COLORADO DEPARTMENT OF PERSONNEL AND ADMINISTRATION
DIVISION OF INFORMATION TECHNOLOGIES DATA CENTER
AND STATEWIDE APPLICATION SYSTEMS

Report on Controls Placed in Operation
and Tests of Operating Effectiveness

For the Period November 1, 2001 through April 30, 2002

STATE OF COLORADO
LEGISLATIVE AUDIT COMMITTEE

2002 MEMBERS

Senator Jack Taylor
Chairman

Senator Ron Tupa
Vice-Chairman

Senator Norma Anderson

Representative Fran Coleman

Representative Glenn Scott

Senator Stephanie Takis

Representative Val Vigil

Representative Tambor Williams

OFFICE OF THE COLORADO STATE AUDITOR

Joanne Hill
State Auditor

Sandy Ronayne
Legislative Auditor

KPMG LLP

Edwin Holt

Cody Daniels

Jedd Pierson

COLORADO DEPARTMENT OF PERSONNEL AND ADMINISTRATION DIVISION OF INFORMATION TECHNOLOGIES DATA CENTER AND STATEWIDE APPLICATION SYSTEMS

Report on Controls Placed in Operation
and Tests of Operating Effectiveness

Table of Contents

707 Seventeenth Street
Suite 2700
Denver, CO 80202

Report of Independent Public Accountants

Members of the State of Colorado Legislative Audit Committee:

We have examined the accompanying description of controls related to the Colorado Department of Personnel and Administration Division of Information Technologies (DoIT) Data Center (Data Center) and the Statewide Application Systems unit related to their support of the Colorado Financial Reporting System (COFRS) application, as described in Section V. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Data Center's and Statewide Application Systems' controls that may be relevant to a user organization's internal control structure, (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 client organizations applied the internal controls contemplated in the design of Data Center's and the Statewide Application Systems' controls, and (3) such controls had been placed in operation as of April 30, 2002. The control objectives were specified by the management of the Data Center and Statewide Application Systems. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the controls presents fairly, in all material respects, the relevant aspects of the Data Center's and the Statewide Application Systems' controls that had been placed in operation as of April 30, 2002. 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 the Data Center's and the Statewide Application Systems' controls.

As discussed in the accompanying description for Control Objectives 2 and 15, access to systems and data is governed by policies established to ensure that (1) proper segregation of duties is achieved in the areas of application development, computer operations and security administration, and (2) Data Center and Statewide Application Systems employees are granted access to systems and data based on the least permission necessary to accomplish their job functions. Access permissions assigned by the Data Center and Statewide Application Systems do not comply with these policies. We noted several instances where proper segregation of duties has not been achieved, as well as employees with access privileges that were inappropriate based on their assigned job functions.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, which are presented in Section VI of this report, to obtain evidence about their effectiveness in meeting the related control objectives, described in Section VI, during the period from November 1, 2001 to April 30, 2002. The specific controls and the nature, timing, extent, and results of the tests are listed in Section VI. This information has been provided to user organizations of the Data Center and of the COFRS application and to their independent auditors to be taken into consideration, along with information about the internal control structure at user organizations, when making assessments of control risk for user organizations. In our opinion, except for the deficiencies referred to in the preceding paragraph, the controls that were tested, as described in Section V, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section VI were achieved during the period from November 1, 2001 to April 30, 2002

The relative effectiveness and significance of specific controls of the Data Center and Statewide Application Systems and their effect on assessments of control risk at user organizations are dependent on 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 of the Data Center and Statewide Application Systems is as of April 30, 2002, and information about tests of the operating effectiveness of specified controls covers the period from November 1, 2001 to April 30, 2002. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls of the Data Center and Statewide Application Systems is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

The information in Section VII describing the Data Center's disaster recovery plan is presented by the Data Center to provide additional information and is not part of the Data Center and Statewide Application Systems' description of controls that may be relevant to a user organization's internal controls. Such information has not been subjected to the procedures applied in the examination of the description of controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

This report is intended solely for use by members of the Legislative Audit Committee, management of the Data Center and Statewide Application Systems, 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.

KPMG LLP

Denver, Colorado
April 30, 2002

SECTION II REPORT SUMMARY

AUTHORITY, STANDARDS AND PURPOSE/SCOPE OF EXAMINATION

This examination of the general controls at the Data Center and Statewide Application Systems was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct audits of all departments, institutions, and agencies of State government. This examination was conducted in accordance with standards established by the American Institute of Certified Public Accountants (AICPA). The period under review was November 1, 2001 through April 30, 2002.

This report on controls placed in operation and tests of operating effectiveness is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the Data Center‘s and Statewide Application Systems' internal controls that may be relevant to a user organization's internal controls. This report, when coupled with an understanding of the internal controls in place at user organizations, is intended to assist in the assessment of overall internal controls relative to the transactions processed by the COFRS application.

Our examination was restricted to selected services provided to users of the Data Center and the COFRS application, and accordingly, did not extend to procedures in effect at individual user organizations. The examination was conducted in accordance with the AICPA Statement on Accounting Standards No. 70, *Reports on the Processing of Transactions by Service Organizations.* It is each interested party's responsibility to evaluate this information in relation to internal controls in place at the respective user organization and assess overall control risk. If controls at user organizations are not in place or are ineffective, controls at the Data Center and Statewide Application Systems are not designed to compensate for such weaknesses.

The control environment represents the collective effect of various factors on establishing, enhancing or mitigating the effectiveness of controls. Our procedures included tests of the following relevant elements of the Data Center's and Statewide Application Systems' control environment:

- Organizational structure and management.
- System software support.
- Application development and modification.
- Protection of physical assets.
- Logical access to systems and data.
- Application processing controls (including input and output).

Such tests included inquiry of appropriate management, supervisory, and staff personnel; inspection of documents and records; and observation of activities and operations.

The description of controls is the responsibility of the Data Center and Statewide Application Systems. Our responsibility is to express an opinion about whether the controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by Data Center and Statewide Application Systems' management, were achieved during the period covered in our report (November 1, 2001 through April 30, 2002).

SUMMARY OF FINDINGS AND RECOMMENDATIONS

The following represents the more significant findings contained in our report:

Logical Access

Logical access controls should provide reasonable assurance that computer resources such as data files and applications are protected against loss, unauthorized modification or disclosure. Logical access should be administered in a manner which restricts users to the minimum access necessary to perform his or her day-to-day job functions. In addition, access to critical system functions (application development, computer operations and system security administration) should be appropriately segregated.

The control environment supporting logical security should include controls to systematically authorize and assign access to new users, monitor the access and actions of existing users, and provide for the timely removal of access privileges when a user's responsibilities change or when employment is terminated.

Security software programs are used to control logical access and are designed to prevent and detect unauthorized access to systems and data. The Data Center uses Top Secret security software to control logical access to the COFRS application.

We reviewed the Data Center's policies and procedures governing the processes of initiating, monitoring and terminating user access. We also reviewed access granted to Data Center and Statewide Application Systems' employees and compared the access to those policies. We noted certain logical access profiles and permissions within are not appropriately restricted to authorized individuals. We recommend the Data Center and Statewide Applications Systems make modifications to Top Secret logical access profiles and permissions including:

- Restrict security administration privileges to appropriate individuals using the least permissive designations.
- Limit user access to data and systems based on specific job responsibilities.
- Minimize the use of common/group accounts.
- Segregate access to critical system functions.

In addition, we recommend the Data Center establish a process to periodically review existing user profiles and access listings to ensure that access permissions are commensurate with users' current job responsibilities. Also, logs that record changes to security profiles should be reviewed on a consistent basis in order to identify and investigate unusual activity.

Finally, we recommend the Data Center perform a thorough review of logical access profiles that are routinely replicated to create new user access permissions. The review should be performed immediately for all existing profiles and repeated periodically to ensure that profiles remain appropriate for use in this manner.

SUMMARY OF PROGRESS IN IMPLEMENTING PRIOR AUDIT RECOMMENDATIONS

The Data Center and Statewide Application Systems have made significant progress in implementing the recommendations from the reports dated May 2000 and September 2001. A complete discussion of the status of implementation is provided in Appendix A – Disposition of Prior Recommendations.

RECOMMENDATION LOCATOR

No.	Page #	Recommendation	Agency Response	Implementation Date
1	12	Restrict logical access to systems and data to only properly authorized individuals.	Agree	September 15, 2002
2	13	Periodically review existing user profiles and access listin gs to ensure that access permissions are consistent with job responsibilities.	Agree	July 15, 2002
3	13	Consistently review the logs that capture changes to security profiles.	Agree	July 31, 2002 – Documentation of the SOP August 1, 2002 – First review
4	14	Configure network settings to maintain password generations and require password expiration.	Agree	August 30, 2002
5	14	Review profiles which are replicated to create new user logical access permissions.	Agree	Ongoing
6	14	Enhance system software change procedures to ensure documentation standards are met.	Partially Agree	September 1, 2002
7	15	Enhance application software change procedures to ensure documentation standards are met.	Agree	September 2002 – Phase-1
8	15	Consider the use of version control software for application changes.	Agree	May 2003
9	16	Implement a security awareness training program.	Agree	October 1, 2002– Course curriculum completed Second week of January 2002 – First class
10	16	Create employee training and development plans.	Agree	July 30, 2003

SECTION III OVERVIEW OF THE DIVISION OF INFORMATION TECHNOLOGIES DATA CENTER AND STATEWIDE APPLICATION SYSTEMS

The DoIT Data Center and Statewide Application Systems both reside under the Colorado Department of Personnel and Administration. The following outlines the mission, funding sources, and organization and functions of both the Data Center and Statewide Application Systems.

DoIT Data Center

Mission

The Data Center currently functions as a service bureau to provide data processing services to the executive, legislative, and judicial branches of State government.

The Data Center's mission is "to efficiently, effectively and economically provide quality information products and services to meet customer program objectives." The Data Center performs various services for State agencies that include converting and processing data, maintaining and backing up data, preparing reports, and ensuring that its computer system can be recovered in the event of a disaster. It also maintains a data communication network from its computer system to agency terminals and minicomputers.

The Data Center has established controls to ensure the security and integrity of users' data, programs and output, and the protection of its own equipment and software. The implementation of the Colorado Financial Reporting System (COFRS) in 1990 eliminated the former General Government Computer Center's responsibility for control of the development and maintenance of other portions of the State's central financial system. COFRS, now part of the Technical Business Applications Section of the Department of Personnel and Administration, has assumed these responsibilities.

The Data Center utilizes two primary methods of customer contact for the purpose of improving the Center: (1) the Customer Roundtable (CR), and (2) the direct customer meeting. The Data Center established the CR Forum to improve communications between itself and its users. The direct customer meeting was established to provide specific input regarding the direction and service levels of the Data Center.

Funding Sources

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, computer 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 2001, the Data Center received an appropriated spending authority of approximately $13 million to provide computer services to State agencies.

Organization and Functions

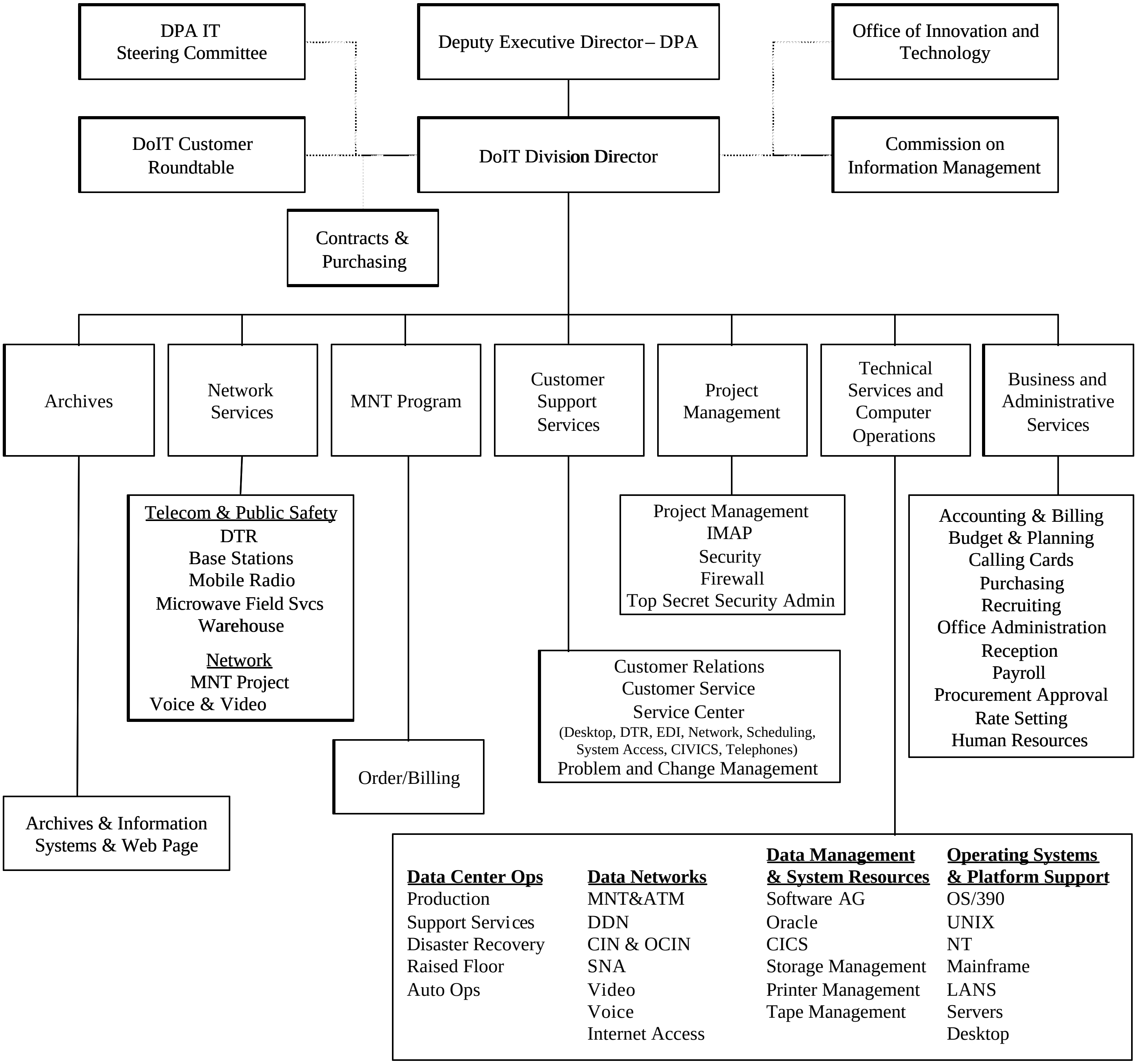
The Data Center operates 24 hours per day, seven days a week, including holidays. Approximately 57 of the DoIT 147 full-time equivalents (FTE) are directly involved with the Data Center. These FTE include:

- **Management:** The DoIT Division Director and Chief Technology Officer each spend approximately 50 percent of their time in the management of the Data Center; the Computing Services Manager is engaged full time in Data Center management. Management includes two FTE.

- **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. Data Center support is provided, in addition to the manager, by approximately two of the six FTEs within the Administrative/Financial and HR Services section. Additionally, the contract administration person adds another .5 FTE of effort.
- **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 Service Center is a functional area within Customer Services providing scheduling, console management, help desk, and video conference support. Approximately 11 of the 13 FTEs in Customer Services and one FTE in Security support the Data Center.
- **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. Desktop, Server and Local Area Network equipment directly operated by DoIT is supported within this functional group as well. These services are provided by 20 of the 42 FTEs in Computing Services.
- **Computer Operations:** These services include installing and operating computer and printing equipment, maintaining disk and tape systems, and the control and distribution of computer output. The disaster recovery function within this area is responsible for developing, implementing, coordinating, and monitoring the Data Center's disaster recovery plan; 20 FTEs from the Computing Services provide these services.

Division of Information Technology

Functional Organization Chart



DPA IT Steering Committee

Deputy Executive Director – DPA

Office of Innovation and Technology

DoIT Customer Roundtable

DoIT Division Director

Commission on Information Management

Contracts & Purchasing

Archives

Network Services

MNT Program

Customer Support Services

Project Management

Technical Services and Computer Operations

Business and Administrative Services

Telecom & Public Safety
DTR
Base Stations
Mobile Radio
Microwave Field Svcs
Warehouse

Network
MNT Project
Voice & Video

Project Management
IMAP
Security
Firewall
Top Secret Security Admin

Accounting & Billing
Budget & Planning
Calling Cards
Purchasing
Recruiting
Office Administration
Reception
Payroll
Procurement Approval
Rate Setting
Human Resources

Customer Relations
Customer Service
Service Center
(Desktop, DTR, EDI, Network, Scheduling, System Access, CIVICS, Telephones)
Problem and Change Management

Order/Billing

Archives & Information Systems & Web Page

Data Center Ops	Data Networks	Data Management & System Resources	Operating Systems & Platform Support
Production	MNT&ATM	Software AG	OS/390
Support Services	DDN	Oracle	UNIX
Disaster Recovery	CIN & OCIN	CICS	NT
Raised Floor	SNA	Storage Management	Mainframe
Auto Ops	Video	Printer Management	LANS
	Voice	Tape Management	Servers
	Internet Access		Desktop

Statewide Application Systems

Organization and Functions

Statewide Application Systems is responsible for acquiring, implementing, operating and maintaining statewide information systems for the State of Colorado. Seven computer software systems meet the definition of "statewide information system" and consequently fall under the responsibility of Statewide Application Systems.

- The **Colorado Financial Reporting System (COFRS)** is the accounting system of final record used by the State of Colorado. All State agencies except higher education institutions use COFRS directly to perform their day-to-day accounting functions. Higher education institutions utilize their own accounting systems, but pass along summarized accounting information to COFRS through interface programs.
- **View Direct/INFOPAC**, licensed from Mobius Management Systems, provides report archiving and management for COFRS reports.
- The **Employee Data Base (EMPL)** tracks the history of all employees, positions and classifications of the State. It implements personnel rules and yearly cost of living increases. The system is used by all State agencies, certain higher education institutions and the judicial branch of government.
- The **Applicant Data System (ADS)** tracks applicants, employment tests and test schedules and monitors the applicant selection process for all branches of state government except the Legislature. The system allows personnel administrators to monitor the status of applicants throughout the application and testing process, and posts job announcements on the Internet. For certain classifications of jobs, ADS develops automated applicant lists.
- The **Colorado Personnel Payroll System (CPPS)**, purchased from Integral Systems Inc., pays the approximately 30,000 employees of the State, plus additional Higher Education employees.
- The **BIDS** system provides a means for agency purchasing staff to advertise bidding opportunities on the Internet, and facilitates the distribution of bid information to interested vendors.
- **Billing Systems** collects information about work performed for other State agencies by various divisions, automatically invoices this work, and interfaces (submits) the invoices to COFRS. This system also provides detailed information from the invoices to departments and agencies.
- **Colorado Automotive Reporting System (CARS)** integrates all aspects of management and billing of the State's vehicle fleet. Using a relational-object database, CARS incorporates full life-cycle management of State-owned vehicles.
- **Financial Data Warehouse (FDW)** provides users with the ability to create their own customized reports and/or views of the data. All data is loaded into the warehouse on a daily basis and is extracted directly from our ledgers.
- **Utility Data Warehouse (UDW)** is a system that is currently under development, parts of which are being utilized by various agencies. This system contains utility bills, payments and other data relevant to energy usage and analysis by state energy managers.

For all applications listed above, activities include: (1) application specification, design, programming and modifications, (2) system administration, monitoring and tuning; development of batch JCL and job scheduling, (3) application assurance verification; provision of consultation, helpdesk, training and documentation services to agencies, (4) development and administration of backup, archiving and disaster recovery programs, and (5) unit and system testing; and management of agency extract and interface processes.

SECTION IV FINDINGS AND RECOMMENDATIONS

Introduction

Our responsibility was to express an opinion about whether:

- The description of controls presents fairly, in all material respects, the relevant aspects of the Division of Information Technologies (DoIT) Data Center and Statewide Application Systems' controls that had been placed in operation as of April 30, 2002.
- The controls, as described in DoIT's Data Center and Statewide Application Systems' description of controls, 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 structure controls contemplated in the Data Center and Statewide Application Systems' controls.
- The controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by Data Center and Statewide Application Systems management, were achieved during the period covered by our report.

We identified opportunities within the Data Center and Statewide Application Systems, specifically the COFRS application, for improving the controls associated with the processing of transactions for clients by the Data Center and the COFRS application. This section contains recommendations regarding the effectiveness of controls specified by Data Center and Statewide Application Systems management.

Limit Logical Access to Systems

Logical access controls should provide reasonable assurance that computer resources such as data files and applications are protected against unauthorized modification, disclosure and loss. Industry standards and Data Center policy dictate that logical access be administered in a manner that restricts users to the minimum access necessary to perform his or her day-to-day job functions. In addition, logical access should be assigned on an individual level to provide specific accountability for system activities. Finally, access to critical system functions (application development, computer operations and system security administration) should be appropriately segregated.

We reviewed logical access to the mainframe that houses the COFRS application. The Data Center uses Top Secret security software, which is designed to prevent and detect unauthorized access to systems and data. We noted that certain security profiles and user permissions within Top Secret are not sufficiently restrictive, specifically:

- Security administrative privileges are not appropriately limited. We reviewed all user accounts (23) with access to security administration privileges and found six Data Center employees that do not need this access to perform their job requirements.
- Access privileges are not assigned in a manner that limits the user to the minimum needed to perform his or her job requirements. A total of 103 access permissions to specific functions within security administration, system software, and scheduling were reviewed. Of these, we noted 22 exceptions where access to the specific function was not required, or where the access level exceeded the level necessary to perform job requirements.
- Common/group accounts and passwords are utilized, although Data Center policy dictates that accounts be associated with individuals to provide accountability.
- Segregation between programming and production is not achieved in all cases. We noted one COFRS programmer that also has security administration responsibilities for Statewide Application Services. Security administration privileges provide access to production systems.

Ineffective logical access controls increase the risk of unauthorized access to data and systems, which may result in the modification, loss, damage or theft of valuable information and/or resources and may ultimately affect data reliability. At a minimum, users may obtain access to sensitive data and systems for which they are not authorized.

Recommendation No. 1

We recommend the Data Center and Statewide Applications Systems make the following modifications to logical access profiles and permissions within Top Secret:

- Limit the use of Master Security Control Administration designation.
- Restrict Security Administration privileges to appropriate individuals.
- Limit user access to data and systems based on specific job responsibility.
- Minimize the use of common/group accounts; make necessary assignments at the individual level to ensure individual accountability.
- Assign separate user accounts to individuals for use when performing functions that are not part of their day-to-day responsibilities (i.e., back-up positions). Audit logging of back-up Access Identifications (ACID) and associated activities should be considered.
- Segregate access to critical system functions. Where complete segregation is not feasible due to staffing limitations, designate separate user accounts for secondary/conflicting roles. Activities associated with secondary/conflicting roles should be logged and independently reviewed.

Response

Agree.

The Master Security Control Administration issue was dealt with immediately upon notification of this potential security discrepancy.

Permissions have been revoked for positions identified during the audit with the exception of those referenced in Standard Operating Procedures (SOP) #8808, which are required to perform day-to-day duties.

We will periodically review day-to-day requirements with the DoIT operating units to update documentation regarding this issue. Any changes to the documentation will be included in SOP #8808. After this review, security access will be limited to those required to perform normal duties.

We will minimize the use of common/group accounts within the boundaries of normal job requirements.

We agree with the intent, but feel that using a separated account is more vulnerable to security risks than using the automatically expiring temporary privileges assigned within the existing account structure. All ACIDs and their activity are already logged and monitored.

Our policy is to limit Top Secret security administration to development managers/leads. We intend to review our policies and procedures this year.

Implementation Date

September 15, 2002.

Review Access Privileges of Existing Users

The control environment processes supporting logical security should include controls to systematically authorize and assign access to new users, monitor the access and actions of existing users, and provide for the timely removal of access privileges when a user's responsibilities change or when employment is terminated.

We reviewed the Data Center's processes for initiating, monitoring and removing logical access to systems and data. The Data Center has processes in place to grant and enhance access for users, and to remove access for terminated users. However, they do not have a process to periodically review access privileges for existing users. As a result, users may have access to systems and data that is no longer commensurate with their current job responsibilities.

Recommendation 2

We recommend the Data Center establish processes to review existing access to ensure that permissions are consistent with users' current job responsibilities. We recommend a thorough review of the profiles for all existing users, cycling through the total group of Data Center employees within the next 1 to 2 years. In addition, a process should be put in place for the ongoing review of access to specific critical functions or systems (i.e., security administration, system software, scheduling, etc.). Combined, these processes will help to ensure that access profiles and permissions are, and will remain, appropriate.

Response

Agree.

DoIT Security Administration will document a process to be followed addressing all of these issues and include in SOP 8808. Additionally, we will initiate the processes defined in this same SOP.

Implementation Date

July 15, 2002.

Review Changes to Security Profiles

The periodic review of system-generated logs can detect security problems, including unauthorized modifications to security profiles. We reviewed the Data Center's policies and procedures related to the audit logging of security profile changes. We noted that while the Data Center generates and maintains logs of changes to security profiles, the logs are reviewed for investigative purposes only after an incident occurs. As a result, inappropriate or unauthorized changes to security profiles may go undetected.

Recommendation 3

We recommend the security profile change logs be reviewed on a consistent basis for the purpose of identifying and investigating unusual activity.

Response

Agree.

A process will be documented and inserted into the SOPs for monthly review of DoIT managed changes by the Manager of Security and the DoIT Security Administrator.

Implementation Date

July 31, 2002 – Documentation of the SOP; August 1, 2002 – First review.

Strengthen Password Settings

Password account settings should be configured to enforce password criteria that are sufficiently robust such that passwords cannot be easily compromised. We reviewed the Data Center's current network Windows NT account settings and noted that passwords are not set to expire at predetermined intervals. In addition, systematic maintenance of password history is not activated. Maintaining password history requires users to create new passwords at each expiration and restricts the reuse of passwords. The current settings do not provide sufficient password protection, and as a result, passwords may be compromised to gain unauthorized access to systems and data.

Recommendation 4

We recommend the Data Center configure network Windows NT passwords to expire every 90 days and to maintain a minimum of eight generations of password history.

Response

Agree.

Setting will be changed to force password changes, and to maintain password generations.

Implementation Date

August 30, 2002.

Review Profiles Used to Grant Logical Access

Data Center policy dictates that users be granted access to systems and data at the minimum level necessary to perform their day-to-day job functions. We reviewed the Data Center's process for granting logical access to users. Security Administration personnel grant access to users after obtaining approval and direction from the employee's supervisor. We noted that access is generally granted by replicating the profile/permissions of an existing user with commensurate responsibilities. Top Secret is a highly effective, yet complex, security software product which allows multiple layers of access permissions and requires detailed profile and data set assignment for each user account. Given this complexity, granting access through replication of an existing user account may result in inappropriate access if the object of replication has not been thoroughly reviewed and deemed appropriate for use in this manner.

Recommendation 5

We recommend the Data Center perform a thorough review of all profiles used for replication. The review should be performed immediately for all existing profiles and repeated periodically to ensure that profiles remain appropriate for use in this manner.

Response

Agree.

The profiles created though replication will be periodically reviewed and the permissions will be integrated into the security review procedures. The replication methodology will continue to incorporate validity review by the system owner. The replicated permissions are developed and reviewed by the owner of the data, such as COFRS, CICS, etc. This serves to ensure necessary and sufficient access for new users.

Implementation Date

Ongoing.

Improve System Software Modification Documentation

We reviewed the Data Center's policies and procedures related to system software modifications. The policies are in place to help ensure that modifications to system software are appropriate, properly authorized, tested, approved, implemented and documented. We noted that policies are not consistently followed relative to the documentation of pre-implementation testing and the updating of inventory records to reflect system software installations or upgrades. Of the six system software modifications we reviewed, one did not have appropriate evidence of testing and was not included in the system software inventory.

Recommendation 6

We recommend the Data Center improve its process for system software modifications to ensure that all phases are fully documented, including evidence of testing.

Response

Partially agree.

The procedures will be reviewed to make certain that updating of the inventory database is included. Testing is, in many cases, performed by the product end-users rather than by Data Center staff. Our procedures will be reviewed to make certain that either adequate evidence of the provision of a means of testing, or the testing itself exists.

Implementation Date

September 1, 2002.

Improve Application Modification Documentation

We reviewed Statewide Application Systems' policies and procedures related to application software modifications. The policies are in place to help ensure that modifications to application software are appropriate, properly authorized, tested, approved, implemented, and documented. We noted that policies are not consistently followed relative to the documentation of pre-implementation testing. Of the six application software changes we reviewed, one did not have appropriate evidence of testing.

Recommendation 7

We recommend Statewide Application Systems improve their process for application software modifications to ensure that all phases are fully documented, including evidence of testing.

Response

Agree.

We are in the process of implementing a new Software Development Methodology, which will address this risk area, to achieve consistent and repeatable processes.

Implementation Date

September 2002 – Phase-1.

Consider Utilizing Version Control Software for Application Development

In reviewing the application modification process, we noted that Statewide Application Systems uses manual procedures to ensure that the correct version of software is being modified. Industry "best practice" standards recommend that version control software be used to maintain software libraries. Version control software helps to ensure that modifications are made to the correct version of software code and can expedite the return of the software to its pre-implementation stage should a modification cause unforeseen problems.

Recommendation 8

We recommend Statewide Application Systems consider the use of version control software to enhance the efficiency and management of implementing application changes to the production environment. Version control software can expedite the return of the application to its post-modification status if necessary.

Response

Agree.

Tool evaluation will be included in the deployment of the new methodology. To the extent possible, we will leverage the existing tools available for the mainframe environment. However, the open systems environment will likely require an investment. Therefore, we will do a cost/benefit analysis to determine the feasibility of purchasing a tool vis-à-vis the risk associated with the existing manual processes.

Implementation Date

May 2003.

Implement a Security Awareness Training Program

We reviewed the Data Center's policies and procedures related to employee awareness of physical and logical security. We noted that current policies do not provide for ongoing training of employees in the area of security. As a result, employees may not be aware of current security risks and the associated policies designed to mitigate those risks. Increased emphasis on security is predominant throughout the industry, with leading organizations implementing continuing security awareness training as part of an overall security program. A security awareness program should include refresher training for all employees, as well as continuing technical training for security officials.

Recommendation 9

We recommend the Data Center implement a security awareness training program to supplement current security policies and procedures. In addition, we recommend all employees be required to sign an annual statement of compliance acknowledging Data Center computer security policies denoting completion of security awareness training.

Response

Agree.

DoIT Security Administration will conduct an annual security awareness-training program to ensure all employees are aware of current security policies and procedures. Each employee will be required to sign an affirmation that they received, understood and will comply with the policies presented in the training.

Implementation Date

October 1, 2002 – Course curriculum completed; Second week of January 2002 – First class.

Create Employee Training and Development Plans

We reviewed the Data Center's policies and procedures related to employee training and development. We noted that while current procedures require the approval and tracking of individual employee training, they do not provide a strategic approach to training and development to ensure that employees receive training that meets the needs of the organization. As such, annual training is not currently provided for all employees, nor is training reviewed as a whole to ensure that planned training is aligned with the strategic direction of the organization

Recommendation 10

We recommend the Data Center create employee training and development plans. Once developed, training plans for a functional department or unit should be reviewed as a whole to ensure that planned training helps to develop needed skills across the department and organization.

Response

Agree.

DoIT Strategic Planning effort has identified this as a target action again for FY03. FY02 processes included preparation of training plans by each manager.

Implementation Date

July 30, 2003.

SECTION V COLORADO DEPARTMENT OF PERSONNEL AND ADMINISTRATION DIVISION OF INFORMATION TECHNOLOGIES DATA CENTER AND STATEWIDE APPLICATION SYSTEMS' DESCRIPTION OF CONTROLS

Prepared by the Data Center and Statewide Application Systems

OVERVIEW OF OPERATIONS

Data Center

The Division of Information Technologies Data Center (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 23 years.

The most recent significant organizational changes were made to further unify the division; to better reflect the working relationships within the division; and to reduce perceived span of control and conflict of interest weaknesses in the change management and security administration practices. Specifically, the Pueblo Data Entry Center was aligned with the Statewide Application Systems and the Archives/Information Systems/Web Page to support E-commerce initiatives; Data Network technical services staff and the Data Center technical and operational staffs were combined into a Technical Design and Infrastructure section to recognize the close relationship between processing and networking of information; and an enhanced customer center was organized under a single manager in order to provide help desk, scheduling, security, and problem/change management for all Data Center and network services.

Services performed for State agencies include computer processing, maintaining system software, processing of computer output, statewide telecommunications network, 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 predominantly 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. This resulted when the Data Center installed and made available high-level programming software packages which are more adaptable and easier for non-data processing personnel to use.

The change to real-time processing has also brought about a change in the type 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 pull resources from the Data Center on an as-needed basis to provide application programming support, PC help desk support, training, and new technology expertise. Customers also are utilizing the secure and highly available physical infrastructure of the Data Center for their departmentally managed mid-range server platforms.

Statewide Application Systems

Statewide Application Systems is responsible for acquiring, implementing, operating and maintaining statewide information systems for the State of Colorado. The Colorado Financial Reporting System (COFRS) is the accounting system of final record used by the State of Colorado. All State agencies except higher education institutions use COFRS directly to perform their day-to-day accounting functions. Higher education institutions utilize their own accounting systems, but pass along summarized accounting information to COFRS through interface programs.

The CORE software, which forms the basis of COFRS, was originally developed by American Management Systems, Inc. Statewide Application Systems now owns the program source code for the CORE software and makes all modifications and enhancements to this and related programs, including COFRS.

GENERAL COMPUTER CONTROLS

Organization and Management

State Personnel Rules and Procedures are followed in all areas concerning the hiring, promotion, leave administration, annual performance management and termination of Data Center and Statewide Application Services employees. Additionally, department and division orientation sessions are made available to all new employees. Employees are informed of their respective responsibilities and duties through distribution of the organization chart and job descriptions when changes are made. General project, organization, service levels and service delivery information is shared with employees through regularly scheduled staff meetings.

The management team meets weekly to ensure the consistency of direction and objectives and to address system performance issues. Consistency and control is further addressed through the publication, maintenance and use of Standard Operating Procedures. General performance and service level indicators are captured and reported to customers and Data Center management through automated continuous data capture and reporting.

Controls are further exercised through the defined division of responsibilities; computer operators are prohibited from accessing programs and data, application programmers do not have access to the production environment and security administration is performed by an organizational work unit that reports neither to the Technical Support nor the Operations Manager. Further, computer operators, data control staff and schedulers do not perform each other's duties unless it is required due to staff vacancies and is achieved through temporary assignment. Application-specific controls are maintained by the customer agency and are not part of the Data Center's control environment.

System Software Support

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. A test LPAR residency (disk space partitioned and independent of the operating platform) is provided for testing. There is a formal installation process for production software, an implementation schedule published to the customers and affected clients are notified via E-mail, 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.

Access to system software is restricted to authorized system programmers at the Data Center and is controlled through the use of Top Secret security software. System programs that allow bypassing of normal systems or application controls (e.g., Super Zap) are also protected by Top Secret security and are used only when necessary. Such usage is reflected in security logs for review and event-documentation.

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, 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.

Application Development and Modification

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

Statewide Application Systems maintains the Client Support Group (CSG) as the starting point for processing problem reports and change requests. CSG receives problem reports from the System Administration staff and also from users via the COFRS Helpline. Change requests may be submitted by staff at user agencies, and also are generated internally within Application Services. Some changes are mandated by legislative action, while others are required by upgrades in Data Center system software (e.g., MVS or CICS). CSG staff verify the existence of a problem or need for the change request, write functional specifications for the proposed modification, and conduct internal and external meetings to elicit comments on the proposed changes. CSG staff maintain contact with COFRS users through personal contact, the Extended Purchasing Subsystem user group, the Inventory user group, the Controller's Forum, the Colorado Financial Management Association, and liaison with State Controller's Office staff.

Within Statewide Application Systems, a group of experienced staff, the Design Review Team (DRT) reviews and approves most change requests. Changes with heavy user impact are also cleared through an appropriate user group. In most cases, DRT sign-off on change requests is required before programming commences. Problem reports are reviewed by CSG. If the problem report has several possible fixes or major system implications, these are reviewed and approved by DRT or a subset of DRT members prior to being turned over to the Technical Services Group (TSG) for implementation.

Beyond a functional specification, TSG 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. This design document must be reviewed and signed off by the TSG manager or his designee prior to actual programming. TSG performs unit testing of each program modification, and the results of this testing are reviewed. Most fixes are supplemented by further testing by the Acceptance Testing Staff. Testing includes any data conversions or data recovery required to implement the new or changed software.

Customer communication regarding application changes takes the form of release letters, documentation, and training. Changes impacting users are communicated to COFRS users in advance via release letters E-mailed to clients. If the problem report was submitted by a user, he or she is contacted directly by COFRS Helpline 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 CSG staff prior to turning the modified software over to the COFRS System Administration (SYAD) 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 DRT 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 subsequently archived. Access to the documentation is made through an online problem/change tracking system. Additionally, SYAD maintains special internal documentation for the CA7 schedules and parameter tables used to administer COFRS.

Computer Operations

Computer Associates scheduling software (CA7) is used to schedule the processing of batch jobs. Top Secret is used to restrict access to CA7 to only appropriately authorized personnel. Access to scheduling files is restricted to Data Center scheduling personnel; agencies have access to the scheduling software to schedule jobs for their agency only. Computer operators are restricted from discretionary use of the computer system as personnel from the Service Center (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). Exceptions to normal operations are reported by schedulers and are published for management review on a Daily Activity History Report. Continual problems are identified and discussed in weekly management meetings.

The automated scheduling system ensures that batch jobs are run on a predetermined schedule and are tracked automatically. Where jobs are irregularly scheduled, schedulers check off jobs as they are completed. Batch jobs that do not run correctly are automatically entered into the system log and are entered into the Problem Management system (INFOSYS). INFOSYS helps to ensure that problems are recorded and tracked to appropriate resolution.

All data, programs and documentation necessary to restore system and data files are stored off-site at Iron Mountain. Specifics of the data retention program include: critical disk packs are duplicated weekly, system data sets and catalogs are duplicated to tape daily, source program libraries are duplicated daily and databases for which DoIT staff function as the Database Administrator (DBA) are backed up to tape each weekday and once during the weekend. The off-site data is physically secured and is accessible only to authorized personnel.

Capacity and performance of Data Center computer resources are actively tracked and recorded through the ongoing, real-time usage of the 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. Capacity and performance metrics are reviewed regularly by management. Certain information is put in graphical and other more readable format, and is made available to requesting customer agencies.

Physical Security

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 cipher lock and are used by employees only. Visitors must check in with reception to pass through the staging areas and complete the roster with their name, time in and who they are seeing. Visitors must be escorted at all times unless granted specific permission for unsupervised admission. Visitors are assigned badges and must wear them 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 computing facility is comprised of three areas: Print/Copy Room, Computer Room and the Telecommunications Room. A unique-combination cipher lock secures each area. Visitors can enter the computing facility only through 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.

Cipher lock combinations are changed when an employee terminates. Additional changes are made at management's discretion. A distribution list is used to inform employees of new combinations. Employees must sign the distribution list indicating they received the new combinations. Employees receive new cipher combinations for only those areas to which they are authorized.

Data files, negotiable warrants and authorizing signature images are physically secured as governed by documented procedures. These procedures address the acceptance and transfer of materials (data products or common deliveries) in and out of the Data Center, the software-managed migration of storage between the Data Center and Iron Mountain, and the proper handling and tracking of all negotiable documents, and the loading and unloading of authorizing signatures.

The Data Center has an uninterruptible power supply (UPS) system to support the Data Center's raised floor equipment. The UPS has a generator alternate power source that is connected and operational on the Data Center's power grid. The technical support and administration area is provided with power outlets (for desktop computers) that are connected to the UPS/Generator backup power supply. 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 Capital Complex Facilities is the custodian for the Data Center building at 690 Kipling Street, Lakewood, CO. 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. During business hours certain Data Center personnel also have responsibility to call the fire department as a secondary notification.

Logical Security

Mainframe

The System Security and Use Standard Operating Procedure (SOP) 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 and Statewide Application Systems 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 Help Desk 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 E-mail from the user's supervisor to the Help Desk explaining the reason for the permission change. A checklist for departing employees is utilized by the administrative staff to ensure deletion of ACIDs for departing employees. A checklist for New/Promoted/Transferred employees is utilized by the administrative staff to ensure assignment of proper ACID profiles for the various systems.

Top Secret security software is used to control access to all mainframe software and data sets. Permissions are defined by ACID and controlled through log-in 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 log-in attempts. Passwords are not displayed as they are input and are encrypted as they are stored.

Top Secret will disable the account if it is not used within six months and will automatically disconnect a log-in session if no activity occurs within a defined period. The Help Desk 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.

Network

Distributed computing logical control is similarly approached for the network. Windows NT is administered by the Operating Systems Support group (OSS) and agency administrators. Each person is given a user ID and temporary password. Additional access requires justification via an E-mail 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).

Network security controls are configured to enforce certain password criteria including minimum length and account suspension after a defined number of failed log-in attempts. In addition, Windows NT generates logs of certain events and the OSS group reviews these logs on a monthly basis including, Logon/Logoff failures, File and Object Access failures. Security Policy Changes and Restart, Shutdown and System Success/Failures

COFRS APPLICATION PROCESSING

Input Controls

Transactions can be input into COFRS by two means, (a) through online use of COFRS or (b) through submission of interface files of transaction data. Agencies are responsible for developing internal policies and procedures to ensure timely input of both online and interface transactions into COFRS and to authorize such input. COFRS itself provides the following features to assist agencies in these activities.

- COFRS provides a message screen (GMSS) displaying the scheduled days and times when COFRS will be available for online use. Scheduled downtimes are publicized well in advance.
- Interface files can be submitted to COFRS at any time. Interfaces received prior to the time when the system is taken down for nightly processing are processed that night. The usual daily deadlines for interfaces are published in COFRS documentation. Any changes in these deadlines are published on the GMSS screen.
- All transactions entered in COFRS are listed on the SUSF table. For online entry, the ID of the user who last entered or modified the transaction is displayed on that table, and the user's terminal ID is displayed on the SUS2 table, an alternate view of the SUSF table. (NOTE: The user ID of interface transactions is recorded as "OFF-LINE").
- The State Controller's Office security procedures require the appointment of a single Agency Security Administrator at each agency to administer mainframe access through Top Secret. The agency must notify the State Controller's Office when any change in the Agency Security Administrator occurs. Periodically, Application Services and the State Controller's Office offer training to new Agency Security Administrators.

- The Agency Security Administrator has update rights on the COFRS ASEC table, the main security table for COFRS, for users in that agency only. The Security Administrator can add and delete users in the table, and grant or revoke their rights to input transactions into COFRS. Transaction entry rights may be restricted to specific types of transactions, if the Security Administrator desires.
- The COFRS Security Administrator is responsible for maintenance of security for critical COFRS tables, and also for monitoring of the general application of security by the Agency Security Administrators. Currently, eight or nine security monitoring reports are used to assist in this function.
- Advance authorization for entry of interface transactions by agencies is obtained from the State Controller's Office. The COFRS System Administrator is then responsible for setting up the COFRS interface control table and related JCL. The JCL validates that the control files are genuine and receives them into COFRS.
- The IFST table in COFRS maintains statistics on the number of transactions received in each agency interface file, including the starting and ending transaction numbers, transaction counts and interface receipt date. Agencies have access to this table and to the IRC01R report which provides further details, to monitor that the interfaces were received on a timely basis and were properly authorized.

COFRS includes batch balancing as a data entry feature. When transactions are entered in batch, the transaction count and total amount from the batch tally or proof sheet must also be entered. COFRS calculates the transaction count and total amount of the batch, and compares it with the proof. It rejects the batch if there is any discrepancy.

The CORE supervisory routines require that all transactions be edited and approved prior to acceptance in COFRS. Editing requirements vary by transaction type, and are specified in the transaction processing software that agency users run through the online "Quick Edit" function. Any errors detected during the edit procedure must be either corrected or overridden prior to approval of the transaction.

Minimum approval requirements are set by the State Controller's Office, although agencies may impose more stringent approval requirements via a COFRS table. Most approvals are performed at the agency level; however, certain transactions require approval by the State Controller's Office.

Errors detected in editing must be corrected online, regardless of how the transaction entered COFRS. To assist users in clearing errors, all error messages specify an error code that can be looked up in the online error documentation. Application Services also supports a Helpline to answer user questions. If errors cannot be cleared from a transaction, the transaction cannot be processed further. In these cases, the transaction may be held in suspense (for up to six months) or deleted by the user.

Once a transaction has been accepted by COFRS, the ledger record it creates cannot be deleted or modified online. This provision creates an audit trail for all financial transactions in the State. In the rare case that a transaction is clearly erroneous and prevents balancing of the ledgers, Application Services staff will manually modify the ledger record in accordance with the standard COFRS Data Modification procedure. This procedure requires maintenance of a manual log detailing all such changes. All changes to the ledgers are authorized in writing by a representative of the State Controllers Office.

To correct minor errors discovered after a transaction has been accepted, COFRS provides a "Modify" transaction. In general, a modify transaction permits the user to reverse the accounting effect of the erroneous accepted transaction. A modify transaction is a new transaction added to the ledgers which in no way affects the ledger record of the original erroneous transaction. The new transaction is subject to the same edit and approval requirements as the original transaction.

The SUSF table displays the current status of all transactions for five days after they are accepted. Unaccepted transactions are held on the table for six months and then purged. Users can easily scan for transactions with specific statuses (waiting for approval, on hold, or failed edits) through a filtering feature of this table.

Two reports are available to assist agencies in following up on transactions: GNL15R displays the status of all transactions on SUSF, and GNL25R lists all transactions that are will be purged when the six-month purge process is next run.

Software features to prevent duplicate transaction processing are built into CORE. Users may not enter two transactions with the same transaction ID. The transaction status is checked before a transaction is processed, and accepted transactions will not be re-processed. If the transaction clears a prior item, e.g., a voucher clearing a purchase order, COFRS will check that the prior item has not been previously cleared by some other transaction.

Processing Controls

Although many transactions are processed online, the bulk of COFRS transaction processing occurs in the Nightly Cycle. All critical programs in this cycle issue termination codes identifying whether any errors were detected by the program. Condition code checking in the JCL and CA7 prevents further processing after serious errors have occurred. COFRS on-call staff is then contacted by the Data Center for instructions on how to proceed. Five backups of tables and ledgers are performed at various points during the nightly processing cycle, enabling complete system recovery in the event of a program abend with potential data corruption.

Following the nightly cycle, a number of system assurance reports are generated. These reports compare balances in tables, ledgers and even in other reports to ensure that system integrity has been maintained. These reports plus the program termination codes are reviewed each morning by System Administration staff. Out-of-balance conditions and error codes are followed up on immediately. Agencies may use the GNL01R report to verify the correct processing of each transaction. This report displays details about each accepted transaction, and can be compared to the original transaction entry.

Output Controls

COFRS output takes several forms, including printed reports, displayed reports, reports saved to files, ledger extracts, table extracts, warrants, and EFTs.

Reports – Application Services relies on the INFOPAC software (licensed from Mobius) for support of report output. For printed reports, INFOPAC batches reports by user ID, creates header sheets between batches, and issues printing commands to the high-speed computer center printers. INFOPAC can be customized to send reports to remote printers, if agencies choose to perform printing at their local sites. Another customization option allows reports to be printed to disk files. INFOPAC also supplies a mainframe user interface allowing users to select and view reports. User identification and agency security are built into this interface.

Warrants – The warrant printing process is partially manual and partially automated. The State Controller's Office and Data Center have developed a procedure to safeguard the purchase and storage of warrant stock. The Data Center maintains a record of each warrant number printed, and before printing a new batch of warrants, asks the computer center operator to visually verify the starting warrant number. Ruined warrants are tracked, and the printed warrants are delivered to the State Controller's Office for review prior to mailing.

EFTs – EFT information is formatted according to bank specifications and transmitted to the bank via a private network during nightly processing. Reports of the EFT's are created for the state controller. The bank faxes an acknowledgment of receipt of the transmission to the controller's office.

Extracts – Table and ledger extracts are prepared by COFRS programs each night, and stored on the Data Center mainframe. Agencies are responsible for importing, storing or otherwise disposing of extract files before they are overwritten by the next set of extracts.

Where COFRS output is passed to the end user without manual intervention by the Data Center, end users are expected to assume responsibility for monitoring the accuracy and completeness of output. Any errors in this regard can be reported to the COFRS Helpline for correction.

Access to COFRS screens requires view rights, which are granted or revoked by the Agency Security Administrators discussed earlier. INFOPAC access requires user IDs and agency codes. Access is established by COFRS Helpline, based on requests submitted by COFRS Report Coordinators in each agency.

SECTION VI INFORMATION PROVIDED BY SERVICE AUDITOR

CONTROL ENVIRONMENT ELEMENTS

An organization's control environment consist of computer systems, processes, personnel and manual and systematic control procedures. This report addresses aspects of the Data Center and Statewide Application Systems' control environment, which may be relevant to user organizations.

The control environment represents the collective effect of various factors on establishing, enhancing or mitigating the effectiveness of controls. In addition to the tests of operating effectiveness described below, our procedures included tests of the following relevant elements of the Data Center and Statewide Application Systems' control environment:

- Organizational structure and management.
- Systems software support.
- Application development and modification.
- Protection of physical assets.
- Logical access to systems and data.
- Application processing controls (including input and output).

Such tests included inquiry of appropriate management, supervisory and staff personnel; inspection of documents and records; and observation of activities and operations. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control objectives described below.

CONTROL OBJECTIVES, DESCRIPTION OF CONTROLS, TESTS OF OPERATING EFFECTIVENESS, AND RESULTS OF TESTS

The following tests were designed to obtain evidence related to the effectiveness of specific controls in meeting the stated objectives.

GENERAL COMPUTER CONTROLS

Organization and Management

Control Objective 1

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.

Summary of Key Controls

- State Personnel Rules and Procedures are followed in all hiring, training, performance evaluation, job responsibilities, vacation and termination practices.
- New employees attend departmental and divisional orientation sessions.
- Employees must sign a Statement of Compliance indicating they have received and agree to the computer usage and data security policy.
- Vacation usage is tracked, balances posted and "Use or Lose" balances are distributed to employees and managers.
- Formal job descriptions exist and are kept current.

- A performance appraisal system is in place. Semiannual reviews are required and annual ratings are performed in July.
- An organization chart is published and kept current.
- Standard Operating Procedure (SOP) manuals exist and are used by Data Center and Statewide Application Systems personnel.
- Employees are trained in accordance with job responsibilities.
- 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.
- A checklist is used for all departing employees to ensure that separation/termination activities are conducted according to policy.

Tests of Operating Effectiveness and Results of Tests

- Inquired of the Data Center Human Resource Manager and determined that State Personnel Rules and Procedures were followed in Data Center hiring and termination practices and all employees attend a department and divisional orientation session.
- Reviewed appraisal system metrics and associated documentation to gain an understanding of the appraisal system process.
- Reviewed the organization chart and determined it was accurate.
- Selected a sample of employees and performed the following:
  - Obtained the employee personnel file and:
    - ? Inspected the new hire checklist indicating they had received a copy of the SOP, with the exception of one employee personnel file which did not contain a completed new hire checklist.
    - ? Inspected a current semiannual performance review form and determined the review was in compliance with policy.
    - ? Verified that the employee vacation balance was tracked and properly recorded.
    - ? Inspected training certificates. Compared the certificates against the employee's job skill title and determined that training courses were appropriate for employee's job responsibilities.
  - Reviewed the employee's associated position job description, verified the date posted/modified and determined the job description was accurate.
- Attended a Data Center staff meeting and determined that relevant changes to the organization were presented.
- Inspected sample of termination packets for recently terminated employees and determined that the departing employee checklist was completed.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 2

Controls provide reasonable assurance that segregation of duties exists among the personnel responsible for application development, computer operations and security administration.

Summary of Controls

- Computer operators are prohibited from making changes to production systems and data.
- Application programmers are not permitted access to production systems and data.
- Access to security administration functions is appropriately limited to authorized individuals.

Tests of Operating Effectiveness and Results of Tests

- Reviewed a sample of Top Secret security profiles for operators and determined that they were appropriately restricted from modifying production programs and changing input data.
- Reviewed a sample of Top Secret security profiles for four application programmers and determined that they were not permitted access to production systems and data, with the exception of one programmer who functions as a security administrator for Statewide Application Systems, and thus had unrestricted access to production systems and data.
- Reviewed all (23) ACIDs with Data Center Top Secret with security administration privileges and determined that access was not appropriately limited to authorized personnel. Six Data Center employees had varying levels of security administration access that was not appropriate or commensurate with their job responsibilities.

Conclusion

Based on the tests of operating effectiveness described above, controls were not operating with sufficient effectiveness to achieve this control objective.

System Software Support

Control Objective 3

Controls provide reasonable assurance that modifications to systems software are appropriate and properly authorized, tested, approved, implemented and documented.

Summary of Controls

- A formal change management system is used to control and document changes to system software.
- Prior to work beginning, system software modifications are authorized by appropriate personnel.
- Systems software modifications and additions are thoroughly tested and approved before introduction into the production environment.
- 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.
- An implementation schedule is published and available to clients.
- Affected clients are notified via E-mail, telephone, or broadcast message prior to placing a modification into production.
- Prior to implementation, management assesses the impact of systems software modifications to client processing.

- Back-out procedures are written to return the system's configuration back to its pre-implementation condition.
- Documentation for system software products is available and current.
- The installation process for system software includes a review/update of associated documentation.
- The inventory of systems is updated for system software modifications.

Tests of Operating Effectiveness and Results of Tests

- Reviewed SOP #8803, Data Center policy and procedures for system software change management, and determined that policies included guidance on the initiation, authorization testing, approval, implementation and documentation of system software changes.
- Observed that a formal change management system (INFOSYS) was used to outline, track and document changes to system software.
- Inspected documentation for a sample of six system software changes during the period and determined that:
  - The system software modification was properly authorized prior to work beginning.
  - Testing took place and approval was obtained prior to moving the change into production, except that evidence of testing was not documented for one system software change. However, based on inquiry and other documentation of the change, it appears the change was tested but was not appropriately documented according to the formal system software implementation methodology.
  - Various factors (impacts) relative to client processing were considered throughout the change process.
  - Back-out procedures were established to return the system's configuration back to its pre-implementation condition.
  - The inventory of system software was appropriately updated, with the exception of one system software change that was not updated in the inventory listing.
- Observed that a dedicated test partition is resident and used as an isolated platform for testing software modifications.
- Reviewed the software implementation schedule and determined that system software modifications were published and the schedule was available to users.
- Inquired of Data Center staff and determined that clients were notified via E-mail, telephone, or broadcast message prior to placing a changes into production.
- Observed that Technical Support Staff have access to current system software documentation instructions on CD-ROM.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 4

Controls provide reasonable assurance that access to system software is restricted to authorized personnel.

Summary of Controls

- Top Secret is used to restrict access to system software to appropriate individuals.

- Top Secret is used to restrict access to those system programs which allow bypassing of normal system or application controls (e.g., Super Zap).

Tests of Operating Effectiveness and Results of Tests

- Reviewed a sample of 20 Data Center employee ACIDs and determined that only authorized individuals have access to system software, with the exception of two employees who had access to system software data sets and did not require this access to perform their job functions.
- Reviewed all (19) ACIDs with access to Super Zap and determined that access was appropriately limited to authorized individuals with the exception of one individual, the Data Center Security Administrator, who did not require this access to perform his job function.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 5

Controls provide reasonable assurance that the acquisition of new utilities software is appropriate.

Summary of Controls

- Documented procedures have been developed and are followed in the requisition, bidding and purchase of new utilities software.
- Appropriate justification and management approval is required before the acquisition of new utilities software.

Tests of Operating Effectiveness and Results of Tests

- Reviewed the policies and procedures related to software requisition and determined that policies include guidance on the bid process, vendor selection and execution of purchase orders.
- Inquired of Data Center purchasing personnel and determined that policies are followed in the requisition, bidding and purchase of new utilities software. A sample of purchases could not be tested for compliance with policies, as there were no purchases of utilities software during the period covered in our report.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Application Development and Modification

Control Objective 6

Controls provide reasonable assurance that modifications to application software are appropriate and properly authorized, tested, approved, implemented and documented.

Summary of Controls

- A formal application change management methodology is used to control and document changes to application software.

- Client Support Group (CSG) staff identifies, analyzes and evaluates the functional specifications and user requirements by conducting internal and external meetings to elicit comments on the proposed changes.
- Members of the Design Review Team (DRT) approve modifications prior to the Technical Services Group (TSG) taking action to modify the source code.
- TSG performs the programming phase, which uses the detailed design developed to code the software and document the updates within a test environment. Upon successful completion of the system tests by TSG, formal acceptance is granted.
- A review of functionality, unit testing and acceptance testing is performed by CSG staff prior to turning the modified software over to the COFRS System Administration group for operational implementation.
- Manual controls are used to ensure the correct version of software is being modified. Controls include:
  - Separate development, test and production libraries.
  - The source code is copied directly from production and used to make modifications.
  - The modified source code is then moved, not copied, from development to test and then to production.
- Complete application documentation and user manuals are maintained and updated, as appropriate, to reflect modifications made to the application.
- Clients are notified of changes to the application if the changes will impact their interaction with the application.

Tests of Operating Effectiveness and Results of Tests

- Reviewed the Change/Problem Life Cycle document, Statewide Application Systems policy and procedures for application software change management, and determined that policies included guidance on the initiation, authorization, testing, approval, implementation and documentation of application software changes.
- Inquired of system programmers and determined that manual version control procedure were used and include separate development, test and production libraries, the source code was copied directly from production and used to make modifications, and the modified source code was then moved from development to test and then to production.
- Inspected documentation for a sample of six application software changes during the period and determined that:
  - Specifications and user requirements were documented for consideration.
  - The change was properly authorized prior to commencing work on the project.
  - Functionality unit and acceptance tests were performed and testing results approved prior to moving change into production, except that evidence of testing was not documented for one application software change. However, based on inquiry of COFRS development personnel and other documentation of the change, it appears that the change was tested but the testing was not appropriately documented in accordance with the formal application change management methodology.
  - Application documentation was maintained and updated.
  - Clients were notified regarding application changes.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 7

Controls provide reasonable assurance that Data Center staff use the computer only for authorized purposes and operators follow prescribed procedures.

Summary of Controls

- Top Secret is used to restrict access to scheduling software (CA7) to appropriate personnel.
- Automated operation of scheduling software minimizes the actions required from an operator in processing an activity/job.
- Operator activities are recorded on the console log.
- Exceptions to normal operations are reported by schedulers and published for management review on a Daily Activity History Report.

Tests of Operating Effectiveness and Results of Tests

- Observed that scheduling software (CA7) was used.
- Reviewed all (43) Data Center ACIDs with access to the scheduling software and determined that access is limited to appropriate personnel with the exception of three employees who had access to CA7 but do not need the access to perform their job functions.
- Observed service center personnel monitoring operations.
- Reviewed the console log and determined that operators' activities were being recorded.
- Reviewed the Daily Activity History Report and determined that the information in the report was timely and accurately depicted the status of operations.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 8

Controls provide reasonable assurance that scheduled processing is monitored appropriately and deviations from scheduled processing are identified and monitored.

Summary of Controls

- Batch jobs are run on a pre-determined schedule and tracked automatically.
- Routine jobs that are processed outside of their normal schedule are checked-off by schedulers as they are completed.
- Scheduling deviations are reported by schedulers and published for management review on a Daily Activity History Report.

Tests of Operating Effectiveness and Results of Tests

- Reviewed the schedule and auto-tracking system and determined that tracking was performed.
- Reviewed a sample of irregularly scheduled jobs and determined that schedulers checked-off on jobs upon completion.

- Reviewed a sample of Daily Activity History Reports and determined that deviations from scheduled programming were noted.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 9

Controls provide reasonable assurance that processing problems are identified, tracked and resolved in a timely manner.

Summary of Controls

- A problem management system (INFOSYS) is used to record, track and resolve identified problems.
- 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.
- Problems identified are immediately entered into INFOSYS, defining the problem and corrective procedures undertaken.
- Exceptions to normal operations are reported by schedulers and are published for management review on the Daily Activity History Report.

Tests of Operating Effectiveness and Results of Tests and Result of Testing

- Reviewed INFOSYS records and determined that the problems, affected systems, and the corrective procedures undertaken were adequately documented.
- Reviewed control processing procedures and determined that adequate guidance was available to address processing problems.
- Reviewed a sample of Daily Activity History Reports and determined that processing problems were published for management review.
- Reviewed supporting documentation for a sample of problems recorded in INFOSYS and determined that problems were actively tracked and resolved in a timely manner.
- Reviewed open items in INFOSYS as of a specific date and determined that all open items were less than three months old with the exception of one item that was approximately six months old. We reviewed the activity on the older item and noted that problem had been actively tracked and progress had been made towards resolution.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 10

Controls provide reasonable assurance that all necessary system software and Data Center-managed database files are adequately backed up and stored off-site.

Summary of Controls

- The following are backed up on the schedule indicated:
  - Critical disk packs are duplicated weekly.
  - System data sets and catalogs are duplicated to tape daily.
  - Source program libraries are duplicated daily.
  - Databases for which Data Center staff function as the Database Administrator (DBA) are backed up to tape each weekday and once during the weekend.
- All back-up media is stored off-site at Iron Mountain.
- The Iron Mountain facility is physically secure and access is restricted to authorized personnel.

Tests of Operating Effectiveness and Results of Tests

- Reviewed a sample of back-up reports (105 Reports) and determined that disk packs, system data sets, catalogs and source program libraries are duplicated consistent with Data Center policy.
- Reviewed the list of databases for which the Data Center functions as DBA, reviewed a sample of the associated 105 Reports and determined that back-up of database files was consistent with Data Center policy.
- Toured the Iron Mountain facility, reviewed the facilities' access policy and procedures and determined that only authorized personnel were allowed access and all personnel must log-in and out of the facility.
- Reviewed the Iron Mountain access roster and compared it to the storage facility authorization letter and determined that only authorized individuals were permitted access to Iron Mountain.
- Selected a sample of items from the 105 Report indicated as stored at Iron Mountain, agreed item to the Iron Mountain inventory report and physically inspected the back-up media and determined items were located as denoted on the inventory report.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 11

Controls provide reasonable assurance that mechanisms are in place for the capture and monitoring of capacity and performance.

Summary of Controls

- System Management Facility (SMF) recording is active and recording options are appropriate to capture and monitor capacity and performance.
- Data Center personnel review SMF information on a regular basis.
- SMF data capture is retained and presented in graphical format for management review.
- 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.

Tests of Operating Effectiveness and Results of Tests

- Inquired of the resource manager and reviewed data recorded by SMF and determined that the appropriate information was captured to monitor processing quality and efficiency and that SMF data was reviewed on a regular basis.
- Obtained SMF data and graphical depictions of performance and capacity information and determined data was retained and distributed to management.
- Inquired of the Network Support Manager and Service Center personnel and determined that the NetMan server was used to monitor availability and that Event Viewer was used to troubleshoot problems.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Physical Security

Control Objective 12

Controls provide reasonable assurance that physical access to computer resources is restricted to authorized personnel.

Summary of Controls

- 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 cipher lock and are for use by employees only.
- Employees and visitors must wear badges.
- Visitors must check in with reception to pass through the staging areas and complete a roster with their name, time in and who they are seeing. Visitors must be escorted at all times unless granted specific permission in person. Visitors are assigned badges and must wear them while in the building. Badges must be turned in before leaving the building and visitor time-out is recorded on the roster.
- The Data Center computing facility is comprised of three areas (Print/Copy Room, Telecommunications Room and the Computer Room). A unique-combination cipher lock secures each area.
- The Data Center has 24/7 operations and someone is on-site at all times and would note and investigate any unfamiliar or unusual activity.
- Visitors can enter the computing facility only through 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.
- Cipher lock combinations are changed when an employee terminates. Additional changes are made at management's discretion.
- A distribution list is used to inform employees of new combinations changes. Employees must sign the distribution list indicating they received the new combinations. Employees receive new cipher combinations for only those areas to which they are authorized.
- There are standard procedures for accepting and transferring materials (data products or common deliveries) in and out of the Data Center.

Tests of Operating Effectiveness and Results of Tests

- Observed the building's main entrance and determined that visitors were required to sign-in and out on a roster before gaining permission from the receptionist to enter. In addition, the receptionist called the person responsible for the visitor who escorted them from the reception area.
- Observed employees entering building and determined that cipher lock combination was required for entrance.
- Reviewed the building main entrance reception log and computing facility access logs and determined that they were used consistently and included adequate information to denote person's name, time in/out and who they were visiting.
- Inquired of Data Center management and determined visitors must be escorted unless they have been specifically cleared for unsupervised admissions.
- Inquired of Data Center shift supervisors and determined that only shift supervisors can grant visitor access to the computing facility and that a shift supervisor is on-site 24/7.
- Toured the computing facility and observed that a unique-combination cipher lock secures each area.
- Reviewed signed distribution lists for cipher lock changes and determined that lock combinations were changed during the period.
- Inquired of Data Center personnel, including the receptionist, and determined there were standard procedures for accepting and transferring materials in and out of the Data Center.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 13

Controls provide reasonable assurance that devices are installed to monitor and protect the Data Center computing resources from damage.

Summary of Controls

- The computing facility is equipped with smoke detectors located above and below the raised flooring and are directly linked to the fire suppression system.
- The computing facility is equipped with a halon gas fire suppression system.
- The halon 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.
- Climatic controls are installed in the Data Center.
- The Data Center has an uninterruptible power supply (UPS) system with a generator-powered alternate power source which is connected and operational on the Data Center's power grid.
- Central monitoring of the building fire alarms is provided by the State Patrol headquarters who will notify the fire department if an alarm is activated.
- The second floor is provided with power outlets (for the personal computers) that are connected to the UPS/generator backup power supply.

Tests of Operating Effectiveness and Results of Tests

- Performed a walkthrough of the Data Center and observed the following: smoke detectors, fire suppression system, temperature and humidity controls, water detection, UPS, raised flooring and additional outlets specially marked and connected to the UPS.
- Reviewed documentation for recent fire inspections and determined that the facilities passed inspections in accordance to state inspections criteria.
- Reviewed current halon inspection documentation and determined that the inspections were performed in accordance with Data Center policy.
- Inquired of Data Center management and determined that monitoring of building fire alarms was performed by the State Patrol.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Logical Security

Control Objective 14

Controls provide reasonable assurance that security policies provide for overall direction and implementation of security and that policies are effectively communicated and monitored.

Summary of Controls

- The System Security and Use Standard Operating Procedure (SOP) #8808 provides clear guidance regarding the responsibilities of Top Secret security administrators and the issuance of access permissions.
- 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 listed 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 responsibilities relative to Top Secret Security Administration.

Tests of Operating Effectiveness and Results of Tests

- Reviewed the SOP #8808 and determined that the SOP was last updated in March 2002 and contains guidance for security administration.
- Reviewed the Statement of Compliance form and determined that it accurately references security and network policies.
- Selected a sample of 25 Data Center employees and inspected the Help Desk files and determined that employees had signed a Statement of Compliance acknowledging their understanding and adherence to policy with the exception of two employees who did not have a signed form on file. We noted that both were long-term employees who had been through several organizational changes; Data Center management indicated the original Statements of Compliance were likely misplaced given the circumstances.
- Inquired of Human Resources personnel and determined that new employees receive a copy of the SOPs governing their expected behavior, rights, and privileges.

- Selected a sample of five Security Administrators and inspected the Help Desk files and determined that Security Administrators had signed an additional statement of compliance acknowledging their responsibilities relative to Top Secret Security Administration.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 15

Controls provide reasonable assurance that logical access to applications, programs, and data are restricted to authorized personnel.

Summary of Controls

Mainframe

- Top Secret is used to restrict access to the mainframe.
- Data Center Top Secret security administration privileges are limited to authorized personnel.
- Standard Operating Policies require that users be granted access to only those resources necessary and appropriate to user's job duties
- 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 title.
- 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).
- User ACIDs and passwords are assigned to individuals to provide accountability.
- Top Secret is configured to enforce password controls including minimum length, password expiration, minimum re-use of password generation and account suspension/lock-out after minimum failed log-in attempts.
- The Help Desk will unlock accounts only after verifying a user's identity using additional private information from INSTADATA.
- Future permission changes/enhancements require an E-mail or other written communication from the user's supervisor to the Help Desk explaining the reason for the permission change request.
- The system automatically disconnects a log-in session if inactive for 15 minutes.
- Top Secret is operating in fail mode, meaning that unauthorized attempts to access data sets are aborted.
- Top Secret logs security violations; logs are reviewed periodically and action is taken to investigate violations.
- Top Secret logs security profile changes; logs are reviewed periodically and unusual items are identified and investigated.
- The administrative staff utilizes a departing employee checklist to ensure that departing personnel's mainframe account is deleted in a timely manner.

Windows NT (Network)

- Windows NT is administered by the Operating Systems Support (OSS) group and agency NT security administrators. Only NT security administrators have the ability to create network accounts and grant access to the network.
- Each person is given a user ID and temporary password. The password must be changed on their first logon attempt or their account will be suspended (locked out).
- Control settings in Window NT enforce adequate account and password controls for the network.
- Windows NT generates logs of the following events and the OSS group reviews these logs on a monthly basis:
  - Logon/Logoff Failures
  - File and Object Access Failures
  - Security Policy Changes
  - Restart, Shutdown and System Success/Failures
- The administrative staff utilizes a departing employee checklist to ensure that departing personnel's network account is deleted in a timely manner.

Tests of Operating Effectiveness and Results of Tests

Mainframe

- Observed that Top Secret software was used to control access to the mainframe.
- Reviewed all (23) ACIDs with Data Center Top Secret security administration privileges and determined that access was not appropriately limited to authorized personnel. Six Data Center employees had varying levels of security administration access that was not appropriate or commensurate with their job responsibilities.
- KPMG obtained and reviewed the DoIT System Security and Use Standard Operating Procedure (SOP) #8808 and determined that it provided guidance for the Security Administrators on managing user access.
- Reviewed all (21) ACIDs with Data Center Top Secret Master Security Control Administration (MSCA) designation and determined that access permissions were not granted at the minimum required to accomplish their jobs. Of the 21 MSCA designates, 16 worked at the Help Desk and performed routine security administration functions. The MSCA designation allows full system access, and is not required for day-to-day security administration functions.
- Inquired of Help Desk personnel and determined that new users were granted initial access to the system based on their supervisor's direction and that initial access granted and minimum permission rights were based on their position title. However, the method by which access is granted was by replication of an existing user. Based on all of the tests performed related to logical access, this method did not consistently result in the grant of minimum permission rights, as many existing users have access that is inappropriate.
- Inquired of Help Desk personnel and determined that 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).
- Inquired of Help Desk personnel and determined that future permission changes/enhancements require an E-mail or other written communication from the user's supervisor to the Help Desk explaining the reason for the permission change request.

- Inquired of the Data Center Security Administrator and determined that he and his staff unlocked suspended accounts only after verifying the user's identity using additional private information from INSTADATA.
- Reviewed a sample of ACIDs and determined that not all ACIDs were assigned to individuals. We noted certain ACIDs assigned to group accounts.
- Reviewed Top Secret control settings and determined that configuration is set to enforce password controls including minimum length, defined password expiration, minimum re-use of password generation and account suspension/lock-out after minimum failed log-in attempts.
- Reviewed Top Secret control settings and determined that security was operating in "fail" mode and will thus abort any unauthorized access attempts.
- Observed that a nonactive session will be automatically logged off after a period of 15 minutes.
- Inspected Top Secret logs and determined that the logging was active and that logs contained appropriate information on security profile changes.
- Inquired of Security Administrator and determined that security profile change logs were not reviewed on a regular basis in order to identify and investigate unusual items.
- Observed Data Center personnel attempting to gain inappropriate access, thus creating access violations. Inspected the resultant Top Secret security violations logs and determined that the violations were appropriately recorded.
- Inquired of Security Administrator and reviewed security violation logs and determined that logs were reviewed on a regular basis and unusual items were identified and investigated.
- Inspected sample of termination packets for recently terminated employees and determined that the departing employee checklist was completed and indicated that mainframe and network access was deleted.

Windows NT (Network)

- Reviewed the listing of NT Administrators and determined that NT security administration privileges are limited to appropriate individuals.
- Inquired of the OSS group personnel and determined that new users are granted initial access to the network with a user ID and temporary password.
- Reviewed Windows NT control settings and determined settings enforced adequate account and password controls for the network, with the exception of password expiration and password generation history settings.
- Reviewed the Windows NT audit policy and determined the system was configured to log the following events:
  - Logon/Logoff Failures
  - File and Object Access Failures
  - Security Policy Changes
  - Restart, Shutdown and System Success/Failures
- Inspected a sample of logs from the NT domain and inquired of OSS personnel and determined that logs were reviewed on a monthly basis.

Conclusion

Based on the tests of operating effectiveness described above, controls were not operating with sufficient effectiveness to achieve this control objective.

COFRS APPLICATION CONTROLS

Input Controls

Control Objective 16

Controls provide reasonable assurance that all input transactions for the COFRS application are received from authorized sources.

Summary of Controls

- All entry of transactions by agencies to COFRS requires advance authorization from the State Controller's Office.
- A user ID and password are required to enter or modify transactions in COFRS.
- One person in each agency is appointed as the Agency Security Administrator. The Agency Security Administrator has update rights for only those users in their agency on the main security table for COFRS, the ASEC table.
- The 1RC01R reports in COFRS are generated and are available to agencies so they can monitor the number of transactions received in each agency interface file and to determine if they were received on a timely basis and were properly authorized.

Tests of Operating Effectiveness and Results of Tests

- Reviewed authorizations from the State Controller's Office granted for entry of interface transactions.
- Inquired of State Application Systems personnel and observed that a user ID and password (ACID) were required to access COFRS.
- Observed an Agency Security Administrator's attempt to update the rights of a user belonging to an agency outside of the scope of their authority and determined that Top Secret successfully denied the administrator's attempt to perform unauthorized changes to user permissions.
- Reviewed 1RC01R reports in COFRS and inquired of an agency user and determined that the reports were generated and available for agency review.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 17

Controls provide reasonable assurance that all input transactions for the COFRS application are validated before processing.

Summary of Controls

- Errors detected in COFRS input cannot be processed until the user corrects them online.
- The CORE supervisory routines require that all transactions are edited and approved prior to acceptance in COFRS.
- Batches are rejected in COFRS if the transaction count and total amount of the batch do not match the proof totals.

- In the rare case that a transaction is clearly erroneous and prevents balancing of the ledgers, Statewide Application Systems staff will manually modify the ledger record. Statewide Application Systems maintains a manual log detailing all such changes. A representative of the State Controller's Office authorizes all changes to the ledgers in writing.
- The SUSF table in COFRS displays the current status (accepted, waiting for approval, on hold or failed edits) of all transactions for five days after acceptance and holds all unaccepted transactions for six months.
- Transactions have a unique ID and users are not able to enter two transactions with the same transaction ID.

Tests of Operating Effectiveness and Results of Tests

- Inquired of Data Center personnel and determined that the CORE supervisory routines were in place and required that all transactions be edited and approved prior to acceptance in COFRS.
- Inquired of Data Center and user agency personnel and determined that edit checks were in place and input transaction errors in COFRS would not process until they were corrected online.
- Inquired of Data Center personnel and reviewed rejection reports and determined that the batches are rejected by COFRS if errors are detected in transaction count or in total amount.
- Inquired of agency user personnel and determined that error reports were delivered and/or available on line in a timely manner for review and error correction.
- Inspected the only general ledger change made during the period and determined that written authorization was received from the State Controller's Office for the change.
- Inspected a sample of transactions captured in the SUSF table and verified that the table contents contained the correct status of each sampled transaction.
- Observed personnel attempt to enter two transactions with the same transaction ID and determined the system properly denied the operation.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Processing Controls

Control Objective 18

Controls provide reasonable assurance that all input transactions for the COFRS application are processed completely and accurately.

Summary of Controls

- All critical programs in the nightly cycle issue termination codes identifying any processing errors detected by the program. Condition code checking in the JCL and CA7 prevents further processing after serious errors have occurred.
- Each morning system analysts review system assurance reports which compare balances, and other reports which will ensure that transactions were processed completely and accurately.

Tests of Operating Effectiveness and Results of Tests

- Reviewed a sample of nightly cycle run termination codes and determined that codes properly identified errors in the program. Also, inquired of Statewide Application Systems personnel and determined that JCL and CA7 prevent further processing after serious errors.
- Inquired of system analysts and determined that system assurance and other reports were reviewed daily; two different analysts independently analyze the reports. The analysts review reports for error codes and as well as positive indicators that transactions were processed completely and accurately.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Output Controls

Control Objective 19

Controls provide reasonable assurance that COFRS output is available in a timely manner

Summary of Controls

- The Data Center maintains a record of each printed warrant number and before printing a new batch of warrants, a computer operator must visually verify the starting warrant number.
- EFT information is transmitted to the bank via a private network during nightly processing.
- Table and ledger extracts are prepared by COFRS programs each night, and stored on the Data Center mainframe. Agencies are responsible for importing, storing or otherwise disposing of extract files before they are overwritten by the next set of extracts.
- Reports are printed via INFOPAC and distributed to user agencies the next business day. User agencies then clerically test reports for mistakes. If mistakes are found, user agencies notify Statewide Application Systems, who then investigates and corrects the mistakes.

Tests of Operating Effectiveness and Results of Tests

- Reviewed a sample of the logs for printed warrants and determined that the Data Center maintains a record of each printed warrant number. In addition, we compared the ending physical warrant number to the ending warrant number on the preceding day’s warrant log and determined that the log was missing one warrant number resulting from a voided warrant not properly recorded by the operator. We then compared the beginning and ending warrant numbers on the log for a sample of days and found all warrants were recorded and accounted for, without exception.
- Inquired of Statewide Application Systems personnel and determined that a notice of transfer was sent to the printer at the controller’s office with each EFT transaction.
- Inquired of Statewide Application Systems personnel and determined that ledger extracts were prepared by COFRS programs each night, and stored on the Data Center mainframe.
- Inquired of user agency personnel who acknowledged they were responsible for importing, storing or otherwise disposing of extract files before they were overwritten by the next set of extracts.
- Reviewed a sample of the INFOPAC reports and determined that reports were sent to agencies the same day or next business day.

- Confirmed through inquiry with Statewide Application Services personnel that user agencies report mistakes to Statewide Application Systems, who then take corrective action.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 20

Controls provide reasonable assurance that output reports are available to users and facilitate user review of data accuracy and completeness.

Summary of Controls

- Weekly COFRS reports are made available to user agencies so that agencies can review the reports for accuracy and completeness.
- Batch balancing is performed and the system verifies resultant (output) reports by matching them against the input data and control totals.
- All reports are logged prior to distribution.

Tests of Operating Effectiveness and Results of Tests

- Inquired of a sample of user organizations and determined that they have access to weekly COFRS output online.
- Inquired of Data Center and verified through observation that COFRS automatically performs batch balancing and users were notified if the totals were not in balance.
- Observed that reports were logged prior to their distribution.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

Control Objective 21

Controls provide reasonable assurance that output of the COFRS application is accessible only to authorized personnel.

Summary of Controls

- INFOPAC is used to control the output of COFRS reports. All reports are batched by user ID.
- For reports printed at the Data Center, a header sheet is generated between batches and printing commands are sent to the high-speed printers. Reports are then logged and sent to the user indicated on the header sheet
- Reports accessed online by users through INFOPAC are restricted to user ID. Users may only access reports assigned to their ID.
- Agency Security Administrators are responsible for granting and revoking user access rights to COFRS reports.

Tests of Operating Effectiveness and Results of Tests

- Observed that INFOPAC is used to control the output of COFRS reports.
- Inquired of Data Center personnel and observed that reports were batched by user ID with header sheets, and were logged prior to their distribution.
- Reviewed a sample of INFOPAC user IDs and determined that access was restricted to only those reports assigned to their ID.
- Observed Agency Security Administrator's attempt to update the rights of a user belonging to an agency outside of the scope of their authority and determined that Top Secret successfully denied the administrator's attempt to perform unauthorized changes to user permissions.

Conclusion

Based on the tests of operating effectiveness described above, controls were operating with sufficient effectiveness to achieve this control objective.

SECTION VII OTHER INFORMATION PROVIDED BY DIVISION OF INFORMATION TECHNOLOGIES DATA CENTER

DISASTER RECOVERY PLANNING

The Data Center maintains an active disaster recovery program through a contractual agreement with a hot-site provider. The viability of the hot site is confirmed through an annual test. This test includes the generation of the Operating System, loading of application databases, establishing communications to customer sites and application restoration and testing by the customers. The generation, loading and file restorations are accomplished by using the actual emergency recovery scripts and data stored specifically for recovery events. This annual test event validates the correctness and sufficiency of the disaster recovery data retention.

APPENDIX A DISPOSITION OF PRIOR YEAR RECOMMENDATIONS

From the SAS 70 – April 2000

No.	Recommendation (response/implementation date)	Disposition
1	• Formal test plans should be written and approved for system software modifications. • Perform load testing on appropriate modifications.	Not Implemented Test plans are not formalized for all modification projects. See current year recommendation No. 6. DoIT disagreed with second recommendation.
2	The Data Center should implement system software version control software to eliminate any human error of not correctly following back-out procedures and save valuable system programmer's time used to perform back-out procedures.	Not Implemented The Data Center has not yet conducted a study to determine the appropriateness of version control software for use with system software development within their environment. See current year recommendation No. 8.
3	The Data Center should add fields to the system software inventory list indicating the date last modified to assist in any attempts to restore previous configurations.	Implemented
4	The Data Center should require that benefit across multiple applications be considered before making the decision to request funding as part of the decision making process for acquiring system software. Additionally, the Data Center should modify documentation to indicate that this process/consideration has been performed.	Implemented
5	Statewide Application Systems should create a database with enough information that ties the application modification to the associated documentation change(s).	Not Implemented Statewide Application Services reports that it does not currently have the staffing resources to implement this recommendation. During testing for the current year, no exceptions were noted relative to the associated user documentation for application modifications.
6	The Data Center should implement more secure procedures in handling the back-up tapes; both in physically securing the metal storage boxes and in transferring the tapes from the Data Center to the vault to ensure back-up tapes are not left unattended in nonsecured areas.	Implemented

No.	Recommendation (response/implementation date)	Disposition
7	The Data Center should use security locks or tamper proof metal bands on tape storage containers to protect against theft, vandalism, or accidents due to mishandling.	Implemented
8	The Data Center should consider using a third party tape storage location, which has industry recommended tape storage conditions, pick-up and delivery, storage security, and quick reaction response in the event of a disaster.	Implemented
9	The Data Center should remove all flammable liquids sitting exposed within the Data Center, Warehouse, and Battery Room and store them in an approved metal storage container. The Data Center should also follow state fire code procedures regarding the location of the fire retardant storage container.	Implemented
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 As only minor equipment changes have been made since the recommendation, this recommendation was not applicable for the current year's testing. However, the Data Center will re-engineer power and cable ducts for all significant future changes.
11	The Data Center should determine a security violation log's retention time frame based on legal requirements and past experiences.	Implemented
12	The Data Center should require all Data Center personnel to sign the General Support Services Computer Usage and Data Security Polic y, which references their acknowledgment and compliance of security policies and procedures.	Not Implemented The Data Center agreed, but has not performed a review of personnel files to ensure signed statements of compliance were present. Some files reviewed during the current year's testing did not contain signed statements. See current year recommendation No. 9.

From the Report on Performance Measures – September 2001

No.	Recommendation (response/implementation date)	Disposition
1	Implement Service Level Agreements with customers.	Implementation plan in Progress Staff has been assigned to project and draft Service Level Agreement is being designed and will be used on a pilot basis by September 2002.
2	Implement customer service management metrics.	Partially Implemented Metrics for performance are currently being generated for certain agencies. There are plans to roll out the program for all customers once the metrics are refined.
3	Define problem management tool requirement and evaluate existing tool.	Not Implemented Funding for this project was denied. In the current year's testing, no exceptions were noted relative to the problem management tracking system.
4	Conduct annual customer survey.	Implemented
5	Implement continuous feedback survey in the service center.	Not Implemented The Data Center reports that it does not currently have the staffing resources to implement this recommendation.
6	Generate monthly performance and capacity management metrics.	Implemented
7	Create a quantitative grading scale for the disaster recovery test.	Implementation in Progress An RFP for a new hot-site provider has been drafted and will be issued approximately June 2002. Upon selection of a provider a quantitative grading scale will be created.
8	Update the contingency plan.	Implementation in Progress The contingency plan is updated for test results and when relevant changes occur in the environment. An RFP for a new hot-site provider has been drafted and will be issued approximately June 2002. Upon selection of a provider the contingency plan will be modified as appropriate.
9	Generate monthly organizational metrics.	Implemented

No.	Recommendation (response/implementation date)	Disposition
10	Update job descriptions to reflect current job skill needs.	Implemented
11	Create training/development plans.	Not Implemented See current year recommendation No. 10.
12	Generate monthly security metrics.	Not Implemented A statewide security assessment was to be performed and provide information that would serve as the benchmark the initial security metrics. The funding for the statewide assessment was denied. However, current year recommendation No. 1, when implemented, provides the baseline information necessary to begin generating these statistics.
13	Match resource charging to customers' utilization.	The Data Center disagreed with this recommendation
14	Trend tape and drive error reports daily.	Implemented
15	Document process and procedures for maintaining and assessing hardware and software inventory lists.	Implemented

APPENDIX B USER CONTROL CONSIDERATIONS

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

The following identifies those control activities that the Data Center and Statewide Application Systems believes should be in place at user organizations and were considered in developing policies and procedures described by the Data Center and Statewide Application Systems 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 to only address those policies and procedures related to the processing of transactions at the Data Center and by the COFRS application. 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 of user organizations.

The purpose of this Appendix 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 the COFRS application. This appendix 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'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 stored in computer files are protected from unauthorized access.
- Application development and maintenance activities are controlled to ensure only authorized changes are installed into production.
- 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.
- Agency applications and data can be recovered in the event of a disaster.

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 back-up Agency Security Administrator or whether the agency relies on the Data Center for security administration duties. Determine whether the agency has a Data Base Coordinator.
- Review the responsibilities of the Agency Security Administrator and the Data Base 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 data sets. These settings include, but are not limited to:
  - The Mode, which prevents access by unauthorized users or merely warns and then allows access.
  - The number of logon 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.
- Review user access identifications to ensure that agency personnel have been granted appropriate access to resources and that such access is limited to "READ, UPDATE, or ALL" access privilege.
- Determine whether agency personnel protect the confidentiality of passwords. Also, determine if personnel share passwords or have multiple access identifications.
- Determine if access identifications are suspended if not used for 60 days. Determine if the agency maintains and reviews a list of access identification assignments and suspensions.
- Confirm that the Agency Security Administrator or the Data Center Customer Service Center is notified promptly when agency personnel changes occur. Review the agency's procedures for purging access identifications.

Physical Access Controls

- 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.
- 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 has implemented procedures to ensure control over agency transactions and data that have been submitted for processing on the Data Center's mainframe computer system. However, it is the agency's responsibility to initiate transactions, 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:

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

Output Controls

- The Data Center's control procedures ensure that agency output is generated and distributed according to agency instructions. However, it is the agency's responsibility to ensure that output is accurate or that corrections are made promptly. When reviewing output controls at the agency, the auditor should:
  - Confirm that exception reports are reviewed promptly and any necessary corrections are made in a timely manner.
  - Look for evidence of management's review of output reports for accuracy, completeness, reasonableness and mathematical accuracy.
  - Review agency procedures for ensuring that output is distributed only to appropriate personnel.

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 agency's policies and procedures to coordinate the agency's disaster recovery plans with those established by the Data Center. Auditors should also review the agency's disaster recovery plans for its own application systems.

Specifically, auditors should verify that agencies:

- Designate resources to be backed up and stored off-site, the frequency of such back-ups, and the methods used to perform the back-ups.
- Establish recover and restart procedures, including coordination with the Data Center's recover and restart efforts. The recover and restart procedures should consider a system designed to establish a priority for critical systems applications.
- Establish 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 off-site, contains all necessary information for locating key personnel, procedures, application programs and data sets.
- Participate in the Data Center "Hot Site" 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.

KPMG

707 Seventeenth Street
Suite 2700
Denver, CO 80202

The electronic version of this report is available on the Web site of the
Office of the State Auditor

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

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

Report Control Number 1462