized in the Service Outage Notification Report that is distributed to senior management.

Description of Controls – Software Acquisition Management

Acquisition of new software requires business justification and manager approval. The Data Center will request funding for software products only when multi-customer 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. The inventory of system software is complete, audited periodically against software installed throughout the Organization and is kept current.

Description of Controls - Technology Acquisition Management

Acquisition of new technology requires business justification and manager approval to ensure 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 customer's application workload. SMF data is 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 format and is made available to requesting customer agencies. Hardware acquisitions may include pre-paid maintenance and support, or funds for renewal of maintenance and support are encumbered prior to expiration.

Description of Controls – 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, an implementation schedule is published to the customers and affected clients are notified via email, telephone or broadcast message prior to placing a change request 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.

Description of Controls – Service Level Management

The Service Level Manager is responsible for ensuring the establishment of service-level performance monitoring and reporting to DoIT management. Service Level Agreements (SLAs) are executed for many server-hosting customers as part of project implementation. Some other DoIT services such as HRDW have SLAs in place with defined service and performance levels for a common understanding of expectations.

Description of Controls – Management of Third-Party Services

Procurement and monitoring of third-party services are managed in accordance with DoIT SOP #0606. DoIT defines these services as: a person or entity other than a state agency or its employees who provides a service for the benefit of DoIT and/or its customers. 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 manger. A Third-Party Services Performance Report is completed as part of this process.

Description of Controls – Logical Security

Mainframe user access as well as access to data sets is controlled through Top Secret administration. The ISOC uses the Remedy Ticketing system for all Top Secret changes. The system security and use SOP #8808 provides clear guidance regarding the responsibilities of Top Secret security administrators and the issuance of access permissions. The SOP requires that users be granted access to only those resources necessary and appropriate to 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 Top Secret security administration. Agency security administrators are responsible for granting and revoking agency user's 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 (ACID), 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 logon 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.

Top Secret security software is used to control access to all mainframe software and datasets. Permissions are defined by user and controlled through login and password. Top Secret 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/lock-out after minimum failed login attempts. Passwords are not displayed as they are input and are encrypted as they are stored.

Top Secret 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 start-up as a means to verify his or her identity). Security violations are logged, reviewed and action is taken to investigate violations. Security profile changes are also logged and periodically reviewed and any unusual items are investigated.

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 DoIT/DPA VPN (Virtual Private Network) Concentrator and the DoIT/DPA Access Control Servers (ACS) as well as the Internet firewalls. The security variance process is used to make any change 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 24-7 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. The ISOC utilizes the Chief Information Security Officer's Incident Response Plan/Policy as a guideline for all incident response activities.

Network/Desktop

Distributed computing logical control is similarly approached for the network, or "desktop," security and is administered by DPA's ITU staff. Agency administrators are responsible for managing their desktop environments. Each person in DPA is given a user ID and temporary password. Additional access requires justification obtained via an email from a user's supervisor. Personnel owning files can grant sharing and access permissions to other users as they deem necessary; however, directory sharing is not activated on a new user's account. The temporary password must be changed upon account activation (log in).

Desktop security controls are configured to enforce certain password criteria, including minimum length and account suspension after a defined number of failed login attempts. In addition, a log is generated containing certain events, including logon/logoff failures, file and object access failures, security policy changes and restart/shutdown and system success/failures.

Description of Controls – Configuration Management

DoIT 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 DoIT 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 anti-spam protection across DoIT 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.

Description of Controls – 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 DoIT 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 request 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.

Description of Controls – Data Management

Several Standard Operating Procedures (SOP) 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 onsite until they are deleted from the catalog.

Dataset backup, archiving and space management is handled with the IBM software packages for DFSMSHSM (DF (Data Facility), SMS (Storage Management Subsystem) and HSM (Hierarchical Storage Management). The datasets backed up and archived are not recoverable at the Disaster Recovery site. Customers are responsible for their own application data backups, and for their own offsite disaster recovery.

Offsite tapes are transported and stored by DocuVault. The transport trucks and the facility where the tapes are physically stored are unmarked. The tapes are secured in locked metal boxes. The offsite facility and transport trucks are unmarked and physically secure; access is restricted to authorized personnel.

Description of Controls – Operations Management

Computer Associates scheduling software (CA7) is utilized to schedule the processing of batch jobs. Top Secret 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 on the Activity History Report. 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's Management Facility (SMF).

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

Physical Security

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 DoIT staff who frequently enter the room on a daily basis in execution of their normal duties. Access to the telecommunications room uses a Cipher lock system. Visitors can enter the computing facility only through the print/distribution room. Visitors must complete a sign-in/out roster and have prior permission granted from upper management

within their agency and/or DoIT management. Any visitor that does not have prior permission may be granted entrance from the shift supervisor, after clearance is confirmed. 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 to which they are authorized.

Description of Controls – Application Controls: HR/Payroll Systems

ADS (Applicant Data System)

Controls - ADS is an in-house developed system utilizing an ADABAS Database Management System (DBMS) and Natural coding language. TMU staff works in conjunction with the Division of Human Resources (DHR) for technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through a DHR representative to ensure system integrity. DHR personnel are responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form.

Customers - The ADS system is the applicant tracking system for all Colorado state classified jobs and is composed of three separate systems: the mainframe based applicant data system, the job announcement system and the online job application system. The primary customers of the ADS system are the individual department and agency personnel analysts and all applicants for State classified jobs.

Service Levels - TMU currently provides systems analysis and programming expertise for the ADS system. This includes after-hours monitoring for database and batch system processing.

Stakeholders - The stakeholders for the ADS system are the personnel directors and personnel analysts at each of the initial departments and the DHR, Department of Personnel & Administration.

Security - The ADS system is a mainframe system utilizing CA-Top Secret, Natural Security and ADS application level security.

CPPS (Colorado Personnel Payroll System)

Controls – CPPS is a packaged system purchased from Integral Systems, Inc. TMU staff works in conjunction with the Central Payroll Office to provide technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through the State payroll manager to ensure system integrity. The State payroll manager is responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form. In addition to normal online updating of data, the CPPS system also facilitates data flows to and from third-party vendors. These data transfers are handled through either a regularly scheduled job on the DoIT mainframe or through a manual push to an encrypted web portal. For each occurrence, the data is protected with either a secure File Transfer Protocol (FTP) or an encrypted transmission process.

Customers - The CPPS system is used to process payroll for all Colorado state employees with the exception of those employees employed at the State four-year colleges.

Service Levels - TMU currently provides systems analysis and programming expertise for the CPPS system. This includes after-hours monitoring for database and batch system processing.

Stakeholders - The stakeholders for the CPPS system are the controllers and payroll officers at each of the individual departments and State payroll manager, Division of Finance and Procurement, Department of Personnel & Administration.

Security - The CPPS system is a mainframe system utilizing CA-Top Secret and CPPS application level security.

HRDW (Human Resources Data Warehouse)

Controls - HRDW is an in-house developed system utilizing a Web FOCUS and a MySQL database. TMU staff works in conjunction with the Office of the State Controller (OSC) and the DHR to provide technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through either an OSC or a DHR representative to ensure system integrity. DHR and OSC personnel are responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form.

Customers - HRDW is the current system of record for all employees of the State of Colorado, including higher education employees. It is used by all personnel analysts to access current and historical information on state employees, positions and class information.

Service Levels - TMU currently provides systems analysis and programming expertise for the HRDW system. This includes after-hours monitoring for database and batch system processing.

Stakeholders - The stakeholders for the HRDW system are the Department of Personnel & Administration and personnel directors and personnel analysts at each of the individual departments and DHR.

Security - The HRDW system is a web-based system utilizing application security on the reporting system, MySQL security on the database and firewall security on the network.

Description of Controls – Application Controls: Financial and Timekeeping Systems

Modifications to COFRS software fall in two categories: problem fixes and functional changes. Procedures have been developed and documented to guide the process of performing these modifications. Problem reports relating to data integrity or system assurance receive the highest priority. Normally, problem fixes are given higher priority than change requests.

Problem reports are created by TMU staff or from users via the COFRS help line. Change requests may be submitted by staff at user agencies or can be generated internally within TMU. Some changes are mandated by legislative action, while others are required by upgrades in Data Center system software. TMU staff verifies the existence of a problem or need for the change request, writes functional specifications for the proposed modification and may conduct internal and external meetings to elicit comments on the proposed changes. TMU staff maintains contact with

COFRS users through personal contact, the Controller's Forum, the Colorado Financial Management Association and liaison with the Office of the State Controller's staff.

The TMU manager approves all change requests and, if a problem report has several possible fixes or major system implications, these are also reviewed and approved by the TMU manager prior to being turned over for development.

Beyond a functional specification, TMU usually requires some technical design document restating the nature of the modification to be made, the programs affected and how the change will be tested. TMU performs unit testing of each program modification and the results of this testing are reviewed. Depending on the size and complexity, problem reports and change request are supplemented by further testing by TMU staff. Testing includes any data conversions or data recovery required to implement the new or changed software. The design document, code and testing are signed off by a supervisor or his or her designee prior to final review.

Customer communication regarding application changes takes the form of release letters, documentation and training. Changes affecting users are communicated to COFRS users via release letters emailed to clients. If a user submitted the problem report, he or she is contacted directly by TMU staff. For more significant changes, documentation and training are offered prior to the implementation date.

Final review of functionality, unit tests and acceptance tests are performed by a TMU manager prior to turning the modified software over to the COFRS system administration group for actual implementation.

Documentation for each problem fix or change request is collected in one or more project folders. The documentation includes the functional design, results of the review, design documentation, documentation of the unit and acceptance tests and changes in user documentation. This documentation is stored on-site for three years and is subsequently archived. Access to the documentation is made through an on-line problem/change tracking system. Additionally, the Systems Administration Group (SYAD) maintains special internal documentation for the scheduling software schedules and parameter tables used to administer COFRS.

Modifications to the KRONOS system can be classified into three major areas: vendor version upgrades, vendor service packs and configuration changes. Application development is completed using KRONOS Connect.

Vendor version upgrades involve KRONOS consultants, DoIT Database Administration (DBA) staff, Server Team members, KRONOS System Administrators and TMU KRONOS staff. Detail project plans are developed and updated. Project status meetings are held with DoIT staff and KRONOS System Administrators. The new version is loaded into a test region and tested by TMU KRONOS staff and KRONOS System Administrators. Implementation is scheduled with all groups and the system is not released to the users until it has been tested.

Vendor service pack release notes are reviewed by TMU KRONOS staff prior to loading the service pack into a test environment. TMU KRONOS staff completes their testing before the KRONOS System Administrators are asked to test. Verbal approval to move service pack into production is usually given at a KRONOS System Administrators meeting.

Configuration changes are initiated from the KRONOS System Administrators. Depending on the change, new configurations or changes to existing configurations are usually tested in a test region prior to moving into production. In some cases, they are made directly in production.

KRONOS Connect is used to program imports and extracts of data. Import and extract change requests are generated by TMU KRONOS staff or the KRONOS System Administrators.

Programming is completed on TMU staff desktop PCs and tested using production data. In most cases, KRONOS System Administrators review the results prior to the move to production.

COFRS (Colorado Financial Reporting System)

Controls - COFRS software is highly customized to meet customer requirements and is no longer on a vendor software upgrade path. TMU staff analyzes modification requests received from customers. TMU management determines the appropriateness of requests and prioritizes them. A paper-based software configuration management process is used with a signoff sheet. A software release letter is sent to customers via email and documentation is available in the financial data warehouse.

Customers - COFRS has approximately 3,500 customers using the application. These include controllers, accountants, accounting techs, purchasing agents, inventory staff, budget analysts, program accountants and grant accountants. The COFRS application attempts to satisfy both the individual business requirements of State departments with very different business needs and the centralized control functions of both the State Controller and the State Auditor.

COFRS provides a mainframe, character-based user interface. Most users today have come to rely on the graphical interfaces provided by personal computers and web browsers. Customers would like easier access to the COFRS data and the ability to download into spreadsheets and word processing documents. The financial data warehouse (FDW) has met many of these requirements for accounting transaction data, but the need is there for future enhancements.

Service Levels - TMU currently provides systems analysis and programming expertise. This includes monitoring and operations support 24 hours a day, seven days a week, problem and data integrity analysis and remediation, modification request analysis and programming, user training and help-line support. The COFRS system is available for use from 7:00 A.M. – 6:30 P.M. Monday through Thursday, 7:00 A.M. – 7:30 P.M. Friday and 9:00 A.M. – 5:00 P.M. on Saturday and Sunday, except when special processing (such as monthly close) is scheduled.

Stakeholders - The major stakeholders are the Office of the State Controller, Office of the State Auditor, state budget officers, department controllers and accountants and inventory staff.

Security - COFRS is a mainframe application and access to its files is maintained by the mainframe CA-Top Secret software. Within the COFRS application, each department controller or his or her designee is the COFRS security administrator for that department. TMU staff provide COFRS security administrator training to the department security administrators. In the absence of trained department controllers, the Office of the State Controller acts as the departments' COFRS security administrator. COFRS security administrators grant appropriate access to department employees to tables and transactions within the COFRS application.

FDW (Financial Data Warehouse)

Controls - FDW has daily and weekly load procedures that are launched by the database. Temporary table records are counted and summed, then compared to log files to verify the import was performed correctly. Extract dates are loaded into history files to prevent files from being loaded twice. After the permanent tables and ledgers are loaded, the system assurance reports are run, then the nightly maintenance jobs are processed. In the first half of 2004, TMU, in conjunction with the Department of Corrections, implemented a disaster recovery site for FDW in Colorado Springs.

Customers - FDW is used by approximately 800 accountants, budget staff and program managers. This system is used daily by many employees but the heaviest usage is at month-end and fiscal year-end. The Office of the State Controller has one staff member who develops specialized reports to meet selected user needs.

Service Levels - This system is available 20 or more hours a day, seven days a week. The only time it is scheduled to be down is during the daily and weekly loads that happen at about 4:00 AM. The ability to move to the disaster recovery site is very important and was used during fiscal year 2004 year-end closing.

Stakeholders - The major stakeholders are the Office of the State Controller, state budget officers, department controllers and accountants and program staff.

Security - User ID and password security was developed within this system. Security is configurable at the statewide, department and agency levels. Department controllers must approve all user access.

KRONOS

Controls - KRONOS is a vendor-maintained product. TMU has kept the KRONOS system on the vendor's upgrade path and the vendor plays a major role in these version upgrades. TMU staff is responsible for testing and implementing service packs issued by the vendor. The KRONOS system is linked into three statewide systems using imports and extracts. On a nightly basis, daily additions (new employees) and changes to our Employee Database (EMPL), which has been replaced by CPPS, are imported into KRONOS. On a bi-weekly and monthly basis, employee hours and related accounting distributions are extracted from KRONOS and imported into the State's payroll system (CPPS). These hours and accounting distributions are also sent to the State's financial system (COFRS) for redistribution.

Customers - The Department of Public Health and Environment, the Department of Natural Resources, the Department of Labor and Employment, the Department of Personnel & Administration and Secretary of State are the main users. Each department uses the KRONOS system a little differently to meet their unique departmental needs. These differences create operational and configuration challenges for TMU staff.

Service Levels - This system is available 20 or more hours a day, seven days a week. Due to an increasing number of users continuing to come on board and the fact that there is particularly heavy usage during the first week of each month, response times and other capacity issues were addressed during the upgrade in December 2006.

Stakeholders - The major stakeholders are the Office of the State Controller, Department of Personnel & Administration, Department of Natural Resources, Colorado Department of Public Health and Environment, and Department of Labor & Employment and SoS.

Security - The system is web-based and users access KRONOS using a browser. All servers are protected by firewalls in accordance with KRONOS recommendation. The user interface is a Secure Socket Layer (SSL) website with user ID and password access functionality. Department controllers must approve all user access.

Description of Controls – Report Management System

Document Direct

Controls – The basic components of the Document Direct for the Internet system are a report database, a recipient database and an request database. The report and recipient databases are populated as new reports are created and as new recipients, or users, require access to identified reports. These two databases are then connected by the request database, which allows a recipient access to the portion of a report or reports that they have a business reason to view.

Customers – Document Direct is used by the COFRS, CPPS and internal billing support applications.

Service Levels – The Document Direct SLA is stored on a specific server's public drive in a folder accessible to those with appropriately defined access.

Stakeholders - The major stakeholders are the DoIT technology management unit and DoIT support staff.

Security – The State of Colorado Infopac/Document Direct Security Access Authorization Form is used to request viewing access for a recipient to a specific portion of a report. The Department Security Administrator must sign this form before the request will be entered into the system. These request forms are filed and retained in case questions arise concerning the viewing authorization.

Description of Controls – Server Housing and Hosting

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 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 SAN. If the server requirements identify that it needs to be a physical system, the server is acquired via approval procurement processes. Upon receiving and/or identifying the required hardware, it is 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

it meets the identified needs of the customer and server 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 it meets the project/task requirements, server access is given to the customer to install their application.

The customer works with the Server Management team to install and configure their 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 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 Team to notify them 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 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.

Summary

The description presented above is designed to provide the reader a brief description of the activities performed by DoIT. DoIT's management believes the activities are appropriate for the services provided.

DoIT's specific control objectives and related control activities are included in Section V of this report, "Information Provided by Service Auditor," and captioned as "Provided by DoIT." Although the specific control objectives and control activities are included in Section V, they are nonetheless an integral part of DoIT's description of controls.

User Control Considerations

Colorado Financial Reporting System (COFRS) and Colorado Payroll and Personnel System (CPPS)

The processing of transactions for clients performed by the Data Center and the Technology Management Unit's (TMU) COFRS/CPPS applications and the control structure policies and procedures at the Data Center and within TMU's COFRS/CPPS applications cover only a portion of the overall internal control structure of the Data Center and TMU's COFRS/CPPS applications. It is not feasible for the control objectives relating to the processing of transactions to be solely achieved by the Data Center and TMU's COFRS/CPPS applications. Therefore, each user organization's internal controls must be evaluated in conjunction with the control policies and procedures of the Data Center and TMU's COFRS/CPPS applications and the testing summarized in Section V – Information Provided by the Service Auditor.

The following identifies those control activities that the Data Center and TMU believe should be in place at user organizations and were considered in developing policies and procedures described by the Data Center and TMU in this report. In order for user organizations to rely on the control policies and procedures presented within this report, each user must evaluate its own internal controls to determine if the following controls are in place and operating effectively. Furthermore, the following controls are identified only to address those policies and procedures related to the processing of transactions at the Data Center and by TMU's COFRS/CPPS applications. Accordingly, the identified controls do not represent a complete listing of control policies and procedures that provide a basis for the assertions underlying the financial statements and personnel reports of user organizations.

The purpose of this section is to identify the general and application controls that must be tested as part of the auditor's review of internal controls at agencies that use Data Center services and TMU's COFRS/CPPS applications. This section also provides examples of specific control considerations that auditors of user agencies should include in their reviews of agency internal controls.

Application Controls

- When reviewing an agency's control environment, the auditor should review the agency's controls over the use of its applications systems. Application controls are the responsibility of each user agency and are not the Data Center and TMU's responsibility. In general, these controls must ensure that:
    - Access to computer terminals, direct-dial phones, modems and official paper input documents are secured against unauthorized use.
    - Data extracted from TMU-managed systems and stored in agency-managed systems are protected from unauthorized access.
    - Requested changes to the COFRS and CPPS systems have been authorized by the appropriate agency personnel.
    - Input data and transactions are authorized, complete, accurate and valid.

- Output reports received by the agency are secured, distributed and used according to management intent.
- Output reports are reviewed for accuracy and corrected promptly if errors are detected.
- Agencies actively participate with TMU in disaster recovery planning and testing.

Specific Control Considerations for User Auditors

We have compiled a list of specific activities that user auditors should complete as part of their agency internal control reviews. This list is not intended to be a comprehensive list of all steps needed to review internal controls. Individual agencies may require additional steps to complete the internal controls review. The activities we identified can be grouped according to the following control considerations:

- Security and access
- Input controls
- Output controls
- Disaster recovery planning

In addition to these categories of control considerations, user auditors should review the extent of the internal Information Technology (IT) auditing performed at the agency and the organization and management of the agency IT department.

Security and Access

Auditors should review the agency's use of Top Secret and any other security software available to the agency. The following steps should be included in an evaluation of an agency's security and access controls:

General Controls

- Determine whether the agency has an agency security administrator and backup agency security administrator or whether the agency relies on the Data Center for security administration duties.
- Determine whether the agency has a database coordinator.
- Review the responsibilities of the agency security administrator and the database coordinator to ensure that these individuals do not perform functions that are incompatible with their security administration duties.
- Review Top Secret security settings established by the agency to control access, especially access to their own applications systems and datasets. These settings include, but are not limited to the following:
    - The Mode, which prevents access by unauthorized users or merely warns and then allows access.

- The number of log-on attempts or unauthorized access attempts allowed before a user is locked out.
- The automatic disconnect time limits for unused terminals.

Logical Access Controls

Review controls relating to the granting of access to resources. If any agency assigns its own access identifications, the auditor should review the agency security administrator controls relating to access identification assignments. The auditor should also confirm that all agency personnel assigned access identifications have signed a statement of compliance and that such statements are maintained in a file.

Physical Access Controls

1. Review the physical access controls over hardware, software, data, official input forms and official forms used to request and approve access identifications. Confirm that procedures exist to ensure that personnel do not leave logged-on terminals unattended, even if the agency uses automatic shut-off time limits.
2. Ensure that access to agency systems and to the Data Center mainframe computer system via terminals, modems and direct-dial phone lines is limited.

Monitoring Activities

Confirm that a Top Secret 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.

Input Controls

The Data Center and TMU have 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, control data and to submit both to the Data Center. In other words, 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 perform the following steps:

1. Confirm input documents are authorized and reviewed by an appropriate level of management.
2. Ensure control totals are used to verify that all transactions are entered.
3. 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:

1. Confirm that exception reports are reviewed promptly and any necessary corrections are made in a timely manner.

2. Look for evidence of management's review of output reports for accuracy, completeness, reasonableness and mathematical accuracy.

3. Review agency procedures for ensuring that output is distributed only to appropriate personnel.

Disaster Recovery Planning

The Data Center has developed a disaster recovery plan to resume Data Center operations at a remote "hot site," including the migration to a "cold site" and a new "home site" in the event of a disaster affecting the Data Center. Auditors should review the DoIT customer agency's policies and procedures to coordinate those agency's disaster recovery plans with those established by the DoIT Data Center. Auditors should also review the agency's disaster recovery plans for their own application systems. Specifically, the auditors should verify that the agency:

1. Designates resources to be backed up and stored off-site, the frequency of such backups and the methods used to perform the backups.

2. Establishes recovery and restart procedures, including coordination with the Data Center's recovery and restart efforts. The recovery and restart procedures should consider a system designed to establish a priority for critical systems applications.

3. Establishes a formalized disaster recovery plan that is also coordinated with the Data Center's plan and is periodically reviewed and updated. Such plan should develop a formal disaster recovery plan document that is stored offsite, contains all necessary information for locating key personnel, procedures, application programs and datasets.

4. Participates in the Data Center hotsite tests and related forums.

Establish adequate contractual arrangements with vendors to replace equipment damaged by a disaster recovery event, subject to State self-insurance policies and procedures.

This Page Intentionally Left Blank

Section V
Information Provided by the Service Auditor

Findings and Recommendations

Introduction

Our responsibility was to express an opinion about whether:

- The description of controls presented by the Division of Information Technologies Data Center and Technology Management Unit present fairly, in all material respects, the relevant aspects of the Division of Information Technologies (DoIT) Data Center and the Technology Management Unit's controls that had been placed in operation as of June 30, 2007.
- The controls, as described by the Division of Information Technologies Data Center and Technology Management Unit, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the client organizations applied the internal control contemplated in the Division of Information Technologies Data Center and Technology Management Unit's controls.
- The controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by DoIT management, were achieved during the period covered by our report.

The opinion described above is contained in Section I. In addition, however, we identified opportunities for improving the controls associated with the Division of Information Technologies Data Center and the Technology Management Unit. This section contains recommendations regarding the controls specified by Division of Information Technologies management.

It should be noted that in several instances, the recommendations are the result of an exception noted during the examination. However, a number of recommendations refer to control objectives and activities that did not exhibit an exception during the examination. This is because, although the Division of Information Technology successfully met the objective, a best practice recommendation is being made to offer improvements to current established controls.

Review of Top Secret Security Violation Logs

The weekly and monthly reviews of the Top Secret log's violations and security profile changes should be fully documented. During our testing, it was noted that there is no formal procedure in place to document weekly and monthly review of security violations and security profile change logs that are required to be conducted by the Mainframe Security Administrator. Management cannot determine with certainty that the reviews have been conducted. This may allow violations or inappropriate profile changes to not be detected in a timely manner. Suggestions for process improvement would be to create a cover sheet, which would include the report name, date of the report, printed name of reviewer, signature of reviewer, date the review was completed and any follow-up actions taken.

Recommendation 1

We recommend that the Division of Information Technologies Data Center and Technology Management Unit implement a standard procedure for documenting both the weekly and monthly reviews of the security violations logs and the security profile changes logs within Top Secret.

Department of Personnel and Administration's Response

Agree – implementation by November 30, 2007. DoIT will implement a procedure for documenting the reviews of security logs. A cover sheet will include documentation of the report name and date, the name and signature of the reviewer, the review date, exceptions found, and follow-up actions taken.

Review of Top Secret Access for Terminated Employees

There should be a formal process in place to identify and correctly address changes in access rights because of changes in employment status. While reviewing the list of terminated employees against the valid Top Secret Security (TSS) Access Identification (ACID)'s, we noted there was not a clear procedure for employees who have had a change in status, but were not terminated. During our testing, it was specifically noted that contractors that had a change in their status from contractor to employee were included on the terminations listing, although they had actually had a status change and their access account remained active. This results in confusion when reviewing the terminated employee listing and may result in allowing access to the system in error. We recommend creating an exception report that shows terminated employees and also identifies individuals that were not actually terminated but had a change in their employment status (for instance, a contractor that changed to a full time employee, etc).

Recommendation 2

We recommend that the Division of Information Technologies Data Center and Technology Management Unit implement an additional formal process to validate that terminated employee's Access Identification are either suspended or marked as not being recycled for a determined time period, or remain active due to a status change.

Department of Personnel and Administration's Response

Agree – implementation by December 31, 2007. DoIT will implement a process to identify employees who have a change in employment status but are not terminated to eliminate confusion when reviewing the access termination listing.

Establish and Monitor User Customer Service Levels

DoIT provides multiple levels of service to department and agency customers, including services related to COFRS, CPPS and technology housing and hosting services. For the housing and hosting services, there are many variations in service expectations among DoIT customers (related prior recommendations can be found in Section VI, September 2001 performance measure Recommendation #1 and June 2005 SAS 70 Recommendation #8). A number of improvements to service level documentation, tracking and reporting have been implemented. During our testing, we reviewed a new Service Level Agreement (SLA) form which had recently been created, but had not been implemented. Our review revealed that no signed SLAs were available for the period, using either the previous forms or the new forms. Furthermore, it is still noted that the documentation of SLAs for all DoIT customers can be improved to provide a more clear indication of service to be provided by DoIT, clarify residual user responsibilities, and assist in SLA performance assessments. During our testing, we discussed with DoIT their planned transition from SLAs to a Service Catalog (please note description in DoIT's response below). We beleive the spirit of these recommendations should be carried forward to the implementation of the Service Catalog.

Recommendation 3

We recommend that the Division of Information Technologies Data Center and Technology Management Unit ensure that current signed SLAs are on file and tracked for all DoIT server housing and hosting customers. SLAs should clearly define services to be provided by DoIT, responsibilities of the user, and performance measures that DoIT should meet.

Department of Personnel and Administration's Response

Agree – implementation by September 30, 2008. DoIT will describe its services in an actionable Service Catalog such that 80% or more of customer orders can be fulfilled based on the described service. This catalog will describe all services by September 30, 2008. This technique will encourage standardization of services and, therefore, processes necessary to deliver and support them.

The service catalog will describe both DoIT and customer expectations, when DoIT will deliver it and all other expectations to fulfill the order and support the service. SLAs may be used from time-to-time for services that have been significantly customized.

Manage Employee/Third Party Documentation

Documentation of new hire checklists and vendor performance reports are important to comply with personnel rules and standard operating procedures (SOPs). During our inspection of the new hire checklists, it was noted that two of the sampled checklists were misfiled, making it difficult to locate the checklists. Also, although the managers are designated to complete vendor performance reports, we found that one out of two samples were not completed. The designated administrative employee should ensure timely completion of vendor performance reports by escalating follow-up to upper management.

Recommendation 4

We recommend that the Division of Information Technologies Data Center and Technology Management Unit establish a review process to ensure that new hire checklists are properly filed and vendor performance reports are completed in a timely manner.

Department of Personnel and Administration's Response

Agree – implementation by December 31, 2007. DoIT will implement a process to ensure new hire checklists are properly filed by November 30, 2007. DoIT will ensure vendor performance reports are completed in a timely manner by implementing a vendor report tracking system no later than December 31, 2007.

Visitor Management

Visitors are required to check-in with DoIT building reception and complete a 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. Out of a sample of sixty-seven visitors, four (6 percent) instances were noted where the visitor had returned the badge but had not signed out.

Recommendation 5

We recommend that the Division of Information Technologies Data Center and Technology Management Unit implement a process to designate responsibility to the employee host to ensure all visitors successfully follow all visitor control procedures, including the return of badges and signing out of the visitor log after hours. Specifically, DoIT should include the addition of space on the log sheet for employees to sign acceptance of visitor arrival and document departure.

Department of Personnel and Administration's Response

Agree – implementation by December 31, 2007. DoIT will modify the current visitor control log to capture host employee acknowledgement of visitor sign in and sign out information. In addition, DoIT will inform all managers of this requirement at two (2) consecutive monthly manager meetings. This will be implemented by December 31, 2007.

Anti-virus on Servers

All servers should be running properly updated anti-virus software, including regular active virus scanning. We observed that the active virus scans were disabled because they may result in slower server performance during the scan. Some viruses, such as NIMDA, are able to attack servers after infecting the workstations, and active scanning is the only way to detect and prevent this type of attack. We also observed that the Linux servers were not utilizing any form of anti-virus software because it is commonly thought within the industry that a properly configured Linux system is more resistant to attack. DoIT should plan for the possibility of an improperly configured Linux system or the release of an effective Linux virus and consider the acquisition and installation of anti-virus software for Linux systems.

Recommendation 6

We recommend that the Division of Information Technologies Data Center and Technology Management Unit consider the purchase and installation of anti-virus software for the Linux servers, and that all servers be set to periodically scan for virus infections.

Department of Personnel and Administration's Response

Agree – implementation by March 1, 2008. DoIT will adjust the schedules of the server virus scans to enable regular scanning of all servers in a way that does not disrupt application availability or degrade server performance. Anti-virus software will be installed on Linux servers.

Management of New Systems

The DoIT hosted server team does not maintain the documentation of the hosted server build process. DoIT server team members use a Server Build Document to guide them through the process of deploying a new server and assisting the customer through the installation of his or her application on his or her server, but do not document the accomplishment of the server build steps. Failure to document the build process can result in the omission of key steps necessary to ensure the hosted server's implementation in accordance with DoIT standards or customer specifications.

Recommendation 7

We recommend that the Division of Information Technologies Data Center and Technology Management Unit implement a Server Build configuration check off sheet to be completed by the DoIT hosted server staff. The check off sheet should be maintained in DoIT customer files for each system added.

Department of Personnel and Administration's Response

Agree – implementation by March 1, 2008. DoIT already has a Server Build Procedure, which will be modified to reflect tasks completed, by whom, and variations from the normal process. This form will be saved for future reference and documentation purposes.

Reporting of Outages

DoIT controls state that significant IT events or failures should be reported to senior management. However, all such events or failures should be tracked and reported to DoIT management. During our testing of outage reporting, it was noted that significant IT events and failures are reported to management due to their critical nature. However, we found some of the groups failed to report an outage to the outage administrator because the group determined the outage was not severe enough to be formally reported. Such selective reporting can distort the effectiveness of current controls and mask significant trends.

Recommendation 8

We recommend that the Division of Information Technologies Data Center and Technology Management Unit re-emphasize the outage reporting process and ensure that all outages are reported regardless of their severity. Further, outages should be included as an agenda item to be discussed at management meetings to ensure that management is made aware of all events regardless of their severity.

Department of Personnel and Administration's Response

Agree – implementation by March 1, 2008. DoIT will re-emphasize the existing SOP, which specifies outage reporting procedures. A discussion of outages will be included on the agenda for the monthly Senior Management meetings.

Review of System Management Facility (SMF) Information

DoIT controls state that SMF information, which is used to monitor system performance and usage, and ensure infrastructure is appropriate to needs) should be reviewed, the review fully documented and performed regularly. Data Center personnel review SMF information on a regular basis to monitor system performance and usage and ensure infrastructure is appropriate to need. During our testing, it was noted that the technical support staff reviews the information, usually on a daily basis. However, there is no documentation of the review process supporting that a review was performed. Although reports are generated automatically and archived, there is no checklist or other form of documentation showing the review was completed. Suggestions for process improvement would be to create a cover sheet which would include the report name, date of the report, printed name of reviewer, signature of reviewer, and date the review was completed. In addition, it was also noted that there is no backup employee who could perform the review in absence of the technical support manager.

Recommendation 9

We recommend that the Division of Information Technologies Data Center and Technology Management Unit implement a procedure to document the review of System Management Facility (SMF) information. Also, DoIT should consider training another employee as a backup to ensure that review is performed on a timely basis in case the regular reviewer is not available.

Department of Personnel and Administration's Response

Agree – implementation by March 1, 2008. DoIT will adopt this recommendation by creating a SOP to specify the frequency and context of the reviews. The SOP will also assign these duties and identify a backup reviewer.

Periodic SAS 70 Meetings

The controls displayed in the SAS 70 report are an indication of broader management efforts to maintain the effectiveness of services provided and the confidentiality, integrity and security of systems entrusted to DoIT's care. Accordingly, regular management attention should be given to the review, evaluation and implementation of appropriate organizational, technical and process controls. The following recommendation is proposed to enhance management's oversight and implementation of appropriate and timely controls and of remediation activities related to ongoing service expectations and prior recommendations.

Recommendation 10

We recommend that the Division of Information Technologies Data Center and Technology Management Unit conduct a periodic meeting (at least on a quarterly basis) of the members of management to ensure that control documentation is updated on a regular basis to reflect the actual controls and procedures in place, to evaluate the effectiveness of current or proposed controls, and to review prior year audit suggestions/recommendations to ascertain they are being implemented on a consistent basis during the year.

Department of Personnel and Administration's Response

Agree – implementation December 1, 2007. DoIT will establish quarterly meetings to maintain currency of controls and related activities. DoIT will establish quarterly meetings to review and update controls and activities as processes and responsibilities change and to ensure that prior recommendations are being addressed/implemented.

Review Document Retention Policies

DoIT staff's documentation of activities performed to comply with the Division's control system should be retained for at least a year. Generally, state statutes require documents to be retained for three years. During our testing, it was noted that not all of the supporting documents necessary to document performance of control activities were retained for the entire fiscal year. To form a proper conclusion as to the operating effectiveness of a control activity, it is crucial to have adequate data from which to test throughout the period.

Recommendation 11

We recommend the Division of Information Technologies Data Center and Technology Management Unit review its document retention policies and require that documents demonstrating performance of control activities be retained for at least one year.

Department of Personnel and Administration's Response

Agree – implementation December 1, 2007. Each DoIT manager will review document retention practices against audit controls and either implement a minimum 15 - 18 month retention period or plan with the Office of the State Auditor (OSA) to save only the required sampling in anticipation of the next audit. Document retention will be discussed at quarterly audit meetings beginning December 2007.

Version Control Software

In the SAS 70 report dated April of 2002, it was recommended that version control software for COFRS be considered. DoIT reported that they considered the purchase and use of automated version control software for COFRS, but there was not sufficient operating or FTE budget to accomplish this. DoIT also felt that, for the relatively few code changes that occur on a system as mature as COFRS, the return on investment is questionable even if the budget were available. No further action is planned. Our current opinion would be that version control software should be reconsidered in the context of all supported systems, not just COFRS. Such software can assist in overall change management, code and version management, as well as contribute to management of segregation of duties and testing. When managing large and complex systems in the absence of version control software, DoIT may inadvertently fail to identify unauthorized changes to software, or may have difficulty tracking problems resulting from system changes. We recognize additional FTE resources will be required to implement and maintain this recommendation.

Recommendation 12

We recommend the Division of Information Technologies Data Center and Technology Management Unit consider the use of version control software, including addition resources as required, for application changes, including COFRS.

Department of Personnel and Administration's Response

Partially agree. Additional FTE are required. DoIT agrees that the concept is valid; currently there are not available funds in the operating or FTE budget to support this implementation.

Power and Signal Cable Duct Re-Engineering

In the SAS 70 report dated April of 2000, it was recommended that as equipment changes in the Data Center or major renovations are performed, the Data Center should re-engineer both power and signal cable ducts to provide separation and safety. DoIT reports that an analysis of their Power Distribution Units was performed in November of 2005 as part of a larger goal of implementing standards for power and signal cabling in the Data Center in general when a sufficient budget is available. DoIT further reports that plans to separate power and network cabling have been tabled until current plans for state data center consolidations are completed. The auditor performing the SAS 70 report dated April of 2000 recommended that as equipment changes in the Data Center or major renovations are performed, the Data Center should re-engineer both power and signal cable ducts to provide separation and safety.

Through inquiry and discussion with management, we have determined this continues to be a significant issue that should be incorporated into current planning.

Recommendation 13

We recommend the Division of Information Technologies Data Center and Technology Management Unit 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.

Department of Personnel and Administration's Response

Partially Agree. DoIT agrees that this is best practice; retro-fitting our existing data center is not financially sound as current plans for State data center consolidations will eventually meet this need.

Control Objectives, Control Activities, Tests of Operating Effectiveness and Results of Tests

Our examination was restricted to selected services provided to system users by DC/TMU, including users of the COFRS (Colorado Financial Reporting System) and CPPS (Colorado Personnel Payroll System) applications, and related EMPL / HRDW and Document Direct interfaces, and, accordingly, did not extend to controls in effect at user locations. It is each interested party's responsibility to evaluate this information in relation to controls in place at each user location in order to assess the total system of internal control. The user and DC/TMU portions of the system must be evaluated together. If effective user controls are not in place, DC/TMU controls may not compensate for such weakness.

Our examination included interviews with key personnel, inspection of available documentation and records and observation of certain security procedures and controls surrounding and provided by the DC/TMU systems. Our examinations were performed as of June 30, 2007, and were designed only to clarify your understanding of the information contained in the attached description. In addition, we applied tests to specific controls to obtain evidence about their effectiveness in meeting the related control objectives, described in this section of the report, during the period from July 1, 2006 to June 30, 2007.

The objective of data processing controls is to provide reasonable, but not absolute, assurance about such things as the following:

- Protection of data files, programs and equipment against loss or destruction
- Prevention of unauthorized use of data records, programs and equipment
- Proper handling of input and output data records
- Reliable processing of data records

The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits derived and, additionally, that evaluation of internal control necessarily requires estimates and judgments by management.

Figure 1: Strategic Planning			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
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 aligns 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.	Through inquiry and inspection of five year strategic plan, external customer survey and internal customer survey, ascertained existence of the strategic plan and stakeholder input.	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.	Through inquiry and inspection of Project Coordination Board (PCB) minutes, ascertained that the PCB does meet on a regular basis overseeing IT functions and activities.	No relevant exceptions noted.
	1.3 – DoIT ensures that IT plans are communicated to business process owners and other relevant parties across the organization.	Through inquiry and inspection of CIO Forum attendee list and meeting minutes, ascertained regular meetings are taking place to communicate IT plans to other agencies.	No relevant exceptions noted.
	1.4 – DoIT monitors its progress against the strategic plan and reacts accordingly to meet established objectives.	Through inquiry and inspection of the Strategic plan, staff, manager and senior manager meeting minutes, ascertained that review of the plan is occurring regularly.	No relevant exceptions noted.

Figure 2: Organization and Relationships			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the IT organization is responsible for managing all aspects of the system environment.	2.1 – Key systems and data have been inventoried and their owners identified.	Obtained and inspected the listing of software.	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.	Obtained and inspected related policy and procedures and ascertained that contracted staff and personnel are subject to DoIT policies and procedures.	No relevant exceptions noted.
	2.3 – IT strategies and ongoing operations are formally defined and communicated to senior management and customer CIOs.	Obtained and inspected a three year master plan that discusses IT strategies and future plans. Inspected CIO forum notes, meeting agendas and minutes to ascertain that IT strategies and ongoing operations are communicated to senior management and customer 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.	Obtained and inspected notifications sent to management reporting outages. In addition, inspected outage reporting forms and noted all items are assigned an "owner" or responsible party, prioritized and given a date of input and status of assigned or unassigned.	No relevant exceptions noted. See Recommendation #8.
	2.5 – Formal job descriptions exist and are kept current.	Obtained a listing of current employees at DoIT and verified that the job descriptions are current for selected employees.	No relevant exceptions noted.

Figure 2: Organization and Relationships			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	2.6 – An organization chart is published and kept current.	Obtained and inspected organization chart for DoIT and ascertained that it is current. The organization charts are updated on a monthly basis by the administrative assistant.	No relevant exceptions noted.

Figure 3: Human Resources Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
These controls provide reasonable assurance that hiring, training, performance evaluation, job responsibilities, vacation 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, vacation and termination practices.	Through inquiry and inspection of Colorado Department of Personnel & Administration (DPA) Employee Data System User Guide, ascertained state personnel rules are followed for personnel matters.	No relevant exceptions noted.
	3.2 – A checklist is used for all departing employees to ensure that separation and termination activities are conducted according to policy.	Through inquiry and inspection of a sample of terminated employees, ascertained that separation and termination activities are conducted according to policy through use of a checklist.	No relevant exceptions noted.
	3.3 – New employees attend departmental and divisional orientation sessions.	Through inquiry and inspection of new hire checklist and employee orientation sign-in sheets, ascertained that new hires are attending orientation sessions.	No relevant exceptions noted. See Recommendation #4.
	3.4 – New employees sign a statement of compliance indicating they have received and agree to the computer usage and data security policy.	Through inquiry and inspection of a sample of new employees and signed Statement of Compliance documents, ascertained that procedures are being followed.	No relevant exceptions noted.
	3.5 – A performance appraisal system is in place. Semiannual reviews are required and annual ratings are performed in April.	Through inquiry and inspection of Performance Evaluation List and Performance Management Forms, ascertained that reviews are being performed.	No relevant exceptions noted.

Figure 3: Human Resources Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	3.6 – Employees are trained in accordance with job responsibilities.	Through inquiry and inspection of Position Description Questionnaire (PDQ), Operators SOP and Training list, ascertained that training is based on job responsibilities.	No relevant exceptions noted.

Figure 4: Communication			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the established reliable system requires participation from all members of the IT organization and that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained.	4.1 – IT management has formulated, developed, and documented policies and procedures governing the IT organization's activities.	Through inquiry and inspection of the Standard Operating Procedures (SOP) manual, it was ascertained that policies exist.	No relevant exceptions noted.
	4.2 – IT management periodically reviews its policies, procedures and standards to reflect changing business conditions.	Through inquiry and inspection of SOP due dates document and emails, ascertained that SOPs are reviewed annually.	No relevant exceptions noted.
	4.3 – IT management has communicated policies and procedures governing the IT organization's activities.	Through inquiry and inspection of staff meeting minutes, ascertained that policies are communicated.	No relevant exceptions noted.
	4.4 – Data Center staff meetings are held monthly or as deemed appropriate by management. These meetings have an open forum and relevant changes to the organization are presented.	Through inquiry and inspection of staff, manager and senior manager meeting minutes, ascertained that meetings are held regularly.	No relevant exceptions noted.
	4.5 – IT management communicates its activities, challenges and risks on a regular basis with the Executive Director.	Through inquiry and inspection of Executive Director meeting agendas, ascertained meetings are held regularly.	No relevant exceptions noted.
	4.6 –SOP manuals exist and are used by Data Center and Statewide Application Systems personnel.	Through inquiry and inspection of the SOP manual, it was ascertained that policies exist.	No relevant exceptions noted.

Figure 5: Risk Assessment			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
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.	5.1- Project risk assessment is addressed as new projects are proposed to the Project Review Board.	Through inquiry and inspection of Project SOP and Project Proposal Forms, ascertained that risk is an element reviewed by the Project Review Board.	No relevant exceptions noted.
	5.2 – Risk assessment is documented in the Project Proposal Form.	Through inquiry and inspection of the Project Proposal Form, ascertained that risk is documented on this form.	No relevant exceptions noted.
	5.3 – Management obtains feedback from DoIT business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process.	Through inquiry and inspection of CIO Forum meeting minutes, ascertained regular meetings are taking place to communicate IT plans to and receive feedback from other agencies.	No relevant exceptions noted.
	5.4 – Newly hired employees are required to pass a background check prior to employment.	Through inquiry and inspection of signed Disclosure Release forms, ascertained background checks are being conducted and any issues identified must be cleared prior to the hiring process continuing.	No relevant exceptions noted.

Figure 6: Facility Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that physical security and environmental controls help the service organization maintain the security and availability of their systems.	6.1 – All visitors must enter the DoIT building 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 padlock combination and are for use by employees.	Obtained and inspected SOP#2900 *Building Security*. By observation and inspection, ascertained that access to the facility is restricted as described.	No relevant exceptions noted.
	6.2 – Employees and visitors must wear badges at all times while in the building.	Obtained and inspected SOP#2900 *Building Security*. Observed employees wearing badges and that failure to display badge resulted in a challenge. Ascertained that continued access required that a badge must be worn to allow continued access to the facility.	No relevant exceptions noted.
	6.3 – 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.	Obtained and inspected SOP#2900 *Building Security*. By observation and inspection, ascertained access through the front entrance required that visitors sign in and out and return visitor badges.	Exception noted. Obtained and inspected a sample of rosters for three dates. Ascertained that of sixty seven visitors who had signed in four visitors had no time out recorded. See Recommendation #5.
	6.4 – Visitors must be escorted at all times unless granted specific permission in person.	Obtained and inspected SOP#2900 *Building Security*. By observation and inspection, ascertained visitors were escorted by DoIT employees.	No relevant exceptions noted.

Figure 6: Facility Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	6.5 – The Data Center computing facility is comprised of three areas (print/copy/service center rooms, telecommunications room and the computer room). A Trilogy Lock System secures each area.	By observation and inspection, ascertained that Data Center access is controlled by the Trilogy Lock System. Obtained and inspected access rights granted by the Trilogy Lock System. By observation and inspection, ascertained that terminated employees had been removed from the Trilogy Lock System. By observation and inspection, ascertained that selected samples of users did not have access not approved within the Trilogy Lock System. Obtained and inspected SOP#8700 *Computer Room Discipline*.	No relevant exceptions noted.
	6.6 – The Data Center has 24 x 7 operations and someone is on site at all times.	By observation and inspection, ascertained that Data Center network operations staff is present in the Data center 24-7-365.	No relevant exceptions noted.
	6.7 – Data Center staff monitor the building cameras for unfamiliar or unusual activity after normal business hours.	By observation and inspection, ascertained that all exterior access points are monitored by CCTV cameras. Ascertained that video is available to the Network Operations Staff for monitoring purposes. By inquiry ascertained that Data Center staff and Colorado Highway Patrol monitor cameras after normal business hours.	No relevant exceptions noted.

Figure 6: Facility Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	6.8 – Visitors enter the computing facility only through the print/copy room. Visitors must complete a sign-in/out roster and obtain permission from the shift supervisor, who confirms the visitor's reason for being in the computing facility.	By observation and inspection, ascertained that print/copy access is controlled by the Trilogy Lock System. Obtained and inspected access rights granted by the Trilogy Lock System. By observation and inspection, ascertained that terminated employees had been removed from the Trilogy Lock System. By observation and inspection, ascertained that selected samples of users did not have access not approved within the Trilogy Lock System. Obtained and inspected SOP#8700 *Computer Room Discipline.* By observation and inspection, ascertained that visitors are escorted, obtain permission from the shift supervisor to gain access, and must sign in and out on a log.	No relevant exceptions noted.
	6.9 – With the Trilogy Lock System employees are assigned individual codes based on need. Departing employees' codes are disabled upon termination. Additional changes are made at management's discretion.	By observation and inspection, ascertained that users are granted unique access codes to the Trilogy system. Tested a selected sample of current and terminated user access and ascertained that user access is controlled by unique assignable code.	No relevant exceptions noted.

Figure 6: Facility Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	6.10 – Employees receive new Trilogy combinations for only those areas to which they are authorized.	By observation and inspection, ascertained that users are granted unique access codes to the Trilogy system. Tested a selected sample of user access and ascertained that user access is controlled by unique assignable code for only those areas to which they are authorized.	No relevant exceptions noted.
	6.11 – There are standard procedures for accepting and transferring materials (data products or common deliveries) in and out of the Data Center.	Obtained and inspected SOP#2900, *"Building Security"*.	No relevant exceptions noted.
	6.12 – The computing facility is equipped with smoke detectors located above and below the raised flooring and are directly linked to the fire suppression system. Water detection sensors are located under the floor.	By observation and inspection, ascertained that the computing facility is equipped with smoke detectors both within the facility and below the raised flooring. By observation, ascertained that water detection devices are installed beneath the computer flooring.	No relevant exceptions noted.
	6.13 – The computing facility is equipped with an FM200 gas fire suppression system.	By observation and inspection, ascertained that the computing facility is equipped with an FM200 fire suppression system.	No relevant exceptions noted.
	6.14 – The gas fire suppression system is inspected annually by a third-party service and it has an automated monitoring system that is checked regularly by Data Center personnel.	Obtained and inspected service agreement with API systems group for testing and maintenance of the FM200 system.	Although a service agreement is in place, no documentation existed to verify inspection had been completed. Exception noted.

Figure 6: Facility Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	6.15 – Temperature and humidity are monitored by Operations staff in the Data Center.	By observation and inspection, ascertained that temperature and humidity sensors are monitored by Network Operations Center (NOC) staff.	No relevant exceptions noted.
	6.16 – The data center has an uninterruptible power supply (UPS) system with a generator alternate power source, which is connected and operates on the Data Center's power grid.	By observation and inspection, ascertained that the Data Center has an installed UPS system and a back up generator in a secured area next to the building.	No relevant exceptions noted.
	6.17 – Central monitoring of the building fire alarms is provided by State Patrol headquarters who will notify the fire department if an alarm is activated.	By inquiry, ascertained that the State Patrol dispatch is notified when an alarm is triggered.	No relevant exceptions noted.
	6.18 – The second floor is provided with power outlets (for personal computers) that are connected to the UPS/generator backup power supply.	By observation, ascertained that dedicated outlets, color coded orange, supply uninterruptible current to computer systems.	No relevant exceptions noted.

Figure 7: Quality Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that quality programs address both general and project-specific quality assurance activities and should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed.	7.1 – The service level manager researches all known major system outages, completes an outage notification and distributes it to senior management.	Obtained and inspected documentation for unscheduled outages and service interruptions. Obtained and inspected file summarizing outages by month and in total, and emails to senior management.	No relevant exceptions noted.
	7.2 – A monthly executive dashboard is completed and posted on the division intranet site.	Obtained and inspected a sample of monthly Executive Dashboard reports. Observed posting on division intranet site.	No relevant exceptions noted.
	7.3 – An annual Top Secret access review for Computing Services is completed.	Obtained and inspected annual Top Secret audit.	No relevant exceptions noted.
	7.4 – Project review sessions (Lessons Learned) are held at the end of projects to determine areas of success and areas for improvement.	Obtained and inspected *Lessons Learned Procedure* and *Lessons Learned Template.* Obtained and inspected seventeen *Lessons Learned* documentation. Obtained and inspected *DoIT Projects Completed in FY06-07*.	No relevant exceptions noted.
	7.5 – SOPs are reviewed against current operations annually.	Obtained and inspected SOP review dates schedule. Compared schedule against supplied SOPs.	No relevant exceptions noted.

Figure 8: Software Acquisition Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that system software is acquired in accordance with organizational requirements.	8.1 – Documented procedures have been developed and are followed in the requisition, bidding and purchase of new utilities software.	Obtained and inspected a copy of the procedures for software acquisition. By inquiry of Administrative / Financial and HR Manager and inspection of selected purchase request forms, ascertained that applicable signatures are obtained before acquisition.	No relevant exception noted.
	8.2 – Appropriate justification and management approval is required before the acquisition of new utilities software.	Through inquiry of the administrative finance and HR Manager and inspection of sampled purchase request forms, ascertained that proper documentation supporting the purchase is obtained before acquisition.	No relevant exception noted.
	8.3 – Software acquisitions include annual support or funds for renewal are encumbered annually prior to expiration.	Through inquiry of the Administrative / Financial and HR Manager and inspection of sampled purchase request forms, ascertained that management's approval and any supporting documentation is obtained before acquisition.	No relevant exception noted.

Figure 9: Technology Acquisition Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms.	9.1 – System management facility (SMF) recording options are appropriate to capture and monitor capacity and performance.	By inquiry of the technical support manager and inspection of report parameters, ascertained the SMF recording options are sufficient to capture and monitor mainframe platform performance.	No relevant exceptions noted.
	9.2 – Data Center personnel review SMF information on a regular basis to monitor system performance and usage and ensure infrastructure is appropriate to need.	By inquiry of the technical support manager and observation of the review process, ascertained that reports are automatically generated and archived for review.	Exception noted: Documentation to confirm that reviews were actually performed was not noted. See Recommendation #9.
	9.3 – SMF data capture is retained and presented in graphical format for management review.	By inspection of a sampled computing services dashboard, ascertained the document displays system resource use and parameters in a graphical format.	No relevant exceptions noted.
	9.4 – Hardware acquisitions include annual maintenance and support or funds for renewal are encumbered prior to expiration.	By inquiry of the administrative finance and HR Manager and inspection of the encumbrance documentation, ascertained that funds are encumbered prior to contract expiration.	No relevant exceptions noted.

Figure 10: Install and Test Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes, and associated controls operate as intended.	10.1 – A formal change management system is used to control and document changes to system software.	Obtained and inspected Division of Information Technologies Computer Operations Section Standard Operating Procedure #8803 *Change Management.* Obtained and inspected samples of DoIT's *Publication of Change Activities.* Obtained and inspected samples of *Change Request Details Document.*	No relevant exceptions noted.
	10.2 – Prior to modifying system software, the modifications are authorized by appropriate personnel.	Obtained and inspected samples of Change Request Details Document. Ascertained that the supplied electronic and email documentation supports the stated activity.	No relevant exceptions noted.
	10.3 – System software modifications and additions are thoroughly tested and approved before introduction into the production environment.	Obtained and inspected samples of Change Request Details Document. Obtained and inspected samples of Lessons Learned Small & Medium Projects documents. Ascertained that the supplied documentation supports the stated activity, including documentation of testing prior to introduction into the production environment.	No relevant exceptions noted.
	10.4 – An independent test LPAR residency (partitioned disk space separate from the operation's partition) and test plans are used by software programmers and clients to functionally evaluate system change modifications.	Obtained and inspected samples of Change Request Details Document. Ascertained that the documentation describes testing on test partitions.	No relevant exceptions noted.

Figure 10: Install and Test Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	10.5 – An implementation schedule is published to the customers.	Obtained and inspected samples of DoIT's emails and web site related to Publication of Change Activities.	No relevant exceptions noted.
	10.6 – Affected clients are notified via email, telephone or broadcast message prior to placing a modification into production.	Obtained and inspected samples of DoIT's Publication of Change Activities.	No relevant exceptions noted.
	10.7 – Prior to implementation, management assesses the impact of systems software modifications to client processing.	Obtained and inspected samples of DoIT's Publication of Change Activities. Obtained and inspected samples of Change Request Details Document.	No relevant exceptions noted.
	10.8 – Back-out procedures are written to return the system's configuration to its pre-implementation condition.	By inquiry and observation, ascertained that DoIT utilizes the IBM *System Modification Program* (SMP/E). Ascertained that SMP/E is the basic tool for installing and maintaining software in z/OS and OS/390 systems and subsystems. Observed that SMP is configured to allow restoration of the Z/OS system to its pre-implementation condition.	No relevant exceptions noted.
	10.9 – Documentation for system software products is available and current.	By inquiry and observation, ascertained that current software documentation is available in both electronic and hardcopy format and is available to authorized personnel.	No relevant exceptions noted.

Figure 10: Install and Test Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	10.10 – The installation process for system software includes a review/update of associated documentation.	Obtained and inspected samples of Change Request Details Document and ascertained the installation process for system software includes a review/update of associated documentation.	No relevant exceptions noted.
	10.11 – The inventory of systems is updated for system software modifications.	Obtained and inspected SMP queries of version control logs. Ascertained that the version control logs appear to be current. Obtained and inspected system & software inventory.	No relevant exceptions noted.

Figure 11: Service Level Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that service levels are defined and managed in a manner that provides a common understanding of performance levels with which the quality of services will be measured.	11.1 – SLAs are executed for Data Center operations.	Through inquiry and inspection of SLAs and SOPs, ascertained that they are being followed.	No relevant exceptions noted.
	11.2 – SLAs are executed for new services.	Through inquiry and inspection of service SLAs, ascertained that do exist.	No relevant exceptions noted.
	11.3 – Service levels are defined and managed to support system requirements.	Through inquiry and inspection of service SLAs, ascertained that service levels are defined.	No relevant exceptions noted.
	11.4 - A framework is defined to establish key performance indicators to manage service level agreements, both internally and externally.	Through inquiry and inspection of SLAs and SOPs, ascertained that performance levels are defined.	No relevant exceptions noted.

Figure 12: Management of Third-Party Services			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.	12.1- A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	Through inquiry and inspection of SOP, Purchase Orders, Price Agreement Third-Party Services Performance Report and work plan and migration documents, ascertained that one of two vendors for audit period had a third-party services performance report completed.	No relevant exceptions noted. See Recommendation #4.
	12.2- Selection of vendors for outsourced services is performed in accordance with the Organization's SOP#0606, *Procuring and Monitoring Third-Party Services*.	Through inquiry and inspection of SOP, Purchase Orders, Price agreement Third-Party Services Performance Report and work plan and migration documents, ascertained that SOP is used as basis for contracting third-party services.	No relevant exceptions noted.
	12.3- IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service.	Through inquiry and inspection of SOP, Purchase Orders, Price Agreement Third-Party Services Performance Report and work plan and migration documents, ascertained that third party contractor candidates are validated as qualified vendors.	No relevant exceptions noted.
	12.4 – Procedures exist and are followed to ensure that services are defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the Organization's policies and procedures.	Through inquiry and inspection of SOP, Purchase Orders, Price agreement Third-Party Services Performance Report and work plan and migration documents, ascertained that services are defined and agreed upon before work is initiated.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of their systems.	13.1 – Computer operators are prohibited from making changes to systems and data.	Obtained and inspected a complete list of Top Secret ACIDs along with a list of privileged accounts. Inspected TSSAUDIT to validate changes made in production were warranted. Verified computer operators cannot make changes to systems and data. Inspected the terminated employee access list and compared it to valid TSS accounts; four employees were listed as terminated, when actually they had a status change from contract to permanent.	No relevant exceptions noted. See Recommendation #2.
	13.2 – Application programmers are not permitted access to operating system files and data.	Obtained and inspected a complete list of Top Secret ACIDs and inspected a complete list of privileged accounts. Inspected the profiles of ACIDs who have special administrative privileges. Verified application programmers were not permitted access to production systems and data.	No relevant exceptions noted.
	13.3 – Access to security administration functions is appropriately limited to authorized individuals.	Obtained and inspected a complete list of Top Secret ACIDs, Divisional Control ACIDs and Central Security Control ACIDs, and inspected a complete list of privileged accounts. Inspected the profiles of ACIDs who have special administrative privileges.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.4 – Top Secret is used to restrict access to system software to appropriate individuals.	Through inquiry and observation, we validated Top Secret is configured to restrict access to production software. Inspected the terminated employee access list and compared it to valid TSS accounts; four employees were listed as terminated, when actually they had a status change from contract to permanent.	No relevant exceptions noted. See Recommendation #2.
	13.5 – Top Secret is used to restrict access to those system programs that allow bypassing of normal system or application controls (e.g., Super Zap).	Obtained and inspected output from the partitioned data set SYS1.PARMLIB and validated protected dataset. Inspected TSS WHOHAS PGM access report to validate the security and usage of special program utilities.	No relevant exceptions noted.
	13.6 – The System Security and Use Standard Operating Procedure #8808 provides clear guidance regarding the responsibilities of Top Secret security administrators and the issuance of access permissions.	Obtained and inspected SOP #8808 *System Security and Use*.	No relevant exceptions noted.
	13.7 – 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 SOP #8808, *System Security and Use*, and Compliance Statements for all employees for July 1, 2006 through June 30, 2007, which are kept in the Data Center in binders listed alphabetically by ACID.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.8 – Security administrators are required to sign an additional statement of compliance referencing and acknowledging responsibilities relative to Top Secret security administration.	Inspected SOP #8808 and additional Statement of Compliance for all Agency Security Administrators (ASA) for July 1, 2006 through June 30, 2007, which are kept in the Data Center in binders listed alphabetically by ACID.	No relevant exceptions noted.
	13.9 – Data Center Top Secret administration privileges are limited to authorized personnel.	Inspected SOP #8808 and additional Statement of Compliance for all ASAs for July 1, 2006 through June 30, 2007, which are kept in the Data Center in binders listed alphabetically by ACID, and verified Top Secret administration privileges are limited to authorized personnel .	No relevant exceptions noted.
	13.10 – Standard operating policies require that the users have access to only those resources necessary and appropriate to user's job duties.	Inspected SOP # 8808 for policy requirement.	No relevant exceptions noted.
	13.11 – Human Resources coordinate 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.	Obtained and inspected a sample of Security Request Forms for July 1, 2006 through June 30, 2007. Verified appropriate supervisor/manager sign-off and that user access is granted through the security team.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.12 – New personnel receive a unique ACID and temporary password. The password must be changed on their first logon attempt or their account will be suspended (locked out).	Through the TSSMODIFY report, observation and inquiry, we validated that new user accounts are setup with a temporary password that will expire immediately after their first logon attempt to the mainframe. Observed the process with Top Secret administrator; noted the user will not be granted access beyond the login screen until the password is changed. Obtained screenshot of TSS command used for setting up new users, new passwords and replacing passwords.	No relevant exceptions noted.
	13.13 – Top Secret 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.	Obtained and inspected a copy of the TSS9661I and TSS MODIFY reports and validated that TSS password controls require a minimum length, have a defined expiration and a maximum for failed logon attempts.	No relevant exceptions noted.
	13.14 – The Help Desk unlocks accounts only after verifying a user's identity using additional private information from INSTADATA.	Inquired and observed the security team administrators Top Secret and user access; observed locking access. Top Secret locks user access after three attempts. Employees must contact DoIT help desk and supply two personal "safe" words before the access can be reactivated. Obtained copy of screenshot showing data used for verification.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.15 – Future 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.	Inquired and observed the security team Top Secret administrators; ascertained users with DoIT access will be changed after receipt of appropriate email from the user's supervisor to the Help Desk explaining the reason for the permission change request.	No relevant exceptions noted.
	13.16 – The system automatically disconnects a TSO session if inactive for fifteen minutes.	Obtained and inspected the TSS MODIFY report for the lock time settings for TSO.	No relevant exceptions noted.
	13.17 – Top Secret is operating in fail mode, meaning that unauthorized attempts to access data sets are aborted.	Obtained and inspected a copy of the TSS9661I and the TSS MODIFY reports and validated that TSS is operating globally in fail mode.	No relevant exceptions noted.
	13.18 – Top Secret logs security violations; logs are reviewed weekly and action is taken to investigate violations.	Randomly selected a sample of security violation logs and inspected for suspicious activity. Observed there is no formal review process of documenting review of the violation logs. Discussion with the mainframe security administrator and staff revealed review is being conducted on a weekly basis. Inspection of the logs indicated occasional tick marks, initials and comments.	No relevant exceptions noted. See Recommendation #1.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.19 – Top Secret logs security profile changes; logs are reviewed monthly and unusual items are identified and investigated.	Randomly selected a sample of security profile change logs and inspected for suspicious activity. Observed there is no formal review process documenting review of the profile change logs. Discussion with the mainframe security administrator and staff revealed review is being conducted on a weekly basis. Inspection of the logs indicated occasional tick marks, initials and comments.	No relevant exceptions noted. See Recommendation #1.
	13.20 – The administrative staff utilizes a departing employee checklist to ensure that the departing employee's user mainframe account is deleted in timely manner.	Verified and obtained a copy of the Checklist for Departing Employees. Verified that mainframe accounts are listed on the checklist. Obtained a copy of the JCL that run the sweeper job to remove unused ACIDs and validated its job position in CA-7.	No relevant exceptions noted.
	13.21 – Changes to access control lists on perimeter security devices is authorized through a security variance process. The security variance form must be signed and the approval of changes must be done in conjunction with performing a risk assessment on the impact of the change.	Obtained and inspected Remedy tickets and security variance forms regarding changes to access control lists on perimeter security devices. Ascertained that security variance forms were signed and risk assessments were performed.	No relevant exceptions noted.

Figure 13: Logical Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.22 – Changes to Perimeter Security Devices are authorized by the Security Manager and are performed in a time window and documented for troubleshooting purposes.	Obtained and inspected Remedy tickets and security variance forms regarding changes to access control list on perimeter security devices. Ascertained that security variance forms are authorized by the Security Manager and that changes are properly documented.	No relevant exceptions noted.
	13.23 – Changes made to security devices such as firewalls, VPN Concentrator and ACS are done in accordance with the Security Variance Process.	Obtained and inspected Remedy tickets and security variance forms and ascertained that changes made to security devices are done in accordance with the Security Variance Process.	No relevant exceptions noted.
	13.24 – 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.	By corroborative inquiry, ascertained that alerts/ advisories are sent to parties affected by malicious traffic/ code. Reports on system security are obtained from a third-party vendor and analyzed for system threats.	No relevant exceptions noted.
	13.25 – Security incidents are handled in accordance with the ISOC Incident Response SOP.	Obtained and inspected a copy of the ISOC Incident Response SOP and ascertained by inquiry that security incidents are handled accordingly.	No relevant exceptions noted.

Figure 14: Configuration Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.	14.1 – System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, are properly configured to prevent unauthorized access.	Obtained and inspected *DoIT Server Build and Deployment Procedure Guide.* Obtained and inspected copy of the online server inventory of systems configured and added to the server pool. Obtained and inspected a selected sample of configuration changes for network devices.	No relevant exceptions noted.
	14.2 – IT management has implemented antivirus and anti-spam protection across the organization to protect information systems and technology from computer viruses.	Obtained and inspected log of all servers with Antivirus installed. Compared log to selected systems. By inspection and observation, ascertained that virus definitions are updated daily within 240 minutes of 8 a.m. Ascertained that the current definition files are on the system. Ascertained that clients check for updates on the server every 60 minutes. Ascertained that clients are not allowed to manually launch live update or affect settings. Ascertained that clients perform a full scan every Wednesday at 12 p.m.	No relevant exceptions noted. See Recommendation #6.
	14.3 – Access Control Server used to monitor changes to critical network equipment.	Obtained and inspected Access Control Server Logs for the first Monday of each month. Ascertained that the supplied documentation supports the stated activity.	No relevant exceptions noted.

Figure 15: Problem and Incident Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
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.	Through inquiry and inspection of Remedy system, ascertained it is being utilized.	No relevant exceptions noted.
	15.2 – Incidents or problems identified are immediately entered into a Remedy ticket.	Through inquiry regarding email and telephone calls received to initiate an incident or problem, and inspection of documented Remedy incidents, ascertained that identified problems are being entered into Remedy.	No relevant exceptions noted.
	15.3 – Customers and DoIT employees report incidents/problems.	Through inquiry and inspection of Remedy incidents, ascertained that both customers and DoIT employees report problems.	No relevant exceptions noted.
	15.4 – Customers are notified of outages.	Through inquiry and inspection of Outage SOP, notification list, checklist and notification documents, ascertained that notification is occurring.	No relevant exceptions noted.
	15.5 – Unplanned outages related to incidents are managed in accordance with SOPs to ensure proper response, investigation and resolution.	Through inquiry and inspection of SOP and outage documentation, ascertained that unplanned incidents are being managed.	No relevant exceptions noted.
	15.6 – Outage Notifications are documented.	Through inquiry and inspection of outage documentation, ascertained that unplanned incidents are documented.	No relevant exceptions noted.

Figure 15: Problem and Incident Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	15.7 – Outage Notification short- and long-term resolutions are reviewed by management.	Through inquiry and inspection of SOP and outage documentation, ascertained that unplanned incidents are being managed.	No relevant exceptions noted.
	15.8 – Service Outage Notification Reports are provided to management.	Through inquiry and inspection of SOP and outage documentation, ascertained that unplanned incidents are reported to management.	No relevant exceptions noted.

Figure 16: Data Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	16.1 – The following are backed up on a defined schedule: critical disk packs, system datasets and catalogs, source program libraries, databases for which the Data Center staff function as the Database Administrator (DBA).	Obtained and inspected SOP #6720 *Full Volume Disk Backup Policy* and SOP#6721 *Off-Site Dataset Storage Procedures.* Obtained and inspected stored SMS/HMS procedures for mainframe backups. Obtained and inspected selected samples of mainframe backup logs. Obtained and inspected selected logs for network backups. Ascertained that the supplied documentation appears to support the stated activity.	No relevant exceptions noted.
	16.2 – Initial storage of data on disk is managed by SMS/HSM.	Obtained and inspected stored SMS/HMS procedures for mainframe backups at DoIT. Ascertained that the supplier documentation appears to support the stated activity.	No relevant exceptions noted.
	16.3 – Backup, archive and retention operations are governed by SMS parameters and CA1.	Obtained and inspected SOP #6720 *Full Volume Disk Backup Policy* and SOP#6721 *Off-Site Dataset Storage Procedures.* Obtained and inspected stored procedures for mainframe backups. Ascertained that the supplied documentation appears to support the stated activity.	No relevant exceptions noted.

Figure 16: Data Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	16.4 – All Datasets are kept until they are either deleted from the catalog or expired.	Obtained and inspected *Enterprise Storage-Symantec-Overview.* Obtained and inspected selected copies of *Tape Operations Daily Schedule* checklists. By inspection, ascertained only current datasets are in catalog.	No relevant exceptions noted.
	16.5 – Backup media is stored off site.	Obtained and inspected *Enterprise Storage-Symantec-Overview.* Obtained and inspected selected copies of *Tape Operations Daily Schedule* check lists. Inspected a sample of send and receive checklists and receipts validating transport to and from off site facility.	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.	Obtained and inspected *Report of The State Auditor Mainframe Disaster Recovery Performance Audit January 2007.* Obtained and inspected a report from the State of Colorado Manager of Disaster Recovery. Ascertained that backup media restoration testing is performed at least annually.	No relevant exceptions noted.

Figure 17: Operations Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.	17.1 – Top Secret is used to restrict access to scheduling Software (CA-7) to appropriate personnel.	Inspected SOP #8808, System Security and Use, and observed job scheduling process. Obtained and inspected a sample of job schedules on the mainframe for both routine and single use. Validated jobs must be scheduled through the automated scheduling program, CA-7. Obtained and inspected a list of authorized users of CA-7.	No relevant exceptions noted.
	17.2 – Automated operation of scheduling software is used.	Inspected SOP #8808 and observed job scheduling process. Obtained and inspected a sample of job schedules on the mainframe for both routine and single use. Validated jobs must be scheduled through CA-7. Obtained and inspected a list of authorized users of CA-7.	No relevant exceptions noted.
	17.3 – Operator activities are recorded on the console log.	Obtained and inspected SYSLOGs and ascertained operator activities are recorded on the console log.	No relevant exceptions noted.
	17.4 – Reports printed at the Data Center are processed per Control Processing Procedures (CPPs). Reports are logged and sent to the user indicated on the CPP.	Obtained and inspected a sample of job log out sheets and ascertained that reports are logged prior to distribution.	No relevant exceptions noted.

Figure 17: Operations Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.5 – Batch jobs are run on a pre-determined schedule and tracked automatically.	Through inquiry of Computer Center Supervisor, ascertained that batch jobs are scheduled based on control processing procedures and are tracked automatically. Inspected SYSLOG and noted all jobs are tracked.	No relevant exceptions noted.
	17.6 – Routine jobs that are processed outside of their normal schedule are checked off by schedulers as they are completed.	Through inspection of sampled daily batch job schedules, ascertained that jobs are checked off by the schedulers as they are completed. Any exception is noted on the activity history report.	No relevant exceptions noted.
	17.7 – Scheduling deviations are reported by schedulers and published for management review on a daily activity history report.	Obtained and inspected a sample of the daily activity history report and ascertained that scheduling exceptions are included in this report, which is available for management's review.	No relevant exceptions noted.
	17.8 – The Data Center has documented Control Processing Procedures, which provide detailed guidance to address processing problems, including whom to contact for system and application specific troubleshooting information.	Obtained and inspected sample Control Processing Procedures and ascertained that proper guidance is included to address processing problems.	No relevant exceptions noted.

Figure 17: Operations Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.9 – Problems identified are immediately entered into Remedy, defining the problem and corrective procedures undertaken.	Inspected SOP #8802 for framework of problem management resolution. Ascertained through inquiry of the Computer Ops Supervisor that problems are entered into Remedy as soon as they are identified. Inspected a sample of Remedy tickets and ascertained that issues and action(s) taken were properly documented.	No relevant exceptions noted.
	17.10 – Exceptions to normal operations as they relate to processing and tracking of problems are reported by schedulers and are published for management review on the daily activity history report.	Obtained and inspected a sample of the daily activity history report and ascertained that processing exceptions are included in this report, which is available for management's review.	No relevant exceptions noted.
	17.11 – Forms are inspected upon receipt of shipment.	Through inquiry of the Materials Handler and Computer Operations Supervisor, ascertained that shipment is inspected and verified against the packing list and internal documents.	No relevant exceptions noted.
	17.12 – Warrants are stored in a secure space.	Through observation and inspection, ascertained that warrants are stored in a secured vault accessible only by authorized individuals.	No relevant exceptions noted.
	17.13 – Standard Operating Procedures require that access to warrant forms are limited to Computer Operations staff.	Per inspection of SOP# 6718 (Laser warrant processing) and inquiry of Computer Ops Supervisor, ascertained that procedures require access to warrant forms restricted to Computer Operations staff.	No relevant exceptions noted.

Figure 17: Operations Management			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.14 – Stock number series are verified prior to and after print processing.	Through inspection of sampled log sheets, ascertained that stock number series are verified prior to and after print processing.	No relevant exceptions noted.

Figure 18: Application Controls: HR/Payroll Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended.	18.1 – A formal change-management methodology is used to control and document changes to application software.	By inquiry of HR/Payroll Systems Manager, change requests are processed upon receipt of a Work Initiation Request form. Work Initiation Request forms are tracked in the Remedy system.	No relevant exceptions noted.
	18.2 – Staff identify, analyze and evaluate the functional specifications and, if needed, conduct internal and external meetings to elicit comments on proposed changes.	Obtained and inspected a sample of change request forms and ascertained that proper analysis of the request was performed before making changes.	No relevant exceptions noted.
	18.3 – Upon completion of software changes, software modifications are tested and formal acceptance is granted.	Obtained and inspected a sample of change request forms and ascertained that changes were tested and formal approval was granted before implementation.	No relevant exceptions noted.
	18.4 – Manual controls are used to ensure the correct version of software is being modified. These include: • Separate development, test and production libraries • The source code is copied directly from production and used to make the modifications • The modified source code is then moved, not copied, from development to test and then to production.	By inquiry of the HR/ Payroll Systems Manager, codes are moved into production once approved by the requestor. Individuals involved in development and testing do not move code into production. Ascertained by review of system parameters that three separate environments are set up and that the code is moved into production upon requestor's approval.	No relevant exceptions noted.

Figure 18: Application Controls: HR/Payroll Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	18.5 – Complete application documentation and user manuals are maintained and updated, as appropriate, to reflect modifications made to the application.	By inquiry of the HR/ Payroll Systems Manager and review of documentation maintained, ascertained that application changes are documented by TMU and that user manuals are updated by the Office of the State Controller (OSC) to reflect the changes.	No relevant exceptions noted.
	18.6 – Clients are notified of changes to the application if it will impact their interaction with the application.	By inquiry of the HR/ Payroll Systems Manager and review of sample notifications sent to the users, ascertained that affected clients are notified by TMU and/or OSC of any changes to the application.	No relevant exceptions noted.
	18.7 – All interfaced transactions by agencies to HR/Payroll require advance authorization from the Office of the State Controller.	Through inquiry of the HR/ Payroll Systems Manager and review of sample of requests for interface setup, ascertained that the OSC must approve interface setup requests.	No relevant exceptions noted.
	18.8 – Errors detected in CPPS input cannot be processed until the user corrects them online.	Ascertained by observation that input transactions cannot be processed until corrected online.	No relevant exceptions noted.

Figure 18: Application Controls: HR/Payroll Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	18.9 – 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 CA-7 prevents further processing after serious errors have occurred. In the event of an abnormal termination, the on-call programmer is notified, who is then responsible for resolution.	Obtained a sample of reports showing daily job runs and noted instances of processing errors detected by the program. By inquiry of the HR/ Payroll Systems Manager and inspection of sampled Remedy tickets, ascertained that the on-call programmers are notified of the errors, and then resolve the issue.	No relevant exceptions noted.
	18.10 – Each morning, system analysts review system assurance reports, which compare balances, and other reports, which will indicate that transactions were processed completely and accurately.	By inquiry and observation, ascertained that the HR/ payroll system programmers review processed logs on a daily basis to ensure no unresolved issues exist.	No relevant exceptions noted.

Figure 19: Application Controls: Financial and Timekeeping Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended.	19.1 – A formal change-management methodology is used to control and document changes to application software.	By inquiry of the Financial Systems Manager, change requests are tracked in the Remedy system. Ascertained that a project checklist is maintained for application changes.	No relevant exceptions noted.
	19.2 – Staff identify, analyze and evaluate the functional specifications and, if needed, conducting internal and external meetings to elicit comments on proposed changes.	By inquiry of the Financial Systems Manager and inspection of sampled Remedy tickets, ascertained that proper communication occurs between the programmers and the requestor before processing the change request.	No relevant exceptions noted.
	19.3 – Proposed changes to software are reviewed and approved prior to development.	Obtained and inspected sample project checklist and ascertained that change requests are reviewed and approved before development.	No relevant exceptions noted.
	19.4 – Upon completion of software development, modifications are tested and approval is granted by the supervisor.	Obtained and inspected sample project checklists and ascertained that testing staff signs off after testing the change. A supervisor reviews the results and signs off on the project checklist. KRONOS updates are tested in a separate environment and approved before moving into production.	No relevant exceptions noted.
	19.5 – Managerial or Requestor review of functionality, unit testing and acceptance testing is performed prior to implementation.	Inspected sampled project checklists and ascertained that testing is performed by the manager or the requestor, as applicable, before implementation.	No relevant exceptions noted.

Figure 19: Application Controls: Financial and Timekeeping Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	19.6 – Manual controls are used to ensure the correct version of software is being modified. These include: • Separate development, test and production libraries • The source code is copied directly from production and used to make the modifications • The modified source code is then moved, not copied, from development to test and then to production.	Through inspection of a sample of project binders, ascertained that Financial Systems Manager signs off on project checklists after verifying code and moves software to production.	No relevant exceptions noted.
	19.7 – Complete application documentation and user manuals are maintained and updated, as appropriate, to reflect modifications made to the application.	By inquiry of the Financial Systems Manager and inspection of project checklists, noted that an individual is designated for updating applicable documentation.	No relevant exceptions noted.
	19.8 – Clients are notified of changes to the application if it will impact their interaction with the application.	Through inquiry of the Financial Systems Manager and inspection of sample release letters/notifications, ascertained that users are notified of the changes, if applicable.	No relevant exceptions noted.
	19.9 – All interfaced transactions by agencies to COFRS require advance authorization from the Office of the State Controller.	Through inquiry and inspection of requests for interfaces, determined that COFRS interfaces are approved by OSC.	No relevant exceptions noted.

Figure 19: Application Controls: Financial and Timekeeping Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	19.10 – A user ID and password are required to enter or modify transactions in COFRS and KRONOS systems.	Observed process requiring login and sign on to modify transactions in COFRS and KRONOS.	No relevant exceptions noted.
	19.11 – One person in each agency is appointed as the Agency Security Administrator. The Agency Security Administrator has update rights only for users in their agency on the main security table for COFRS, the ASEC table.	Inquired of the Financial Systems Manager and inspected authorization forms signed by OSC for appointing agency security administrator for COFRS. KRONOS security administrators are set up by the KRONOS team upon receipt of an access request form. No authorization is needed from OSC.	No relevant exceptions noted.
	19.12 – Errors detected in COFRS and KRONOS input cannot be processed until the user corrects them online.	By inquiry and observation of the Financial Systems Manager, ascertained that inputs are not processed until transactions are correct.	No relevant exceptions noted.
	19.13 – The CORE supervisory routines require that all transactions be edited and approved prior to acceptance in COFRS.	By inquiry and observation of the Financial Systems Manager, ascertained that inputs are not processed until transactions are correct.	No relevant exceptions noted.
	19.14 – Batches are rejected in COFRS if the transaction count and total amount of the batch do not match the proof totals.	Obtained and inspected a sample of batches rejected/ accepted and ascertained that transaction/batch counts must total.	No relevant exceptions noted.

Figure 19: Application Controls: Financial and Timekeeping Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	19.15 – 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 maintain an electronic log detailing all such changes. A representative of the Office of the State Controller authorizes all changes to the ledgers in writing.	Through inquiry of the Financial Systems Manager, noted that manual ledger changes must be authorized by OSC. Obtained and inspected written authorization granted by OSC for making manual change in the ledger.	No relevant exceptions noted.
	19.16 – 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 account transaction IDs and noted IDs edit against an ID table, batch numbers are unique and IDs must be unique during accounting period.	No relevant exceptions noted.
	19.17 – 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 CA-7 prevents further processing after serious errors have occurred. In the event of an abnormal termination, on call programmer is notified who is then responsible for resolution.	Inspected instances where the process was abnormally terminated and ascertained that a programmer was notified to resolve the issue.	No relevant exceptions noted.
	19.18 – Each morning, system analysts review system assurance reports, which compare balances, and other reports, which will indicate that transactions were processed completely and accurately.	By inquiry and observation, noted that the Financial Systems Manager/ programmers review daily logs. No documentation is retained after the review.	No relevant exceptions noted.

Figure 19: Application Controls: Financial and Timekeeping Systems			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	19.19 – Access to Infopac and Document Direct financial reports is granted upon individual agency's approval and is maintained by COFRS helpline. Users may access only reports assigned to their ID.	Based on inquiry of the COFRS helpline staff and inspection of sample access authorization form, ascertained that proper approval is required before granting access to financial reports.	No relevant exceptions noted.

Figure 20: Report Management System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that Document Direct processing controls are in place.	20.1 – Access to reports or portions of reports are limited to users with a business reason view.	Obtained and inspected selected emails requesting access be modified for specific reports. Obtained and inspected Distribution Cross-reference by Recipient report. Obtained and inspected initial document access request forms. Obtained and inspected screen shots of report access for selected users.	No relevant exceptions noted.
	20.2 – An SLA exists describing service expectations.	Obtained and inspected Document *Direct Service Level Announcement.* Ascertained that the supplied document defines the expected service levels.	No relevant exceptions noted.
	20.3 – Access to reports is requested using an access authorization form.	Obtained and inspected selected emails requesting access be modified for specific reports. Obtained and inspected initial document access request forms. Ascertained that for an existing Document, Direct user access modification requires that the requester submit the recipient's ID, the requested report ID and the agencies requested.	No relevant exceptions noted.
	20.4 – Access to reports is authorized by customer department security administrators.	Obtained and inspected selected emails requesting access be modified for specific reports. Obtained and inspected Distribution Cross-reference by Recipient report.	No relevant exceptions noted.

Figure 20: Report Management System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	20.5 – Access authorization forms are saved.	Obtained and inspected initial document access request forms. Ascertained that no new access requests were submitted during the period.	No relevant exceptions noted.

Figure 21: Server Housing and Hosting			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that server deployment and management processes are common and repeatable to successfully support Hosted test and production servers.	21.1 – The Server Team Technical and Project Lead uses the Project Planning document to identify application requirements so that Hosted server resources are configured appropriately.	Obtained and inspected selected samples of completed project plans.	No relevant exceptions noted. See Recommendation #3.
	21.2 – Weekly review of Server Team projects provide an avenue for Server Team leads to give status updates on server deployments, which allows collaboration amongst the team to verify processes or tasks are not out of sync with documented expectations. The Project List is used to help track the status of ongoing projects, along with the Project Planning document.	Obtained and inspected selected samples of project flow chart and project weekly review/status reports.	No relevant exceptions noted.
	21.3 – Servers are acquired via the DoIT procurement approval process, which uses a Purchase Request Form identifying details of the merchandise to be purchased.	Obtained and inspected Department of Personnel & Administration Procurement Requests.	No relevant exceptions noted.
	21.4 – Server 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.	Obtained and inspected DoIT *Server Build and Deployment Procedure Guide*. Obtained and inspected copy of the online server inventory of systems configured and added to the server pool.	No relevant exceptions noted. See Recommendation #7.

Figure 21: Server Housing and Hosting			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	21.5 – A Remedy ticket is created to identify the necessary approval and action requirements needed to properly initiate a change on a server.	Obtained and inspected Remedy tickets listing. Ascertained that changes are entered into the Remedy system to identify the necessary approval and action requirements.	No relevant exceptions noted.
	21.6 – All changes are approved by the customer and Server 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.	Obtained and inspected selected samples of change requests. Observed that approvals were indicated by the customer and by DoIT/ISOC personnel.	No relevant exceptions noted.
	21.7 – Changes are entered in Remedy to identify steps to accomplish the change. Updates are recorded in the activity pane of the change ticket until the change is successfully completed.	Obtained and inspected Remedy tickets listing. Ascertained that changes are entered into the Remedy system and tracked through to completion.	No relevant exceptions noted.
	21.8 – 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, who use Event Viewer (log viewing program) to access server logs to further troubleshoot the problem.	By observation and inspection, ascertained that NetMan Server is implemented and is monitored by the Network Operations Center (NOC) 7X24X365. Obtained and inspected screen print of DoIT servers monitored by the NOC.	No relevant exceptions noted.

Section VI
Status of Implementation of Prior Recommendations

Status of Prior Recommendations

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
	From the SAS 70 for Fiscal Year Ended June 30, 2005		
1	DoIT should provide for more centralized review and guidance for backup and restoration procedures for all systems housed and hosted at DoIT.	**Implementation Date: July 2006.** The Computing Services organization was restructured on April 1, 2006, to meet this need. A new storage management group has been formed and a job announcement has been posted to hire a storage manager.	**Partially Implemented.** The storage manager is hired. Backup and restore capability for housed services are an agency responsibility. A Storage User Group is planned for implementation in Fiscal Year 2008.
2	DoIT should implement regular internal data recovery testing on a sampling basis in addition to the formal annual data recovery test.	**Implementation Date: June 2006.** Standard Operating Procedures executed by the storage management group to meet backup service level commitments will be modified by June 30, 2006, to perform the suggested recovery testing.	**Partially Implemented.** 1. A storage user group has been formed to collect statewide backup and restoration requirements. 2. A test virtual server and archive storage device have been installed and tested at eFORT. 3. Two Storage Area Network (SAN) devices are being collaboratively purchased and installed at eFORT between DPA and CDHS. DoIT reports that personnel constraints in the storage management group have not allowed them to fully implement this recommendation to date.

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
3	DoIT should review and enhance segregation of duties among programming and testing staff.	**Implementation Date: June 2006.** For CPPS, software testing and approval is always required by the requestor of the software change. In most cases, this is either a representative from the Central Payroll Unit of the Office of the State Controller or from the Division of Human Resources. In all other cases, testing and approval goes back to the requesting agency. Resource constraints prohibit the segregation of duties between design and programming. Changes will be instituted to require a design review by management for large or high impact projects. These changes will take effect not later than June 30, 2006. For COFRS, implementation (the move of software into production) is a separate function. The complete separation of design and testing is not practical because of the maturity of the system, the budgeted level of staff and the volume of work. However, mitigating controls have been implemented. For example, the Financial Management Systems manager reviews and approves design and system testing.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
4	DoIT should improve its management of third-party service contracts.	**Implementation Date: June 2006.** Currently, this process is being done by several individuals on a risk-based approach. We believe this is an appropriate practice at this time. The Department will review its control objectives and revise as appropriate.	**Partially Implemented.** An SOP was written and the process implemented in January 2007. The process includes a checklist to track DoIT assets allocated to a contractor and access granted. The process also includes a Performance Report for tracking the progress of the contactor against deliverables throughout the life of the engagement. However, note current year Recommendation #4.
5	DoIT should strengthen the Top Secret security administration.	**Implementation Date: October 2006.** (1) The Information Security Operations Center (ISOC) has assumed all TSS responsibility for DoIT except for very basic administration functions such as password resets and access to some datasets that are performed by the Service Center. The ISOC is working on documenting procedures to formalize these roles. (2) Our primary administrator has completed advanced TSS training and the backup is scheduled for advanced training in October 2006. (3) The ISOC has commenced the annual TSS audit for DoIT and will be developing a Standard Operating Procedure describing the audit procedures.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
6	DoIT should institute documented incident response criteria and response escalation procedures.	**Implementation Date: June 2006.** We have developed and tested incident response and escalation procedures. These procedures involve logging all security events that the ISOC investigates in a ticketing system and measuring response time through that system. A contractor has been retained to write a formal incident response plan.	**Implemented.**
7	DoIT should evaluate and improve physical security around warrant stock during processing.	**Implementation Date: May 2006.** Additional controls have been implemented. For example, there is now a combination lock on the vault door accessed by individually-assigned codes. Individual access can be monitored via access logs and access can be verified as to being in response to valid processing activity.	**Implemented.**
8	DoIT should implement and track service level agreements for all DoIT clients.	**Implementation Date: April 2006.** The Computing Services organization was restructured on April 1, 2006, to meet this need; an individual is now responsible for establishing service level performance monitoring and reporting to DoIT management.	**Partially Implemented.** DoIT is moving away from formal SLAs in favor of an actionable Service Catalog. However, note current year Recommendation #3.

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
9	DoIT should institute a process to retain source documents for reference and audit for an appropriate period commensurate with the data.	**Implementation Date: June 2006.** Source documents will be scanned and kept electronically.	**Partially Implemented.** Signed approval and review forms from SOP review process are retained and emails are sent to all DoIT staff notifying them of changes to the SOPs and these emails are retained. DoIT reports that other source documentation such as agendas, emails, and checklists needed for audit purposes will be kept as well. However, note current year Recommendation #11.
10	DoIT should ensure critical information and decisions are communicated and reinforced with affected employees.	**Implementation Date: June 2006.** When SOPs are published, an email will be sent to Computing Services staff notifying them of the updates. General Staff meeting agendas and follow-up comments will be implemented by fiscal year end.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
11	DoIT should review documentation against control objectives and current operations to ensure consistency with current practice.	**Implementation Date: July 2006.** June 2006 – SOP 2900 was re-written appropriate to the change to Trilogy locks (from Cipher locks) on all doors on the raised floor. July 2006 – SOP 8806 was rewritten to enable a post outage review to ensure root cause of outages is determined, long-term resolutions implemented or responsibility for these items is assigned to individuals for remediation. Effective June 2006 – As SOPs are reviewed, next review date is set to one year in the future and reviewed annually thereafter. In 2004, a standard form for CPPs was created. Because there are thousands of CPPs, we cannot get customer cooperation to re-write all CPPS in the new format immediately. It has been an ongoing process since 2004 to provide this standard form to customers when they need to update or create new CPPs and to reject CPPs sent in any other format.	**Implemented.**
12	DoIT should eliminate the redundancy between the outage notifications and remedy issue tracking system.	**Implementation Date: April 2006.** The Computing Services organization was restructured on April 1, 2006, to meet this need. An individual has been identified as responsible for the consolidation of outage reporting and defining processes for Remedy issue tracking.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
	From the Report of the State Auditor for Fiscal Year Ended June 30, 2004		
17a	The Department of Personnel & Administration should ensure that the technology management unit improves its controls over COFRS access by requiring financial system team management to provide end dates enabling the automated process to suspend contractors' access.	**Partially Implemented.** The controls implemented in February 2005 continue to be followed.	**Implemented.** See Recommendation #2.
17b	The Department of Personnel & Administration should ensure that the technology management unit improve its controls over COFRS access by implementing a process to ensure financial system team management reviews access privileges in a timely manner when employee and contractor assignments change.	**Partially Implemented.** The controls implemented in February 2005 continue to be followed.	**Implemented.** See Recommendation #2.
	From the SAS 70 – March 2003		
3	Implement a security-awareness training program to supplement current security policies and procedures. All Data Center and TMU employees should be required to sign an annual statement of compliance acknowledging Data Center computer security policies and denoting completion of security awareness training.	**Partially Implemented.** A security awareness course was designed and implemented in 2003 but was not conducted in 2004. A DoIT specific security awareness training class with signoff is planned for 2006. Expected implementation date: December 31, 2006.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
	From the SAS 70 – April 2002		
8	Consider the use of version control software for application changes.	**Not Implemented.** DoIT reported it considered the purchase and use of automated version control software for COFRS but there is still not sufficient operating or FTE budget to accomplish this. Given the relatively few code changes that occur on a system as mature as COFRS, the return on investment is questionable even if the budget were available. No further action is planned. BKD Note: Version control software should be reconsidered in the context of all supported systems, not just COFRS. Such software can assist in overall code and version management, as well as contribute to management of segregation of duties and testing.	**Not Implemented.** DoIT reports that there is still not sufficient operating or FTE budget to accomplish this. See Recommendation #12.
9	Implement a security awareness training program.	**Partially Implemented.** A security awareness course was designed and implemented in 2003 but was not conducted in 2004. A generic training class has been procured through a Homeland Security grant and will be implemented for 2006. Expected implementation date: December 31, 2006.	**Implemented.**

No.	Recommendations	Prior Audit Report Status	August 2007 Update/Comments
	From the Report on Performance Measures – September 2001		
1	Implement service level agreements with customers.	**Partially Implemented**. Seven service level announcements have been created for mainframe computer operations. Service level agreements are generated for each new server housing or hosting customer effective July 1, 2004. Note: However, note September 2005 SAS 70 recommendation #8.	**Partially Implemented**. DoIT is moving away from formal SLAs in favor of an actionable Service Catalog. See Recommendation #3.
12	Generate monthly security metrics.	**Not Implemented.** According to DoIT, metrics were not implemented due to staffing limitations and intrusiveness of tools. Event correlation is under development. No implementation date provided.	**Implemented.**
	From the SAS 70 – April 2000		
10	As equipment changes in the Data Center or major renovations are performed, the Data Center should re-engineer both power and signal cable ducts to provide separation and safety.	**Not Implemented.** According to DoIT, preparations are underway to analyze power capacity and usage as part of a larger goal of implementing standards for power and signal cabling in the Data Center in general when a sufficient budget is available. No implementation date provided.	**Not Implemented.** DoIT performed an analysis of its Power Distribution Units in November 2005. Plans to separate power and network cabling have been tabled until current plans for State data center consolidations are completed. See Recommendation #13.

Section VII
Other Information Provided by the Division of Information Technologies Data Center and Technology Management Unit

Glossary of Acronyms

Acronym	Definition
ADS	Applicant Data System
ATL	Automated Tape Library
ATM	Asynchronous Transfer Mode
BCV	Business Continuity Volume
BI/ETL	Business Intelligence/Extract, Transform and Load
BGP	Border Gateway Protocol
BPOP	Boulder Giga POP
CBI	Colorado Bureau of Investigation
CBMS	Colorado Benefits Management System
CDHS	Colorado Department of Human Services
CDLE	Colorado Department of Labor and Employment
CDOR	Colorado Department of Revenue
CDOT	Colorado Department of Transportation
CDPHE	Colorado Department of Public Health and Environment
CDPS	Colorado Department of Public Safety
CICSP	Customer Information Control System Production
CIN	Colorado Information Network
CIVICS	Cooperative Interactive Video in Colorado State Government
COFRS	Colorado Financial Reporting System
CPOPs	County Points of Presence
CPPS	Colorado Personnel Payroll System
DBA	Database Administrator
DDN	Digital Data Network
DLT	Digital Linear Tape
DoIT	Division of Information Technologies
DNR	Department of Natural Resources
DOR	Department of Revenue
DPA	Department of Personnel & Administration
DR	Disaster Recovery
DS-1	Digital Signal 1
DSL	Digital Subscriber Line
DST	Daylight Savings Time
DU	Denver University
EFT	Electronic Funds Transfer
EMPL	State Employee Database System
ERP	Enterprise Resource Program
ESCON	Enterprise Systems Connection
FDW	Financial Data Warehouse

Glossary of Acronyms cont.

Acronym	Definition
FICON	Fiber Connectivity
FLC	Fort Lewis College
FMLA	Family Medical Leave Act
FR	Frame Relay
FRGP	Front Range Giga POP
FTC	FRGP Technical Committee
FTP	File Transfer Protocol
GFS	Government Financial System
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HBA	Host Bus Adaptor
HRDW	Human Resources Data Warehouse
IBM	International Business Machines
ICG	International Coordination Group
IML	Initial Machine Load
IPL	Initial Program Load
ISDN	Integrated Services Digital Network
DDN	Digital Data Network
JUNOS	A routing operating system designed specifically for the Internet
KVM	Keyboard, Video Mouse switch
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
MIPS	Million Instructions per Minute
MNT	Multi-Use Network
MUX	Multiplexer
MVS	Multiple Virtual Storage
N20	Natural Application Change Management System
NCAR	National Center For Atmospheric Research
NE	North East
NOAA	National Oceanic and Atmospheric Administration
NOC	Network Operations Center
OC	Optical Carrier
OCIN	Open Colorado Information Network
PAC	Predict Application Control
PDU	Power Distribution Unit
PM	Preventive Maintenance
PROD LPAR	Production – Logical Partition
Q&As	Questions and Answers
RAID	Redundant array of independent disks
SAN	Storage Area Network
SMS	Storage Management System

Glossary of Acronyms cont.

Acronym	Definition
SONET	Synchronous Optical Network
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSN	Social Security Number
SU	Service Unit
TEST LPAR	Test – Logical Partition
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSS	Top Secret Security
UCAR	University Corporation for Atmospheric Research
UCB	Unit Control Block
UDP	Utility Distribution Panel
UDW	Utility Data Warehouse
UPSA or D	Uninterruptible Power Supply “A” or “D”
USPS	United States Postal Service
UW	University of Wyoming
VM	Virtual Machine
VSAM	Virtual Storage Access Method
VTS	Virtual Tape Storage
WAN	Wide Area Networking

Distribution Page

The electronic version of this report is available on the Web site 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 1897 when requesting this report.