Gonzales Consulting Services, Inc.
633 17th Street, Suite 1600
Denver, Colorado 80202
303.383.5500

REVIEW OF INTERNAL CONTROLS AT COLORADO INFORMATION TECHNOLOGY SERVICES DATA CENTER

JUNE 30, 1999

LEGISLATIVE AUDIT COMMITTEE
1999 MEMBERS

Senator Doug Linkhart
Chairman

Representative Jack Taylor
Vice-Chairman

Senator Norma Anderson
Representative Ben Clarke
Senator Doug Lamborn
Representative Gloria Leyba
Senator Peggy Reeves
Representative Brad Young

STATE AUDITOR'S OFFICE STAFF

J. David Barba
State Auditor

Joanne Hill
Deputy State Auditor

Tanya Olsen
Legislative Auditor

GONZALES CONSULTING SERVICES, INC. STAFF

Andrew Martinez, Jr.
John Griffith

Report on Internal Accounting and Administrative Control

Members of the Legislative Audit Committee:

We have examined the accompanying description (Appendix A) of the Colorado Information Technology Services Data Center (Data Center). 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 policies and procedures that may be relevant to a user organization's internal control structure, (2) the control structure policies and procedures included in the description (Appendix A) were suitably designed to achieve the control objectives specified in the description; if those policies and procedures were complied with satisfactorily and client organizations applied the internal control structure policies and procedures, contemplated in the design of the Data Center's policies and procedures, and (3) such policies and procedures had been placed in operation as of May 31, 1999. The control objectives were specified by the Data Center. Our examination was performed in accordance with standards, including SAS No. 70 - Reports on the Processing of Transactions by Service Organizations, 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.

We did not perform procedures to determine the operating effectiveness of policies and procedures for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of the Data Center's policies and procedures, individually or in the aggregate.

In our opinion, the accompanying description of the aforementioned system presents fairly, in all material respects, the relevant aspects of the Data Center's policies and procedures that had been placed in operation as of May 31, 1999. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described policies and procedures were complied with satisfactorily, and if client organizations applied the internal control structure policies and procedures contemplated in the design of the Data Center's policies and procedures.

The description of policies and procedures at the Data Center is as of May 31, 1999 and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specified policies and procedures at the Data Center is subject to inherent limitations and, accordingly, errors or irregularities 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 may alter the validity of such conclusions.

This report is intended solely for use by members of the Legislative Audit Committee, management of the Data Center, the user agencies, and the independent auditors of the user agencies. 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.

Gonzales Consulting Services, Inc.
Certified Public Accountants
Denver, Colorado
June 30, 1999

Table of Contents

REPORT SUMMARY
Colorado Information Technology Services Data Center Report on Internal Accounting Controls at a Service Organization

JUNE 1999

Authority, Purpose, and Scope

This audit of the general controls at Colorado Information Technology Services Data Center (Data Center), a section of Colorado Information Technology Services (CITS) was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the State Auditor's Office to conduct audits of all departments, institutions, and agencies of state government. This audit was conducted in accordance with generally accepted government auditing standards. Audit work was performed between April and June 1999.

The State Auditor's Office annually reviews internal controls at the Data Center according to the Statement on Auditing Standards Number 70, Reports on the Processing of Transactions by Service Organizations (SAS 70). Information provided by the Data Center can be found in Appendices A and B of this report where the Data Center has identified its general control objectives and interdependent control procedures. The purpose of this review is to assure the State Auditor, federal auditing agencies, and any contracted audit firms of the integrity of the Data Center's stated general and application controls. Comments on the reliability of controls at the Data Center may be found in the section of the report entitled *Report on Internal Accounting and Administrative Control*. Although this audit does not include a review of performance issues, it does include some comments concerning performance, as deemed applicable.

Our audit objectives did not include a review of controls over the Data Center's customer applications. Auditors of user agencies are responsible for reviewing user agency application controls. Such application controls may include security administration, system development and maintenance, and input and output controls. For example, the Colorado Financial Reporting Section is responsible for developing and implementing application controls over the Colorado Financial Reporting System and auditors of Colorado Financial Reporting System data are responsible for reviewing compliance with these controls. This is the case for other agencies as well, such as the Departments of Human Services, Health Care Policy and Financing, Revenue, and Labor and Employment. A guide for performing reviews of user agency data processing controls can be found in Appendix C.

The control procedures at the Data Center interact with those at state agencies to protect data, systems, and programs from loss or unauthorized access. Therefore, some of the general controls that are tested during this annual audit can be relied upon as part of an auditor's review of user systems processed on the computer at the Data Center, such as prevention of systems analysts from operating the computer to implement unauthorized changes and maintenance of Top Secret Security access.

Control Objectives Achieved

When we tested the general and application control procedures described by the Data Center, we found the control procedures to be effective in achieving the Data Center's stated control objectives. To test the Data Center's compliance with its stated controls, we interviewed various personnel, reviewed documentation and procedures, conducted observations, and performed other tests of

compliance with internal procedures.

Although the Data Center operates efficiently and controls are in place for day-to-day operations, our findings indicate that the Data Center's controls could be improved in certain areas. The main issues revolve around the risks associated with security, organization and management of the Data Center, segregation of duties, and disaster recovery.

The following is a summary of some findings contained in the report.

YEAR 2000 COMPLIANCE

As of the date of this report, the Data Center is currently participating in the Year 2000 (Y2K) *Independent Verification and Validation* process for Information Technology projects, as mandated by the Governor's Office and overseen by the Commission on Information Management Y2K Project Office. The final report of the *Independent Verification and Validation* is scheduled for completion by September 1999 and will include findings and recommendations with opportunity for response from the Data Center.

The Data Center plans to comply with all recommendations from the results of the *Independent Verification and Validation* process, which will have an impact on the Data Center's systems software and hardware for Y2K compliance.

ACCESS TO THE INTERNET

In Fiscal Year 1998 Network Support Services installed a firewall that is more sophisticated than the prior firewall used at the Data Center. However the firewall is not fully installed with all of its optional upgrades. Although the new firewall is operational, additional protections are necessary to fully protect the Data Center's mainframe and other computer resources from security breaches and other forms of unauthorized access.

Conditional communications environments, like the one that now exists, restrict access to only those persons who arrange for it in advance. This is now accomplished by the use of a method known as Internet Protocol Unique Addressing. On the other hand, an open communications environment requires agencies and the Data Center to install and maintain their own firewalls and hence, takes away the protection afforded by a system of pre-arranged access. An independent Security Vulnerability Study shows that "although the Data Center mainframe is adequately protected by security software, the network that connects it to the public is not. A secure computer on an insecure network is not desirable."

The Data Center's management team should implement all changes within budget limits recommended by the independent Security Vulnerability Study before proceeding with full *open* attributes of the Data Center's Internet process.

DATA CONTROL / HANDLING

Maintaining proper inventory control at the Data Center has been compromised due to several occurrences of missing tapes and mishandled reports. This has created the potential for unauthorized access to warrants and other materials leaving the Data Center. Results of these problems could cause, at a minimum, liability issues which include the additional expense of reprinting reports, reprocessing data, and reissuing warrants at the Data Center's expense.

It is recommended that the Data Center list tape numbers of foreign tapes on the inventory sheet. Additionally, the Data Center should require a copy of the inventory sheet, be included in the sealed container sent to each agency, and receipt procedures should be employed. Warrants should be shipped with an inventory sheet, enclosed in the tamper-proof container.

ORGANIZATION / SEGREGATION OF DUTIES

The Data Center has reorganized and restructured its operations over the past fiscal year. Changes have included reductions in staff, management shifts, modified lines of authority and communication, and new procedures. The reassignment has required certain control objectives, discussed in Appendix B of this report, to be modified. During our review, we noted several problems with segregation of duties.

We recommend that all duties of security administrative individuals be segregated from all operational duties including any and all alternate operational positions.

SECURITY ADMINISTRATION

System security with respect to the Data Center and customer resources is critical to ensure data integrity. The Data Center must not only have adequate system security controls in place, it must also regularly monitor those controls and investigate any security violations. During our audit, we identified the following potential security issues:

- All adaptable database passwords had not been updated annually.
- The Data Center does not have proper procedures regarding assignment/reassignment of new or in use Accessor Identification (ACIDs).
- The Data Center has inappropriate and possibly widespread access to various mainframe computer programs, to include Top Secret Security files and related access to the Security Authorization Table.
- The Data Center has inconsistency of users not following proper security guidelines and standard operating procedures. Potential risk to the system data could result from the granting of security access during emergency circumstances.

The Data Center should ensure that all software passwords are updated on a regular basis, and procedures should be followed when assigning certain level accesses to users of various computer programs.

DISASTER RECOVERY PLAN, AND PRODUCTION MAINTENANCE

During our audit, we noted the following matters relating to the Disaster Recovery Plan and accompanying backup procedures:

- The Data Center is not conducting quarterly backup tape inventories.
- The two standby high speed communication lines connecting the Hot Site with the planned Denver metro area command center are not sufficient to provide service to all Data Center customers. A protocol must be established for the sharing of one of the lines to enable the Data Center to service its customers outside of the Denver metro area.

The Data Center should perform quarterly physical backup and disaster recovery tape inventories, and commission its customers to develop a plan to share one of the two standby, high-speed communication lines connecting the Hot Site with the planned Denver metro area command center.

PROTECTION OF BACKUP AND DISASTER RECOVERY TAPES AND ACCESS TO THE OFFSITE BACKUP TAPE VAULT FACILITY

In cooperation with the Department of Revenue, the Data Center maintains an offsite backup tape vault facility at 1375 Sherman Street in Denver. The facility is used to store tapes for normal Data Center backup maintenance and tapes needed in the event of a disaster. During our audit, we noted the following items that may jeopardize the integrity and usability of backup and disaster recovery tapes:

- The environmental conditions and security features of the tape vault facility may not be adequate to protect the tapes.
- The list of personnel with authorized access to the tape vault facility was not updated to reflect the most recent Data Center personnel changes.
- Access into the vault is compromised by use of standard-type doors, and does not properly provide adequate security to protect tapes.

The Data Center should perform a comprehensive analysis to identify an alternate offsite tape vault facility that provides appropriate environmental, safety and security features. Management should maintain the list of personnel who are authorized to access the tape vault facility, and consider improving access into the facility by installing heavy-duty fireproof steel doors with dead-bolt locks.

RECOMMENDATION LOCATOR

Rec No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	12	Implement all changes within budget limits recommended by the security vulnerability study before proceeding with full *open* attributes of the Data Center's Internet process.		
2a	13	List tape numbers of customer owned tapes on the Inventory Sheet. Require a copy of the Inventory Sheet, to be included in the sealed container being sent to each agency, and receipt procedures should be employed. Warrants should be shipped with an Inventory Sheet, enclosed in the tamper-proof container.		
2b	13	Maintain the Sign In/Out sheets for the Loading Dock.		
3	15	Separate security administration staff from all operational duties including any and all alternate operational positions. The Data Center should isolate the responsibilities and duties of the Master Security Administrator to report only to the Data Center Manager.		
4a	16	Ensure that the continued software updates required to update adaptable database software passwords is maintained. Passwords should be updated immediately. The Data Center should utilize either alternate resources within the Data Center, or employ the services of another vendor for password update automation.		
4b	16	The Data Center should implement an assignment/reassignment checklist.		
4c	17	1. Review all personnel user IDs and Group Profiles. 2. Identify and restrict access to Top Secret Security console attributes. 3. Change the level access granted to the Customer Service Schedulers.		
4d	18	The Data Center should: • Identify security violations owned by the Data Center and recommend any investigative, follow-up or disciplinary actions, which is monitored by the Data Center Central Security Administrator. • Carefully review the Data Center Group Profile that permits the Data Center Technology Services Group to modify its security access in extreme emergencies and ensure that access to this Group Profile is restricted to an absolute minimum number of Data Center personnel.		
5	19	Consider discontinuing the annual Customer Satisfaction Survey as now administered, and investigate alternative methods of acquiring customer feedback.		

Rec No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
6a	20	Ensure that the Telecommunications Section finalizes its formal *Disaster Recovery Plan*, which coordinates with the Data Center's *Disaster Recovery Plan*. The Data Center should encourage its customers to work together to develop a plan to share one of the two standby high speed communications lines connecting the Hot Site with the planned Denver metro area command center.		
6b	20	Follow the standard operating procedure requiring quarterly physical backup and disaster recovery tape inventories.		
6c	21	Commission: • All Data Center and customer disaster recovery personnel periodically update the vital records portion of the REXSYS disaster recovery database. • Data Center's customers to obtain a proper software utility program to perform interpretation maintenance to backup appropriate data sets and application programs that will be stored offsite.		
6d	21	Modify backup procedures relating to the Data Center and customer adaptable database resources so that they are fully automated.		
6e	22	Determine the most cost-effective method to implement a back-up printing capability to ensure that customer service interruptions are minimized. The Data Center should communicate the service needs with the vendor and implement any recommendations that arise from the *Printer Service Plan.*		
7	23	• Perform a comprehensive analysis to identify an offsite tape vault facility that provides appropriate environmental, safety and security features. Consider the cost/benefit of relocating the existing tape vault facility. • Properly maintain the authorized personnel list. Any personnel not on the list should not be given access into the tape vault facility.		
8	24	Instruct the Safety Committee to: • Continue to address safety and non-safety issues on a routine basis and schedule more proactive safety meetings with Administration. • Maintain adequate written evidence (certificates of inspection) in an administrative file to verify that all fire prevention systems have been inspected on a regular basis. • Draft a schematic for each floor plan for proper fire escape routes and place such maps throughout the facility at 690 Kipling Street.		

Chapter One

Overview of the Colorado Information Technology Services 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. As such, it is one of the busiest computer centers in the State.

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, in conjunction with the CITS Telecommunications Section, 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 GGCC's responsibility for control of the development and maintenance of other portions of the State's central financial system. COFRS, now part of the Application Services Section of CITS, has assumed these responsibilities.

The Data Center has two main customer groups that provide suggestions for improving the Center: (1) the Customer Roundtable (CR), and (2) the Chief Information Officers' Forum (CIO Forum). The Data Center established the CR Forum to improve communications between itself and its users. The CIO Forum was established to provide input regarding the general direction 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 1999 the Data Center received an appropriated spending authority of about $12 million to provide computer services for state agencies.

Organization and Functions

The Data Center operates 24 hours per day, seven days a week, including holidays. It has a staff of 70 full time equivalents (FTE), predominately located at the Data Center. They are organized into the following functional sections:

- **Manager:** The Manager (1 FTE) oversees the entire operation of the Data Center and the Pueblo Data Entry Center.

- **Business and Administrative Services:** This section provides the support services required to operate the Data Center. It is responsible for budget preparation, control, and monitoring. It is also responsible for internal accounting, personnel functions, word processing, and switchboard and receptionist services at the Data Center. Organizationally, these staff report to a manager in the CITS division parallel to the Data Center Manager. This section has 5 FTE.

- **Customer Support Services:** This section's primary responsibility is providing customer support. Its responsibilities include change management, Y2K coordination, 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 Support providing scheduling, console management, help desk, and video conference support. This section employs 17 FTE.

- **Technical Services:** This section is responsible for 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. This section has 21 FTE.

- **Computer Operations:** This section consists of the Data Center's computer operations unit, the disaster recovery unit, and the Service Center. It is responsible for installing and operating computer and printing equipment, maintaining disk and tape systems, and the control and distribution of computer output. This section maintains responsibility and control for problem management and scheduling production work. The disaster recovery unit is responsible for developing, implementing, coordinating, and monitoring the Data Center's disaster recovery plan. A total of 26 FTE work in Computer Operations.

The 38 FTE from the Pueblo Data Entry Center in previous years reported to the Data Center Manager. These personnel are no longer included due to a change of reporting to the Business Manager of CITS. This change retains the Pueblo Data Entry Center within CITS, but removes it from the Data Center.

Chapter Two

Performance of the Data Center

YEAR 2000 COMPLIANCE

Year 2000 (Y2K) compliance issues result from the inability of computer programs or computerized equipment to calculate, store, or use a date subsequent to December 31, 1999. Although the erroneous date can be interpreted in a number of different ways, the Year 2000 is typically interpreted by a computer as the Year 1900. This interpretation may result in a system failure or miscalculations that may cause disruptions of operations, including a temporary inability to process transactions.

The Data Center has addressed Y2K compliance by expanding the size and capacity of its mainframe computer and subdividing or partitioning its mainframe Central Processing Units into three pre-defined areas or partitions. These three areas are known as the production, test, and Y2K logical partitions. The Y2K partition utilizes an alternative date/time clock to test the Data Center operating system and customer application software products for Year 2000 compliance. After software products are successfully tested in the Y2K partition, they are moved into the production partition for live processing.

An Information Management Committee has been charged with the mission of assisting statewide Data Center customers with Y2K compliance. This includes requiring the Data Center and its customers to inventory all software products now in use and to provide monthly progress reports to ensure that all Y2K compliance projects are completed in a timely manner.

The Data Center has assigned personnel to coordinate, manage, monitor, and report on the Data Center Y2K compliance. The management process includes an inventory of all Y2K compliance projects and assignment of projects to appropriate members of the Data Center staff.

Audit review of the Y2K procedures and underlying documentation indicated the following. The Y2K internal compliance target date was August 1999. However, according to reports received by the Data Center's Y2K Coordinator, all projects identified as fatal or critical were completed by March 1999. All in-house applications, systems software, and mainframe hardware have been inventoried, assessed, remediated, tested, and implemented in production. In-house billing programs, PC remediation, and other miscellaneous tasks of no impact to the state agencies are considered non-fatal/critical and are scheduled for completion by December of 1999.

The system verification process for all fatal and critical information technology projects, as mandated by the Commission on Information Management (IMC) Y2K Project Office, is complete.

The Data Center's Y2K Embedded Systems project is complete as of July of this year. The inventory, assessment, and detail planning phases of the project are complete. Only a few building system components require replacement for Y2K compliance. The Division of Real Estate Services will perform the work with oversight by the IMC's Embedded Systems Project Office. The Legislature appropriated funding for the projects in April, and the replacement equipment has been ordered. Work was completed in late June and July of 1999.

As of the date of this report, the Data Center is participating in the Y2K *Independent Verification and Validation* (IV&V) process for Information Technology projects, as mandated by the Governor's Office and conducted by the IMC Y2K Project Office. Results from this Independent Verification and Validation process will indeed confirm the outcome and impact on the Data Center's systems software and hardware for Y2K compliance.

We reviewed and discussed with the Data Center Y2K Coordinator, the Independent Verification and Validation process update, which is summarized as follows:

The Y2K IV&V process is underway for the CITS Data Center. The IV&V process consists of two phases, one in which remediated code is reviewed, the other in which process management, project management and project progress are reviewed. Two separate vendors were chosen by the Y2K Project Office to conduct this work.

The first phase of the IV&V process is a review of code remediated by the Data Center. The Data Center sent three packages of code to the contracted vendor, Reasoning, Inc. These included separate packages for Natural, COBOL, and Assembler code. IV&V results for Natural code were returned from the vendor on July 12, 1999. No action items were requested. Results for COBOL and Assembler are to be returned from the vendor on July 19, 1999.

The second phase of the IV&V process is an on-site audit of the Data Center's process management, project methodology and Y2K project progress. The vendor for this phase is Hitachi Data Systems Corporation. The scope of this audit is not limited to Y2K efforts, but includes determining findings and recommendations for any process improvements that the contractors observe. This phase will begin on July 20 and continue for one or more weeks.

The deliverables for the project include Reasoning, Inc.'s code review results for the Data Center's Natural, COBOL, and Assembler code and a Final Report covering process, project methodology and project progress from Hitachi Data Systems Corporation. The Final Report will include findings and recommendations with opportunity for response from the Data Center. The Final Report is expected in August or September.

The Data Center has five days to analyze any code errors returned by Reasoning, Inc. The Data Center's first code package was returned by the vendor with no errors found. This is the first "no error" package in the State. The remaining code will be returned on July 19th. Any errors found will be analyzed for their validity and corrected if necessary. CITS management will consider all recommendations for process improvement and project methodology made in the Final Report from Hitachi Data Systems Corporation.

We have been informed that the Data Center intends to follow-through with the recommendations made in the Final Report of the Y2K Independent Verification and Validation process for Information Technology projects to confirm the outcome and impact on the Data Center's systems software and hardware for Y2K compliance.

ACCESS TO THE INTERNET

The Colorado Information Technology Services (CITS) Division is composed of six sections. The Data Center is one of such sections and CITS Telecommunications Services is another section. The Network Support Services group in the Telecommunications Services Section works closely with the Data Center and manages the Data Center's data routing and security services related to the Internet.

Although flexibility is the key term used in service-oriented companies, privacy is the ultimate concern when confidential documents are presented electronically. CITS offers its customers several avenues to access the readily available records managed by the Data Center. The Internet provides the most flexible, cost effective, effortless, and high-speed access for high-performance networking applications to be developed. Ultimately, Internet access provides CITS customers with the most flexible means to easily retrieve, review, and modify records. The ongoing responsibility of CITS staff, as security administrators, is to allow proper agency access through the sophisticated capabilities within the information network, while denying access to unauthorized users.

As the Internet has adapted for business use, numerous Internet security issues have emerged. Some of these are related to the architecture of the protocols that are used on the Internet. Others are related to the broad diversity of applications, operating systems, and computer types that are used on the Internet.

The Data Center limits access to its mainframe computer and the *closed* (protected) portion of the Colorado Information Network through the use of Top Secret and other security software and hardware products collectively known as a firewall.

In Fiscal Year 1998 Network Support Services installed a firewall, which is not installed with all of its optional upgrades. The new firewall is operational, but additional protections are necessary to fully protect the Data Center's mainframe and other computer resources from security breaches and other forms of unauthorized access. This is because the firewall will allow Network Support Services to change the existing communications environment to either a *conditional* or an *open* one.

Conditional communication environments, like the one that now exists, restrict access to only those persons who arrange for it in advance. This is now accomplished by the use of a method known as Internet Protocol Unique Addressing. *Open* communication environments require agencies and the Data Center to install and maintain their own firewalls and hence, eliminate the protection afforded by a system of pre-arranged access.

An independent network security study was performed by Vertex, Incorporated. The completed June 30, 1999 study shows that "although the Data Center mainframe is adequately protected by security software, the network that connects it to the public is not. A secure computer on an insecure network is not desirable." Presently, the Data Center network appears to be operating with minimal security measures in place. A single router provides present access to the mainframe host from the Internet. This router's operating system does have security features that could be used, but are not implemented. Other security tools that could be employed in other portions of the network are also missing. The study further states that, "Many steps, explained and outlined in this report, can be taken to improve the security of the Data Center network. Some are easily implemented, others require a larger effort. A complete commitment

to robust security may well require a proportional commitment to staff time and training. Security is not an easy technical challenge – it requires time, planning, and funding."

Although it is an advantage for the CITS Data Center to rely upon the Internet for provision of computing services to several Colorado state agencies, the consequences of continuing to postpone security planning and implementation could be expensive.

Without increasing security on the network, the Data Center could potentially encounter computer hackers to gain access to sensitive data and programs.

Recommendation No. 1

The Data Center management team should implement all changes within budget limits recommended by the security vulnerability study before proceeding with full *open* attributes of the Data Center's Internet process.

Data Center Response:

The Data Center agrees with this recommendation. The Data Center will proceed in conjunction with Network Services, the IMC and the Office of Innovation and Technology in determining network security strategy. Recommendations discussed in the security vulnerability study will be considered for implementation. The author of the study acknowledges that full implementation will span years, require dedicated staff and require a million dollar expenditure.

DATA CONTROL / HANDLING

Maintaining proper inventory control at the Data Center has been compromised due to occurrences of missing tapes and mishandled reports. According to the Data Center management team, missing tapes primarily happen during inventory counts, and mishandled reports occur very rarely. Although very few incidents of missing articles of the Data Center occur, data contained on such media is too sensitive and costly to compromise. Unsecured containers have created the potential for unauthorized access to warrants and other materials leaving the Data Center. The implementation of tamper-evident security tape has mitigated these problems. However, service agency liability issues continue to cause additional expenses of reprinting reports, reprocessing data, and reissuing warrants at the Data Center's expense.

Inventory Sheet Process

Customer owned tapes are generated outside the Data Center and are shipped to the Data Center for future manual access. The audit and Center staff discussed the concept of using the current *log out sheet*, used primarily for tracking customer owned tapes, as an *inventory sheet*. The *log out sheet* will require modifications to serve as the *inventory sheet*. Every out-going container from the Data Center should contain a copy of such *inventory sheet*. The *inventory sheet* would list the contents within the container, and general instructions for the receiving agency. Upon receipt, the appropriate agency would be required to sign the *inventory sheet* as confirmation of receiving all materials. For agencies with more than one receiving department, it is the responsibility of the first person of the receiving agency that breaks the sealed container to sign the *inventory sheet*, and immediately fax the signed *inventory sheet* back to the Data Center. To minimize or eliminate lost reports, tapes, or other critical documents, each receiving agency is

required to have a select number of personnel authorized to sign the *inventory sheet*. In order to maintain accurate inventory control of materials circulating to and from the Data Center, it is important that each agency comply with the *inventory sheet* process. We believe that these procedures can be employed without incurring any additional cost or contracting any additional employees.

Recommendation No. 2a

It is recommended that the Data Center list tape numbers of customer owned tapes on the *inventory sheet*. Additionally, the Data Center should require that a copy of the *inventory sheet* be included in the sealed container sent to each agency, and receipt procedures should be employed. Warrants should be shipped with an *inventory sheet*, enclosed in the tamper-proof container.

Data Center Response

The Data Center agrees with this recommendation and is currently implemented. Customer owned tapes are specifically listed on the inventory sheet and returned with the tapes to customers. Enhanced, tamper-proof shipping containers for warrants will be further discussed with the State Controllers Office.

Sign In/Out Loading Dock Sheets

The sole purpose of the Sign In/Out loading dock sheets is to maintain a list of all authorized personnel arriving and departing the loading dock area of the Data Center. An unauthorized access to a high-risk area could occur if the Data Center does not properly maintain a log to allow only authorized personnel access to the Data Center's resources.

The Sign In/Out sheets for the Loading Dock have not been maintained appropriately since November 5, 1998. The Data Center stated that effective June 1, 1999, Sign In/Out Sheets for the Loading Dock will be maintained.

Recommendation No. 2b

The Data Center should maintain the Sign In/Out sheets for the Loading Dock.

Data Center Response

The Data Center agrees with this recommendation and is currently implemented. Sign In / Sign Out sheets are utilized at the loading dock.

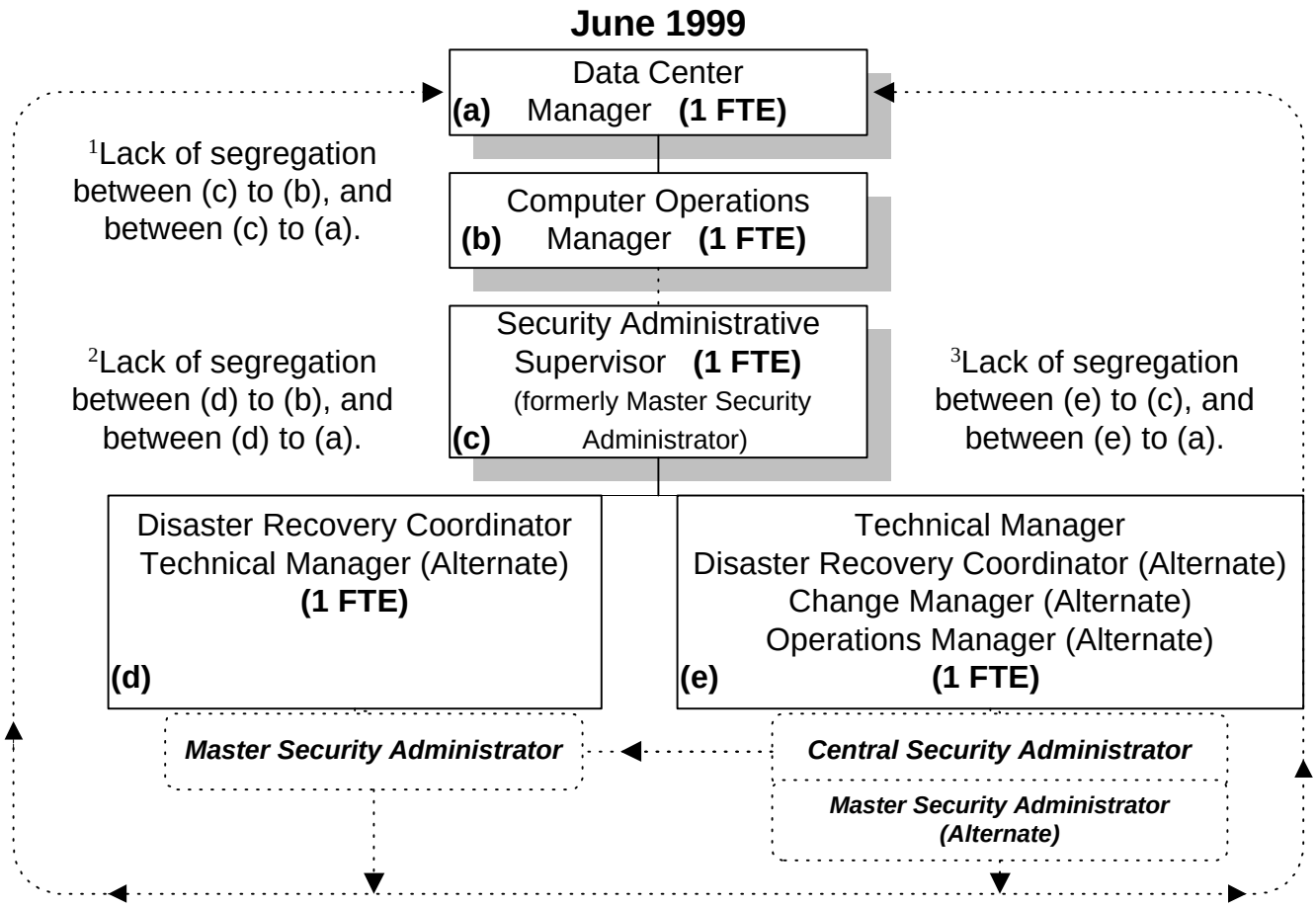
ORGANIZATION / SEGREGATION OF DUTIES

Segregation of Duties

Over the past fiscal years, the Data Center has reorganized and restructured its operations. The changes have included reduction in staff, change in management, changes in lines of authority and communication, and modifications to the procedures employed by the Data Center. These restructuring changes and reduction in staff have resulted in added responsibilities for the remaining Data Center personnel. The reassignment of responsibilities has required certain control objectives, discussed in Appendix B of this report, to be modified. Despite restrictions

placed on access to resources by the Data Center customers, it is logical that within a service center, such as the Data Center, access to resources through Top Secret Security should be separated from the production of output for service center customers.

Prior year audit reviews conclude that a continuous problem arises with segregation of duties between security administration and computer operations. From June 1998 through May 1999, the Master Security Administrator reported to the Computer Operations Manager. This reporting relationship violates the concept that security administration should be segregated from computer operations to prevent unauthorized access and to ensure physical control of resources. The current Master Security Administrator has the added responsibility of Disaster Recovery Coordinator and is an alternate to the Change Manager.



[1]In June 1999, the person who functioned as the former Master Security Administrator was named the Security Administrative Supervisor. The responsibility of the Security Administrative Supervisor is to train the Disaster Recovery Coordinator, and the Technical Manager. Although supervisory duties do limit the immediate control of security functions, the reporting relationship with management has been compromised. Security issues are presently being reported to the Data Center Manager (a), and any operational issues are reported directly to the Computer Operations Manager (b). Conflict of interest occurs when the Security Administrative Supervisor (c), reports to two separate managers at different company levels.

[2]The Disaster Recovery Coordinator (d), is also the alternate Technical Manager and the current Master Security Administrator. The Disaster Recovery Coordinator ultimately reports to the Computer Operations Manager (b). This reporting relationship results in a segregation of duty conflict. The Master Security Administrator reports directly to the Data Center Manager (a). Presently the Data Center Manager's position is vacant. The current Director of the Data Center is acting as the Data Center Manager to oversee the duties of the Master Security Administrator.

[3]The Technical Manager (e), who is presently the Central Security Administrator, has a conflict of segregation of duty as an alternate to the Master Security Administrator. Both the Disaster Recovery Coordinator/Master Security Administrator, and the Technical Manager/Central Security Administrator (e), presently report to the Security Administrative Supervisor (c), who reports to the Computer Operations Manager. If the Technical Manager is performing the duties as the alternate Master Security Administrator, who is to report to the Data Center Manager (a), conflict in management reporting occurs when the alternate Master Security Administrator reports to the Security Administrative Supervisor, who reports to the Computer Operations Manager.

Recommendation No. 3

Individuals responsible for security administration should be separated from all operational duties including any and all alternate operational positions.

The Data Center should isolate the responsibilities and duties of the Master Security Administrator to report only to the Data Center Manager.

Data Center Response:

The Data Center disagrees with this recommendation. Though the suggested absolute segregation of duties for the security administrator may well be desired, neither staffing nor security work load support full isolation of the security administration function. This recommendation will be again evaluated if implementation of the security vulnerability study includes additional skilled security personnel.

SECURITY ADMINISTRATION

System security with respect to the Data Center and customer resources is critical to ensure data integrity. The Data Center must not only have adequate system security controls in place, it must also regularly monitor those controls and investigate any security violations. To achieve this objective, the Data Center has appointed a non-Technology Services Master Security Control Administrator who monitors all user ID's and Top Secret Security Violation Reports for violations. Additionally, the Data Center sponsors quarterly meetings and training sessions to assist agency security administrators with monitoring of access controls.

Adaptable Database Password Updates

The importance of the adaptable database software program allows the Data Center customers to communicate directly with the Data Center mainframe using different types of computer languages. We performed a limited review of the Data Center's adaptable database security and

passwords. Despite the Data Center's efforts to install a software product update, that will automatically inform the agency to change the password annually, we noted that not all agencies had annually updated their passwords. Although partial implementation of changed passwords was accomplished as a result of the 1998 audit recommendations, the Data Center is planning all password changes for all agencies by the end of August of 1999. Since the review of this summary, the vendor withdrew the software product update.

Recommendation No. 4a

The Data Center should ensure that the continued software updates required to update adaptable database software passwords is maintained. Passwords should be updated immediately. With the updated knowledge of the vendor withdrawal from the software product, it is further recommended that the Data Center utilize either alternate resources within the Data Center, or employ the services of another vendor for password update automation.

Data Center Response:

The Data Center agrees with this recommendation. All agency annual password change is supported by the Data Center. Next year's password change schedule is being advanced so that changes are complete prior to the annual audit rather than in-progress at the time of the audit.

Accessor Identification

The Data Center does not have proper procedures regarding assignment/reassignment of new or in use Accessor Identification(s) (ACIDs). For example, when an employee leaves, his or her identification number is reserved for a replacement employee. Old identification profiles are not discontinued, and new profiles are not generated. In turn, the new employee may have access to areas that are not appropriate. Hence, the individual internal sections of the Data Center are not informed of access limitation by that particular ACID. The Data Center's administration does not presently have a checklist of who has access on what ACID. Further, the Data Center offers security services for agencies without their own security administrator.

Recommendation No. 4b

The Data Center should implement an assignment/reassignment checklist, which originates with administration, is monitored by the Master Security Administrator, and is constantly updated through each internal section of the Data Center. When an employee is reassigned or terminated, their ACID should be cancelled and a new ACID is issued in accordance with the job requirements. ACID assignments outside of the Data Center, which are serviced by the Data Center security administration, should be monitored closely by the Master Security Administrator, and procedures should be the same as the internal access limitations of ACIDs.

Data Center Response:

The Data Center agrees with this recommendation to better monitor and maintain system security authorizations of its employees at the Data Center through administratively processing security access specifications as part of personnel re-assignment or termination.

User IDs and Group Profiles

During our audit, we examined samples of User IDs and Group Profiles that are permitted access to various resources and found that access is generally appropriate. However, we noted that certain user IDs and Group Profiles were either inappropriate or warranted further investigation due to employee separation, changes in organizational structure, or inherent risks to the Data Center or customer resource integrity. Example: An employee who has level access before a transfer, and not restricted when moved to another department/area, could cause potential risk.

At given occurrences, the Data Center personnel have been given limited access to production programs. Such privileges compromise security controls. We reviewed access, through user IDs, Group Profiles, and specific software applications, to the Data Center's primary security file and computer consoles. Although the Data Center has established control objectives that state "programmers and system analysts are not permitted to operate the computer" and "operators are prohibited from making changes to production programs," certain situations require that the Data Center personnel have limited access to resources. Such access is needed to solve operating system and customer application software problems pursuant to the Data Center's Standard Operating Procedure # 8813. However, the policy does not state the length of time an operator has access to certain production programs for modification, or any restrictions of level-access in any given program.

With respect to our review of the primary security file and the related security authorization table, we noted that Top Secret security console attributes, which permit authorized personnel to change Top Secret security settings, have been granted to many of the Data Center and vendor personnel. Despite the need for backup personnel in an emergency, the extremely critical nature of Top Secret Security settings, indicates that the number of persons granted Top Secret Security console attributes appears to be too large. According to policy, only authorized personnel, limited to security administration, are to be given access.

We reviewed the appropriateness of security administrator security levels granted by the security administration. These allow the user certain degrees of access within program applications. We noted during our review that certain personnel who have been granted central, divisional, or departmental Security Administrator status should not continue to be granted such status. For example: Customer Service Schedulers have Security Administrator access, which is greater than required.

Recommendation No. 4c

To maintain a secure level of access using proper security IDs, the Data Center should:

1. Thoroughly review and document all of the Data Center user IDs and Group Profiles that grant access to console attributes. Identify and restrict access to console attributes to a critical need basis only.
2. Identify and restrict the appropriateness of all the Data Center and vendor personnel granted access to Top Secret Security console attributes. The Data Center should restrict access that permits the changing of Top Secret Security settings, such as logging functions.
3. Review, monitor, and document the level access granted to the Customer Service Schedulers.

Data Center Response

The Data Center agrees to:

1. User ID's and group profiles will be reviewed.
2. Identify and restrict the appropriate access to Top Secret Security console attributes, but must review on a case by case basis before restricting specifically recommended authorities. Technical review is necessary before further committing.
3. Scheduling services now provided to the agencies by Service Center Staff must be continued. Agree that no higher level of access security needs to be granted then that which allows the full set of services to continue.

Security Administration Policy

The strategy of the Data Center is to maintain records and control the appropriate access to all programs, and data contained therein. The following matters relate to the inconsistency of users not following proper security guidelines and standard operating procedures:

- The Data Center issued a Top Secret Security Administration Policy on April 30, 1997 which assigns responsibility for security administration to Agency Security Administrators and provides information relating to the identification of security violations, but does not recommend any investigative, follow-up, or disciplinary actions. Standard Operating Procedure #8813 states that any activity authorized by it "is monitored by the Data Center Central Security Administrator and security officer." The standard operating procedure does not specify what procedures are to be followed by the Central Security Administrator with respect to investigating and resolving security violations, except that "inappropriate use of this provision...is grounds for disciplinary action...provided by law." Standard Operating Procedure #8808 does discuss the procedures to be followed in connection with "processing attempted security violations."

- This year and in past years, we determined that in emergency circumstances, the Technology Services Section of the Data Center has the ability through a special Group Profile to modify its own security access. Although this modification of security access may be necessary in certain circumstances and is monitored through a Data Center audit tracking file, it creates a vulnerability to abuse and potential risk to system data integrity.

The following actions are necessary to restrict access to the Data Center and customer resources without violating the Data Center's control objectives and sacrificing customer service. They are also intended to prescribe uniform procedures to investigate and resolve security violations.

Recommendation No. 4d

The Data Center should:

- Identify security violations owned by the Data Center and recommend any investigative, follow-up or disciplinary actions. This process is monitored by the Data Center Central Security Administrator. Procedures should be followed by the Central Security Administrator with respect to investigating and resolving security violations or the attempt of security violations, with grounds for disciplinary action provided by law.

- Carefully review the Data Center Group Profile that permits the Data Center Technology Services Group to modify its security access in extreme emergencies and ensure that access to this Group Profile is restricted to an absolute minimum number of Data Center personnel.

Data Center Response

The Data Center agrees with this recommendation. Security Administration will document violations and will pass such documentation to the appointing authority for consideration of corrective or disciplinary action consistent with Personnel procedures. The Data Center Group Profile will again be reviewed to insure that capabilities to modify security access in emergencies is sufficiently restricted and that compensating controls are evident.

CUSTOMER SATISFACTION SURVEY

Over the past several years the Data Center has distributed an annual Customer Satisfaction Survey. The main purpose for the survey is to gain feedback from customers and personnel.

The survey response rate over the past four years has declined from 32 percent in Fiscal Year 1996 to two percent in Fiscal Year 1999. Since the response rate was so low, the Data Center did not publish survey results for the Fiscal Year 1999 survey and is considering discontinuing the survey distribution.

Because of the importance of customer service feedback, the Data Center should explore other sources of receiving information from customers such as an Internet or an e-mail approach.

Recommendation No. 5

The Data Center should investigate alternative methods of acquiring customer feedback. The Data Center may consider an Internet or e-mail approach in acquiring information from customers and personnel.

Data Center Response

The Data Center agrees with alternative methods for acquiring customer feedback will be explored.

DISASTER RECOVERY PLAN, AND PRODUCTION MAINTENANCE

The *Disaster Recovery Plan* outlines the steps necessary for the State to recover critical resources in the event of a fire, flood, earthquake, or other type of disaster. The Data Center has worked to coordinate and facilitate statewide disaster recovery efforts by updating the *Disaster Recovery Plan* on an ongoing basis, conducting hot site tests, and meeting regularly with its customers to discuss disaster recovery and hot site test strategies. Currently, a set of documents which represents the Data Center's codified *Disaster Recovery Plan* is located at both the Data Center and the Department of Revenue offsite backup tape vault facility.

During our audit, we noted the following matters relating to the Data Center's *Disaster Recovery Plan* and backup procedures:

Telecommunication Disaster Recovery Plan

Since telecommunications is an integral part of the Data Center operations, a formal CITS Telecommunications disaster recovery plan must be established. The CITS Telecommunications Section, which the Data Center relies upon for data transmission, has not finalized its formal Disaster Recovery Plan.

Since only two T-1 communications lines will be available at the hot-site instead of the usual five T-1 lines, a protocol must be established for the sharing of one of the lines to enable the Data Center to service its customers outside of the Denver metro area.

Currently, there is no Telecommunications Disaster Recovery Plan established or finalized. There are not enough dedicated lines for disaster recovery operations, and there are no changes from prior year's audit report.

Recommendation No. 6a

The Data Center should ensure that the Telecommunications Section finalizes its formal Disaster Recovery Plan, which coordinates with the Data Center's Disaster Recovery Plan.

The Data Center should encourage its customers to work together to develop a plan to share one of the two standby high speed communications lines connecting the Hot Site with the planned Denver metro area command center.

Data Center Response

The Data Center agrees with this recommendation. The Data Center continues to encourage the finalization of the communications Disaster Recovery Plan. Customers continue to be encouraged to work together to develop a resource sharing approach to the limited communications facility.

Inventory Control

Pursuant to Recommendation 8a in the 1998 audit report, the Data Center revised their procedures to require quarterly inventories of physical backup and disaster recovery tapes. As of the date of this report, the Data Center has not conducted all quarterly backup tape inventories. The results of the Data Center's March 1999 annual physical backup tape inventory indicated that the backup and disaster recovery tape management systems is sufficient to support a successful disaster recovery mission; however, prior inventories did not provide the same degree of accuracy. The semi-annual inventory of September 1998 showed an inventory count of 69 missing tapes. The February 12, 1998 inventory count showed 20 missing tapes. Quarterly inventories will increase the reliability of backup and disaster recovery tape management systems.

Recommendation No. 6b

The Data Center should perform quarterly backup tape inventories (Standard Operating Procedure # 6717).

Data Center Response

The Data Center agrees with this recommendation and is currently implemented. Physical Inventories are scheduled quarterly as specified in Standard Operating Procedure # 6717.

Updating Software

The software needed to update the appropriate needs of various agency computer software programs for disaster recovery is REXSYS. In order that the Data Center may fully service all agency data needs in response to a disaster, the vital records portion of the REXSYS Disaster Recovery database needs to be updated on an ongoing basis to ensure the success of a disaster recovery mission.

Access Mediation

The Data Center is presently testing a software gateway product, which enables access to non-relational mainframe data resources. Data Center customers do not presently have the proper software utility programs necessary to perform interpretation maintenance to properly utilize backup appropriate data sets and application programs. The ORACLE data base product, which is currently being tested by the Data Center, will pass all Top Security reviews before final implementation is made on the network or mainframe. The results will enable Data Center customers with ORACLE-based systems to acquire information on the Data Center network and mainframe.

Recommendation No. 6c

The Data Center should ensure that:

All Data Center and customer disaster recovery personnel periodically update the vital records portion of the REXSYS Disaster Recovery database.

Its customers obtain a proper software utility program to perform interpretation maintenance to backup appropriate data sets and application programs that will be stored offsite.

Data Center Response

The Data Center agrees with this recommendation. The Data Center staff is expected to provide updates to the vital records portion of the Disaster Recovery Database.

The Data Center will establish adequate backup, recovery and security procedures before releasing the software gateway product.

Adaptable Database Automated

Data Center customers use different types of computer languages to access their data from the mainframe. Manual updates of the computer language software are presently being performed by the Data Center to ensure that all agencies are able to retrieve their data at various versions of their unique software. Backup procedures are equally being performed manually by the Data Center's personnel. The backup procedures relating to the Data Center and customer adaptable database resources are not fully automated and are subject to human error which could adversely affect Data Center customers. Changing the procedures of the customer adaptable database, to allow automation within the program, will minimize human error and reduce time.

Recommendation No. 6d

In order that all agencies gain full access to their data and that the Data Center may better service the needs of their customers, the Data Center should modify backup procedures relating to the Data Center and customer adaptable database resources so that they are fully automated.

Data Center Response

The Data Center agrees with this recommendation and is currently implemented. The Data Center believes that the backup process is already at a secure and effective level.

Printer Production

Presently, the Data Center looks at solutions to printer problems after the problem occurs. With the level of limited service from Xerox (vendor for the Data Center's printers), the Data Center should acquire a Service Plan that details a solution-oriented approach in resolving problems. This approach will ultimately increase value to the Data Center's customers and streamline production. A Service Plan was requested from Xerox in June 1999, but has not been received by the Data Center's management team. This Service Plan will be used to minimize down-time, increase productivity, and further give the Data Center a selection of solutions as printer problems arise out of the ongoing issues from the new/backup printer implementations. The Service Plan should also indicate all alternative costs associated with upgrades, the time frame for implementation, and a cost-benefit impact analysis.

Recommendation No. 6e

The Data Center should determine the most cost-effective method for a back-up printing capability to ensure that customer service interruptions are minimized. The Data Center should communicate the service needs with the vendor and implement any recommendations that arise from the *Printer Service Plan*.

Data Center Response

The Data Center agrees with this recommendation. The redundant printers are now in full production offering on-site back up printing ability. The delayed service response during conversion to the printers has all been rectified. The Data Center will work with Xerox to acquire a *Printer Service Plan*.

PROTECTION OF BACKUP AND DISASTER RECOVERY TAPES, AND ACCESS TO THE OFFSITE BACKUP TAPE VAULT FACILITY

In cooperation with the Department of Revenue (DOR), the Data Center maintains an offsite backup tape vault facility in the DOR Building at 1375 Sherman Street in Denver. The facility is used to store backup tapes for normal Data Center maintenance and to ensure that operations may be recovered in the event of a disaster.

Inside the vault facility is a large DOR power supply system, which if it were to over-heat or explode would cause damage to the tapes. Due to the sensitivity and critical nature of back-up and disaster recovery tape resources, the Data Center and DOR should work together to prevent any and all potential security risks.

During our audit, we visited the tape vault facility and noted the following matters:

- The environmental conditions at the vault facility, which include a DOR power supply unit, may not be appropriate for the storage of backup and disaster recovery tapes. For example,

the power supply unit is located next to the backup tapes, which could be prone to explosion or fire. We observed an air conditioning system that operates with a powerful fan unit that exposes tapes to excessive blowing dust, and a basement location susceptible to flooding.

- The list of personnel with authorized access to the tape vault facility did not reflect the most recent Data Center personnel changes. According to standard operating procedure, entry into the facility should be allowed only with formal permission.

Recommendation No. 7

The Data Center should:

- Perform a comprehensive analysis to identify an offsite tape vault facility that provides appropriate environmental, safety, and security features and then consider the cost/benefit of relocating the existing tape vault facility, especially the Data Center's Disaster Recovery tapes. If possible, the tape vault facility should only be staffed by Data Center personnel. See Fiscal Year 1998 Recommendation No. 9.
- Properly maintain the authorized personnel list. Any personnel not on the list should not be given access into the tape vault facility. (Standard Operating Procedure # 3000) See Fiscal Year 1998 Recommendation No. 9.

Data Center Response

The Data Center agrees with this recommendation. The Data Center agrees with the benefit of a comprehensive analysis of the offsite tape facility and that only designated personnel should be given access. The Data Center will work with the Department of Revenue to address findings from the comprehensive analysis. The Data Center does not have sufficient staff to support the off site location.

BUILDING SECURITY AND SAFETY

The Data Center and the Colorado Bureau of Investigation, a division of the Department of Public Safety, share the Dale Tooley State Office Building located at 690 Kipling Street in Lakewood. Since the Data Center and the Colorado Bureau of Investigation handle sensitive information and maintain valuable records, building security and safety are critical.

During our audit, we inspected building security and safety features, and fire prevention systems and noted the following matters:

- Safety meetings have been held only on an as needed basis.
- Adequate fire prevention systems appear to be in place at the Data Center. However, adequate written evidence (certificates of inspection filed centrally) does not exist to substantiate that all fire prevention systems (the FM 200 and Halon 1301 systems) have been inspected on a regular basis as established by the contracted vendor.
- Fire escape maps were not strategically located throughout the Dale Tooley State Office Building.

Recommendation No. 8

The Data Center should instruct its Safety Committee to:

- Continue to address safety and non-safety issues on a regular basis and routinely schedule more proactive safety meetings with the Data Center's Administration, to increase awareness and decrease incidents.
- Maintain adequate written evidence (certificates of inspection) in an administrative file to verify that all fire prevention systems are inspected on a regular basis.
- Draft a schematic for each floor plan for proper fire escape routes, and place such maps throughout the facility at 690 Kipling Street.

Data Center Response

The Data Center agrees with this recommendation. The Safety Committee will continue to act on a proactive basis in the spirit of increasing awareness and decreasing incidents. Certifications of fire prevention equipment will be obtained from the inspecting agent and filed centrally. Floor Plan maps indicating fire escape routes will be posted.

Disposition of Prior Audit Recommendations
Fiscal Year Ended June 30, 1999

Following are Fiscal Year 1998 audit recommendations together with their disposition at June 30, 1999.

Recommendation	Disposition
1. Data Center management should:	
• Continuously review, identify, and address security and data integrity issues related to the Internet.	• Implemented
• Conduct a security vulnerability study to determine whether or not Internet Protocol Unique Addressing increases the risk of unauthorized access to protected state resources.	• Implemented
• Fully install the conditional access firewall.	• Partially Implemented (See Recommendation # 1)
2. Ensure that the reporting of task progress to the Information Management Committee reflects actual percentages of completion based on realistic estimates.	• Implemented
3a. Require all customers to use only locked and well-conditioned containers to transport magnetic tapes and other media.	• Implemented
3b. Implement a bar-coded environment for foreign tape volumes, or use high-speed data transmission lines to transmit customer transactions to eliminate handling of volumes.	• Not Implemented (See Recommendation # 2a)
4. Review current organizational structure and lines of authority to ensure that conflicts of interest do not exist and that the authority of the Change Manager is not compromised.	• Partially Implemented (See Recommendation # 3)
5a. Ensure that the software update required to update Adaptable Database software passwords is installed or that such passwords be updated immediately.	• Partially Implemented (See Recommendation # 4a)
5b. Review:	
• All personnel user IDs and Group Profiles.	• Partially Implemented (a)
• All automated production schedule access.	• Partially Implemented (a)
• The appropriateness of all Data Center and vendor personnel granted access to Top Secret Security console attributes.	• Partially Implemented (a)
• All Data Center Central, Divisional, and Departmental Security Administrator status to avoid or eliminate actual or potential conflicts of interest.	• Partially Implemented (a) (a) The Data Center has taken steps towards implementation.
5c.	
• Codify and merge Standards Operating Procedures #8808 and #8813, and its Top Secret Security Administration Policy, dated April 30, 1997.	• Implemented
• Review the Data Center Group Profile that permits the Data Center Technology Services Group to modify its security access in extreme emergencies and ensure that access to this Group Profile is restricted.	• Partially Implemented (b) (b) See Recommendation # 4d

Recommendation	Disposition
6a. • Consider discontinuing the Daily Activity History Report. • Alternatively, improve the cross-referencing of problems between both the InfoSys Problems Report and the Daily Activity History Report by using the Problem Management Application (PMA) 6b. Review the InfoSys change classes CHGMGR, TECHMGR, and SERVMGR and restrict authority to close/change records.	 • Implemented • Implemented • Implemented
7. Review and update the format and content of its annual Customer Satisfaction Survey and continue its distribution either on an annual or biannual basis.	• Implemented (See Recommendation # 5)
8a. Revise Standard Operating Procedure #6717 to require quarterly physical backup and disaster recovery tape inventories. 8b. Encourage: • All Data Center and customer disaster recovery personnel to cooperate with the Data Center's Disaster Recovery Team to periodically update the vital records portion of the REXSYS Disaster Recovery database. • Customers to obtain the proper software utility programs necessary to perform catalog maintenance to backup appropriate data sets and application programs to be stored offsite. • Customers to develop a plan to share one of the two standby, high-speed communication lines connecting the Hot Site with the planned Denver metro area command center. 8c. Review and modify backup procedures relating to Data Center and customer adaptable data base resources so that they are fully automated. 8d. Work with the: • Telecommunications Section to develop a formal Disaster Recovery Plan. • Departments of Revenue and Labor and Employment to explore methods of compatible backup printing.	• Implemented • Not Implemented (See Recommendation # 6c) • Partially Implemented (See Recommendation # 6c) • Not Implemented (See Recommendation # 6a) • Not Implemented (See Recommendation # 6d) • Partially Implemented (See Recommendation #6a) • Partially Implemented (See Recommendation # 6e)
9. • Perform a comprehensive analysis to identify an offsite tape vault facility that contains appropriate environmental, safety and security features and consider relocating the existing facility. • Revise Standard Operating Procedure #3000 to include a provision that requires regular update of the list of personnel who have authorized access to the tape vault facility. • Ensure that the tape vault facility's fire prevention system is inspected and tested on a regular basis.	 • Not Implemented (See Recommendation # 7) • Partially Implemented (See Recommendation # 7) • Implemented
10. Instruct the Safety Committee to: • Ensure that all fire containment or prevention systems are regularly inspected and maintained. • Update or revise the Emergency Evacuation Plan.	 • Partially Implemented (c) • Not Implemented (c) (c) See Recommendation # 8

APPENDIX A

Colorado Information Technology Services Data Center's Description and Control Objectives

Overview of Operations

Organization and Management

The Colorado Information Technology Services (CITS) Data Center was established as a division of the Department of Administration on July 1, 1978, as a service organization, to deliver data processing services to various governmental entities. Prior to that date, the Division of Automated Data Processing (ADP) was responsible for both the oversight of statewide data processing and the operation of a computer center. This dual responsibility, in effect, required the Division of ADP to oversee itself, and this provided the motivation for the separation of the functions organizationally.

Today the CITS Data Center is the result of the consolidation of several data centers over the last 21 years.

- 1978 - The Division of ADP's computer center and the Department of Social Services' computer center merged to create the General Government Computer Center (GGCC).
- Late 1978 - The Legislature mandated that the Colorado Judicial Department computer center be consolidated into the GGCC.
- 1986 - GGCC was established as a statutory-defined agency (CRS 24-30-16).
- 1988 - The Department of Revenue and the Department of Labor and Employment computer centers consolidated into the GGCC.
- 1994 - The Information Systems Group, a section within GGCC was transferred to the Executive Director of the Department of Administration.
- 1995 - The Department of Personnel and the Department of Administration were merged by HB 95-1362 to form the Department of Personnel / General Support Services. The GGCC was a division of that Department.
- 1996 - GGCC, along with three other Divisions – Archives, Telecommunications, and the Statewide Application Software Support – consolidated to form a new division called the Colorado Information Technology Services (CITS). This organization officially became effective July 1, 1996.
- In fiscal year 1997-98, the CITS Computer Center changed its name to the CITS Data Center to encompass the non-mainframe aspects of the services it provides.
- In Fiscal Year 1998-1999, the Pueblo Data Entry Center reporting relationship changed from reporting to the Data Center Manager to the Business Services Manager. This change retains the Pueblo Data Entry Center within CITS, but removes it from the Data Center.

Mission

The mission of the CITS Data Center is to efficiently, effectively, and economically provide quality information products and services to meet customer program objectives.

Services Provided

Services performed for state agencies include converting data to computer-usable form, computer processing, maintaining system software, processing of computer output, partnering with the Telecommunication Services section of CITS to provide a statewide telecommunications network, and ensuring that the computer system can be recovered in the event of a disaster to the Data Center.

Although the basic mission and objectives of the CITS Data Center have not changed, the overall philosophy pertaining to the use of the computer system has evolved since the creation of GGCC. There has been a noticeable change in the types of services requested by CITS Data Center customers. Traditional batch processing, where input is turned over to the CITS Data Center for scheduling and running of jobs with later return of output to the customer, has predominately given way to real-time processing. In real-time processing, users have remote, instant access to the computer through terminals connected to the CITS Data Center's computer via telecommunications lines. This change to real-time processing places a greater demand on the computer system.

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 CITS 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 CITS Data Center expand its services beyond the realm of mainframe processing. They suggest the CITS 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 CITS Data Center on an as-needed basis to provide application programming support, PC help desk support, training, and new technology expertise.

A Customer Roundtable (CR) with representatives from all customers, meets monthly at the Data Center. During this meeting, the roundtable reviews the past performance of the Data Center and provides recommendations on how the Data Center might better serve its customers. The roundtable serves as a major communication tool between the Data Center and its customers'

technical staff. However, it is not a decision-making body.

A Customer Management Council (CMC), with representatives from all agencies, was formed in 1990. The CMC's mission was to act as the former GGCC's management guidance group who, in participation with GGCC, determined the strategic direction and governing procedures of the GGCC in support of the selection and delivery of quality services and products. Since the inception of CITS, the CMC has disbanded, and its function has been replaced by the Chief Information Officer's (CIO) Forum. The CIO Forum meets regularly, and periodically establishes subcommittees to review specific technology areas. These subcommittees make recommendations to the CIO Forum, and as appropriate, to the Commission on Information Management.

While both the CR and the CIO Forum provide guidance to the CITS Data Center, the Manager of the Data Center is charged with making decisions which can impact multiple users and with assuring that resources are equitably allocated. The general organization chart of the CITS Data Center is shown on page 35.

The CITS Data Center has 70 full-time equivalent (FTE) staff predominately located at the Data Center, including a portion of the Business and Administrative Services Unit. The 38 FTE from the Pueblo Data Entry Center, reported in previous years, are no longer included due to the reporting relationship change discussed earlier. The Data Center personnel allocation follows:

Functions	Number of Staff
Manager	1
Business & Administrative Services	5
Customer Support Services	17
Technical Services	21
Computer Operations	26
Total	70

In general, personnel are restricted from direct or indirect control over assets and do not have authority to disburse funds, originate transactions, or perform incompatible accounting functions. CITS Data Center personnel typically do not perform more than one function indicated above and generally have no overlapping duties or responsibilities at the Data Center or user agencies.

The CITS Data Center organization supports the following functions:

Business and Administrative Services - The Business and Administrative Services section, as part of their CITS-wide services, provides support services required to operate the Data Center. Responsibilities include budget preparation, control, and monitoring. The section is also responsible for processing internal accounting, providing personnel interface and reporting, word

processing support, switchboard support, and receptionist support for the entire building at 690 Kipling. In addition, the section acts as the building maintenance and security liaison.

Customer Support Services – In Fiscal Year 1993, the Service Delivery section changed its name to Customer Support Services to better reflect the emphasis on providing customer support. The section has the responsibility for handling customer service requests. Ongoing production service requests and problem reporting are addressed through this units 24' x 7' Service Center. Additionally, the Customer Support Services section provides very limited analytical and programming support to state agencies. Master Security Administration routine functions are performed by this section, but are administered by the Disaster Recovery team.

As the Change Manager, the Customer Support Services Manager or his/her designee provides change management for all changes to the CITS Data Center environment. Changes are reviewed prior to implementation to ensure proper notification is given to the customer base. Changes are again reviewed at completion to assess customer satisfaction in the Data Center's handling of the change. Computer-based training is also monitored by this section.

Technical Services - Responsibility for the installation and maintenance of all computer systems software resides in the Technical Services section. This section provides database administration support for all shared databases and supports database activity as requested for dedicated databases. All hardware and software evaluations are performed by the Technical Services staff. In addition, the group provides technical training and documentation for all CITS Data Center customers.

The Resource Management unit within Technical Services generates internal management reports on utilization, system performance, and billing. The Technical Services staff provides 24 hours per day, seven days per week support for system software.

Operations - Operations consist of the Data Center's computer operations unit and the Disaster Recovery unit. Responsibilities include installing and operating computer and printing equipment, maintaining disk and tape systems, and the control and distribution of computer output. As the Problem Manager, the Operations Manager or his/her designee ensures all system problems are handled in a timely and proper manner. This unit is responsible for the development, implementation, and monitoring of the Data Center's disaster recovery plan, and for disaster recovery coordination.

The Data Center operates 24 hours per day, 7 days per week including holidays and is staffed accordingly by the Operations section.

Network Services Group

With the formation of CITS, the Network Services Group is now managed by the CITS Telecommunication Services section. The Data Center maintains a strong and close working relationship with the Network Services staff via the Service Center, project planning, and the problem and change management process. The telecommunications functions include providing problem diagnosis, tuning, and modifications to the communications network

Internet Access

The CITS Data Center currently provides a T-1 speed (1.5 Mbps) connection to the Internet for customers that subscribe to the Colorado Information Network (CIN). This connection is available for customers to use without restriction on traffic, or service accessibility for sessions originating on the CIN and directed out to the Internet. Traffic from the Internet to the CIN, however, is severely restricted or firewalled. In order to protect State computing resources attached to the CIN, which is defined as a "private" network, CITS does not allow *any* inbound traffic from the Internet, except for electronic mail transmission, domain name service (DNS) queries, and unique Internet Protocol (IP) addressing.

CITS enforces an Internet access policy within CITS only. Employees wanting access to Internet e-mail and standard Internet services (web, ftp, etc.) must complete an "Employee Access Authorization" form, signed by the employee, the immediate supervisor, and the Manager of the appropriate CITS section.

This form states: "… to provide access for the benefits of information exchange necessary to the business of Colorado State Government. It is the responsibility of all State Employees who use the resources of the Internet to use them in the beneficial interest of their agency and the citizens of Colorado. Any other use of this resource is considered contrary to the intent of this access service, and will warrant disciplinary or corrective action."

CITS has recommended that a similar policy statement be published for other Divisions within General Support Services, as well as other departments.

Hardware and System Software

In October 1998 the Data Center replaced its Hitachi Data Systems 8624 computer with a Amdahl Millenium 775 with a MIPS capacity rating of 446 million instructions per second. Computer processing operates on a 24-hour, 7-day per week schedule.

All application systems are processed on the computer under the control of an IBM OS/390 (MVS/ESA) operating system. The computer is configured with one billion bytes (1 GB) of memory plus one billion bytes (1 GB) of extended memory, 1158 billion bytes (GB) of on-line disk storage, and 56 tape drives (32 of which are virtual). Telecommunications software is IBM's Time Sharing Option (TSO) and Customer Information Control System (CICS), which support approximately 12,000 terminals located throughout the State.

Other major system software used on the computer and contributing to an efficient and secure environment includes:

- JES3, a product whose function is to receive jobs into the system, process their resource requirements, schedule their execution, and direct their output.
- PANVALET, a source library maintenance system that provides:
  - The ability to establish, maintain, and protect a central library of source programs, object programs, documentation, job control language, and data files.
  - The assurance that the latest version of a library member is processed by assigning an initial version number and incrementing it each time the member is modified.

- TOP SECRET, a state-of-the-art access-control software security package. Top Secret protects access to system facilities by requiring that users be explicitly authorized to use the facility; it also controls which resources can be used and which data sets may be accessed or modified.
- ASM2, an integrated disk storage management system which provides:
  - Simplified data management and controls.
  - Extensive exception reporting tools.
  - Independent subsystem functions.
  - Centralized approach to physical device management.
- CA1, a tape management system (TMS) which provides the Center and its users with:
  - Comprehensive tape information.
  - Reduced human effort to operate the computer system.
  - Increased efficiency throughout by reducing program work time.
  - Data protection.
  - Capability to handle non-labeled tapes.
- MICS, which provides the Data Center management with a cost accounting and resource utilization system that includes total resource accounting, unit reporting, and job costing.
- CA7, an automated production scheduling package that also minimizes human effort to operate the computer system.

Operations

The Operations, Service Center, and Data Control units have the responsibility of ensuring the timely and accurate operation of applications, from receipt of input data from the various sources through distribution of output for agencies using the CITS Data Center's scheduling and printing services.

Various data tapes for input to customer applications also arrive at the Data Center by mail and by courier. In addition, some agencies enter data by teleprocessing it directly to the Data Center, either for real-time applications or for batch processing. Job Control Language (JCL) statements for production jobs are organized into JES3 networks and CA7 schedules, which ensure that jobs are executed in the correct sequence.

Schedulers designate the particular networks needed for each cycle and update control statements with the dates, parameters, etc., needed to run the batch jobs. The finalized schedule is submitted for execution and printed on hard copy. The hard copy becomes the control and tracking mechanism used to ensure that all production batch jobs are addressed. However, not all jobs are scheduled through these procedures. Any authorized customer of the CITS Data Center may submit a production job.

Output reports are usually spooled to disk and tape units during the processing cycle and are printed after processing is completed. Some output is sent directly to remote printers. Copies of the daily console log are kept on file for one month and are reviewed by appropriate personnel for operational questions or problems that arise at a later time. Job run output, including JCL and allocation and completion messages, is available through TSO after jobs are completed. Customers are charged with reviewing this output daily. If a problem occurs, this output is printed on hard copy to aid in problem resolution. The output is generally not saved but can be retrieved from tape files if needed.

Operating instructions for systems scheduled by the CITS Data Center are maintained in the Operations, Scheduling, and Data Control areas in loose-leaf binders. The instructions include the following types of information.

- Program identification data
- Preceding program identification
- Formal run instructions
- Operator messages
- Output form requirements
- Control statement requirements
- Input/output distribution instructions

Operators are responsible for monitoring system performance and for identification of abnormal conditions. They generally do not know what tapes are to be mounted (except by number) or any other information about the processes executed. This provides security from operators improperly manipulating jobs. However, as a result, Operators cannot act in a control capacity to prevent errors in job control or data control information.

If a system fails, Operators refer the problem to the Scheduler. The Scheduler checks the job instructions to see if anyone is on call for that job. If an individual is on call, the problem is referred to that person for immediate resolution. If not, no further action is taken, and output from the failed job is delivered through the normal delivery procedures. The Scheduler coordinates failure resolution and restarts the failed job as directed by the customer/programmer. Customer application system maintenance programmers may take a dial-up terminal home to correct job control language problems and minor program problems for the systems they support. No one single Operator is assigned to any one application. Therefore, the responsibility for running the systems rotates among different operators.

Hard-copy output from jobs is generally printed on a Storage Technology impact or Xerox laser printers. Output is then routed to data control where it is reviewed for neatness and alignment, checked against customer requests, boxed by customer destination, and logged for courier pickup. The courier signs for the documents when the pickup is made and also obtains a signature from the customer agency upon delivery.

Several positive control measures are exercised over Data Center access. These measures have been designed to enhance the security of the Data Center and to reduce the chance of loss of hardware and computer files. Controls include the following:

- The building is always locked.
- The receptionist is on duty from 7:30 a.m. to 4:30 p.m. All visitors entering the building must sign in, wear a color-coded badge to gain authorization to visit specific areas, and be escorted to those particular areas.
- Access to the computer room is controlled by cipher combination locks. The locks are changed when personnel terminate or transfer.

Backup and Recovery

The system packs, containing the files required to initialize the system and establish the Data Center operating environment, are backed up on a daily basis. Backup data tapes are retained as specified by customers. Backup tape copies are kept in vaults off-site. External labels on the tapes identify them by number only and contain no written identification as to tape contents. Consequently, the Tape Management System index listing is required in order to identify the contents of any tape volume.

Disk data, other than the customer-requested files indicated above, are copied to tape and stored on a predetermined schedule as follows:

- Disk packs are backed up weekly as part of the off-line processing cycle.
- Some system data sets are backed up to tape daily.
- PANVALET source program libraries are backed up daily.
- Operating systems and program files are backed up daily.
- Databases for which the CITS Data Center staff functions as the Database Administrator are backed up once per workday and once per weekend.

All of these backup tape copies are stored at an off-site storage location.

Halon 1301 and FM200 fire control systems, as well as heat and smoke detectors, are installed in the computer room.

All equipment is under preventive maintenance contract.

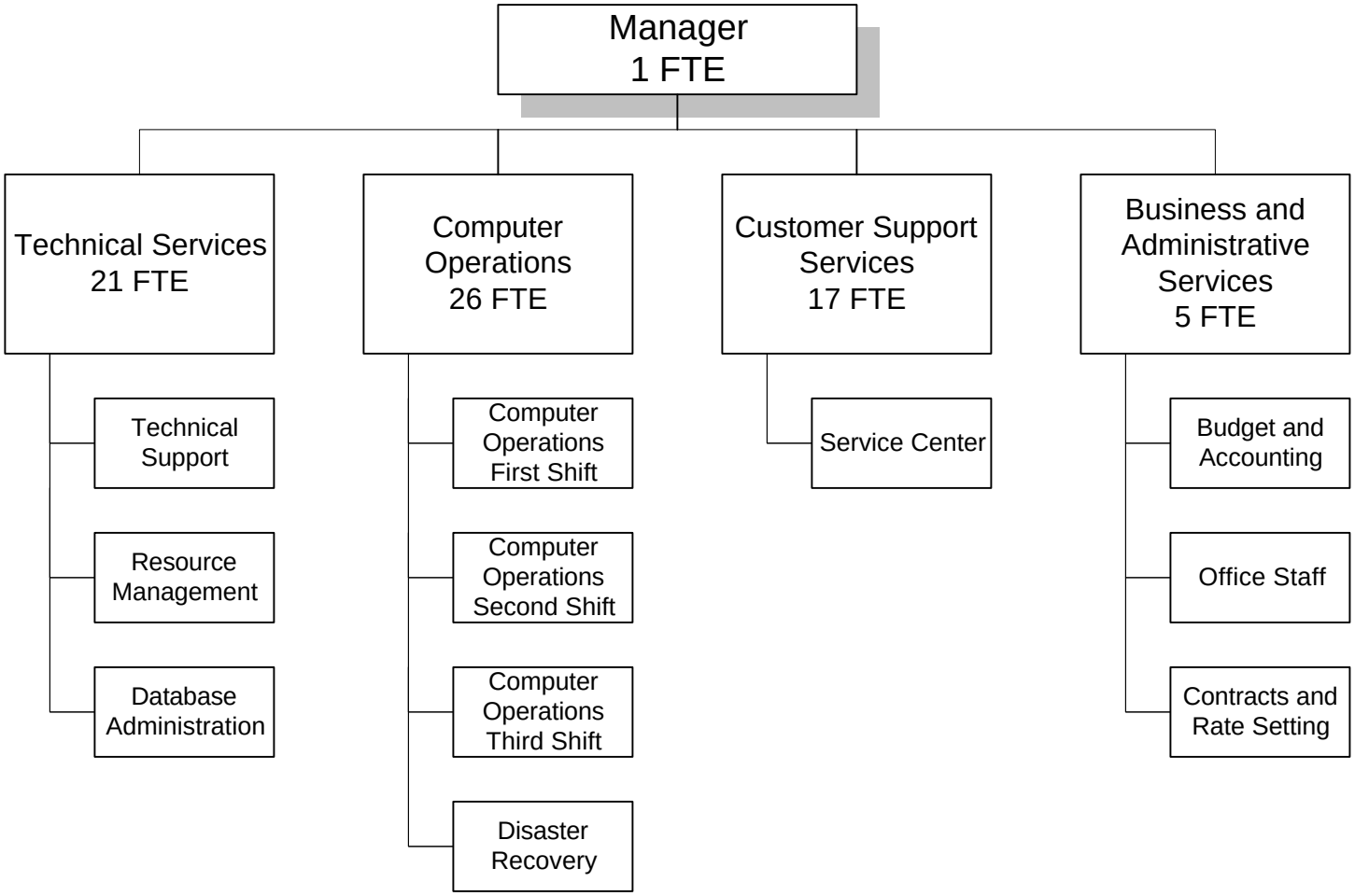
In the event of a power outage, an Uninterruptible Power Supply (UPS), that utilizes batteries and a generator, will support the mission-critical hardware configuration. This equipment also allows continuing operation of the computer in the event of a major power failure. The UPS is maintained by Physical Plant Maintenance personnel, who have been provided instructions for its use.

In the event of a disaster affecting the Data Center, a Disaster Recovery Plan has been developed to recover Data Center operations at a remote “Hot Site,” including the migration to a “Cold Site” and a new “Home Site,” if needed.

Colorado Information Technology Services Data Center

ORGANIZATION CHART

FISCAL YEAR 1999



APPENDIX B

Interdependent (General) Control Procedures

Interdependent controls apply to all computer-related activities, and they are considered basic to the effectiveness of specific application controls. Various categories of interdependent controls are discussed below in terms of control objectives and are followed by descriptions of control procedures employed by the Colorado Information Technology Services (CITS) Data Center to assist in obtaining the indicated objective.

Organization and Management

1. Objective: Definition and Communication of Responsibilities (authorization objective)

What techniques are used to define and communicate the CITS Data Center organizational structure, policies, and procedures that will provide reasonable assurance that CITS Data Center personnel perform their duties correctly and that procedures and controls will be followed?

Controls

The management team meets weekly to discuss the prior week's performance. Abnormal situations are discussed and corrective actions identified.

- As illustrated on page 35, an organization chart is published and kept current.
- Formal job descriptions exist and are kept current.
- Standards and operating procedure manuals exist and are used by CITS Data Center personnel.
- Adequate supervision and approval levels exist in each functional area at the CITS Data Center.
- A performance appraisal system is employed to relate performance to objectives.
- Data Center staff meetings are held as necessary. These meetings have an open forum, and all changes to the organization are presented.

2. Objective: Segregation of Incompatible Duties (physical safeguard objective)

To what extent does the organization of the CITS Data Center provide for segregation of incompatible duties?

Controls

- Operators are prohibited from making changes to production programs.
- Operators and data entry personnel are not allowed to make corrections to erroneous source input data.
- Programmers and system analysts are not permitted to operate the computer.
- The scheduling and data control function is not performed by computer operators except

during staff vacancies requiring temporary assignment of data control duties to computer operators.

- Master Security Administration is not performed by the Technical Support staff. Disaster Recovery Services has assumed responsibility for this function.
- CITS Data Center personnel have no duties in customer operations and take no responsibility for controls maintained by customers.
- Personnel take regular vacations.

The Customer Services Manager is at a comparable level to the Operations Manager and Technical Support Manager and reports directly to the Data Center Manager. The Customer Services Manager, or his/her designee, functions as the Change Manager. The Operations Manager, or his/her designee, functions as the Problem Manager.

Computer Operations

3. Objective: Formal Operations Procedures (authorization objective)

What techniques are used to provide reasonable assurance that the computer is used only for authorized purposes and that operators are following prescribed procedures?

Controls

- Scheduling and submission of computer application jobs are normally controlled by separate personnel from the Computer Operators.
- Automated operation of the computer through system software minimizes the actions required from an operator in processing an application.
- Batch jobs are processed based on a predetermined schedule; schedulers check off jobs on the schedule as they are completed.
- Access to scheduling files is restricted to scheduling personnel by means of security software.
- All users of the computer system must be authorized under Top Secret Security software by either the customer's Security Administrator or the Data Center Master Security Administrator.

4. Objective: Supervision and Review of Operations (authorization objective)

Are supervision and review of operations sufficient to provide reasonable assurance that the computer is used only for authorized purposes and that operators are following prescribed procedures?

Controls

- All operator activities are recorded by Top Secret Security software logging functions on the console log and System Monitoring Facility.
- Exceptions to normal operations are reported by operators on a dictaphone and published for management review on a Daily Activity History Report.

5. Objective: Restricted Access to Computer Operations (physical safeguard objective)

What techniques are used to provide reasonable assurance that access to computer operations is limited to authorized personnel?

Controls

- There are written policies concerning who is authorized access to the computer operations area.
- Locked doors, operated by electric combination systems, are used to restrict access to the operations area.
- Access to the Data Center is controlled through the use of a reception log, badges, escorting of visitors, television monitors, and electric combination locks.

Systems Software Support

6. Objective: Authorization and Approval of Modifications to Systems Software (authorization objective)

What techniques are used to provide reasonable assurance that all modifications to system software are properly authorized, approved, and tested?

Controls

- A formal change management system is used to control and document changes to system software.
- There is thorough planning, supervision, documentation, and testing of all changes in system software.
- There is a formal software product installation process.

7. Objective: Restricted Access to System Software (physical safeguard objective)

Is access to system software and the related documentation restricted to authorized personnel?

Controls

- System software access is restricted to authorized system programmers at the CITS Data Center by use of security software. Security access authorization tables are secured against changes or access by unauthorized personnel.
- System programmers are not allowed to operate the computer.
- System programs that allow bypassing of normal systems or application controls (e.g., Super Zap) are security-software protected and are used infrequently.
- Application program documentation is located with the users and is not available to system programmers without owner approval.

8. Objective: Quality of System Software and Related Documentation (authorization objective)

Is the quality of system software considered before purchase, and is the documentation adequate?

Controls

- System software has been obtained from reliable software developers.
- System software has not needed extensive modification.
- Documentation of system software is complete and is kept current.

Data Entry

9. Objective: Acceptance of Approved Input (transaction processing objective)

What techniques are used to provide reasonable assurance that only approved input is accepted by the CITS Data Center for processing and that all approved input has been received?

Controls

- A data control function reviews input data for user approval and logs all input physically received at the Data Center.
- Operators process only input received from the data control function.

10. Objective: Restricted Access to Data (physical safeguard objective)

What procedures does the CITS Data Center have in place to restrict physical access to data to authorized persons?

Controls

- The data control section controls all physical input received until submitted to operations.
- Tape files are located in restricted-access computer rooms and are under the control of automated library software. CITS Data Center tape volumes require external labels that do not indicate the nature of the data contained in the volumes.
- Computer output and the distribution thereof are under strict control of the data control function and of the Department of Administration couriers. Logs of output received from operations are maintained.
- Blank warrants, signature software, and signed warrants are controlled and secured. Blank warrants and signature software are kept in locked storage except during processing. All warrant numbers are accounted for. Warrants are transported in sealed containers.
- During processing, computer operators compare the warrant numbers printed against the preprinted warrant numbers. Computer operators record the beginning and ending warrant numbers on a control form. Data Control matches the warrants received and processed in Data Control to the control form completed by computer operators. A control log is kept for signed warrants released to an authorized courier who must also sign for them.
- MICR printed warrants (Accounts Payable) are now printed by the Xerox 96NPS Laser printer. The fonts needed to print these warrants are locked in the filing cabinet in the

locked storage room and must be signed for by the operator. Control procedures include the preparation of a sample document to ensure that signature and MICR lines are present. For additional information see the Warrant Printing on Xerox Laser 96NPS MICR Printer control procedures in the computer operations area.

Backup and Off-Site Storage of Data Files and Programs

11. Objective: Backup of Key Data and Programs (physical safeguard objective)

To what extent have data and programs been duplicated or stored?

Controls

- Critical disk packs are duplicated weekly.
- System data sets and catalogs are duplicated to tape daily.
- Source program libraries are duplicated daily.
- Data sets on storage packs, which have had additions or modifications, are backed-up daily using automatic storage management system software (ASM2).
- Databases for which CITS Data Center staff functions as the Database Administrator are backed up to tape once per workday and once per weekend.
- All duplicated data are stored off-site.
- Access to the off-site backup files is restricted to authorized personnel.
- Recovery and restart procedures exist and are used on a recurring basis.

APPENDIX C

Control Considerations for User Agency Auditors
Fiscal Year Ended June 30, 1999

The internal controls at the Colorado Information Technology Services Data Center (Data Center), are audited annually in compliance with the Statement on Auditing Standards Number 70, Report on the Processing of Transactions by Service Organizations. The annual audit includes a review of general controls at the Data Center.

Many state agencies use the Data Center mainframe computer system to run their electronic data processing (EDP) applications. The Data Center receives input from the state agencies, processes the related data, and generates reports and other output which are distributed according to agency instructions. The control procedures at the Data Center interact with those at state agencies to protect data, systems, and programs from loss or unauthorized access.

Our audit objectives do not include a review of application controls over user applications. Auditors of user agencies are responsible for reviewing user agency application controls. For example, Departments, such as Human Services, Revenue, and Labor and Employment, are responsible for developing and implementing application controls over their own applications. Auditors of these agencies are responsible for testing compliance with these controls.

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. This appendix also provides examples of specific control considerations that auditors of user agencies should include in their reviews of agency internal controls.

DATA CENTER GENERAL CONTROLS

General or interdependent controls apply to all computer-related activities and are considered basic to the effectiveness of specific application controls. The Data Center audit included a review of general controls and the techniques used to meet control objectives. The following are the general controls in place at the Data Center:

- Organization and management.
- Computer operations.
- Systems software support.
- Backup and off-site storage of data files and programs.

The specific control objectives and techniques that the Data Center has identified for each of the areas listed above and which we tested can be found in Appendix B.

AGENCY GENERAL CONTROLS

General controls at the Data Center interact with general controls at user agencies. This is helpful to auditors of user agencies because auditors can rely on certain general controls as a result of the Data Center audit. Specifically, user auditors can rely on the Data Center's general controls over the following areas:

- Computer operations.
- Operating system software support.
- Disaster recovery procedures for the operating system.
- Centralized data control, if the user agency subscribes to this service.

Auditors of user agencies must review all other general controls at the agency level.

APPLICATION CONTROLS OVER COLORADO PERSONNEL PAYROLL SYSTEM

When reviewing an agency's control environment, the auditor should review the agency's controls over the use of its application 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 EDP auditing performed at the agency and the organization and management of the agency EDP department.

SECURITY AND ACCESS

Auditors should review the agency's use of TOP SECRET and any other security software available to the agency. These include the Colorado Personnel Payroll System Transaction Application Processing System and the security systems relating to the ADABAS data management system and NATURAL programming language. 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 log-on attempts or unauthorized access attempts allowed before a user is locked out.
  - The automatic disconnect time limits for unused terminals.

Logical Access Controls:

- Review controls relating to the granting of access to resources. If an 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 has been 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. If an access identification has been granted access to the Colorado Personnel Payroll System, confirm that in addition to the above-described notifications, procedures have been established to notify the Security Administrator at Accounts and Control.
- Determine how the agency Data Base Coordinator administers ADABAS file passwords and NATURAL user identifications to control access to ADABAS and NATURAL resources. Confirm that passwords are changed annually, not hard-coded within source programs and that access to password files is controlled.

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.
- Confirm that the Agency Security Administrator or the agency personnel/payroll manager reviews the Colorado Personnel Payroll System Transaction Applications Processing System security access and violation log on a daily 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.

- Determine if the agency provides instructions to the Pueblo Data Entry Center, which addresses key verification requirements and data validation needs for the application. This step is necessary only for agencies using Pueblo Data Entry Center data entry services.

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 reasonableness and mathematical accuracy.
  - Confirm that management reviews Payroll Audit Reports and labor distribution reports prior to each pay day.
  - Look for segregation of duties between employees who initiate payroll records and those who receive and distribute payroll advices. This should be reviewed carefully in agencies where the payroll and personnel functions are combined.
  - 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 backups.
- 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.

Distribution

Copies of this report have been distributed to:

Legislative Audit Committee (12)

Colorado Information Technology Services (10)

Joint Budget Committee (3)

Department of Personnel
d.b.a. General Support Services
Executive Director (2)
State Comtroller (2)

Honorable Bill Owens, Governor

Office of State Planning and Budgeting (2)

Depository Center, Colorado State Library (4)

Joint Legislative Library (6)

State Archivist (permanent copy)

National Conference of State Legislatures

Legislative Legal Services

Auraria Library

Colorado State University Library

Copies of the report summary have been distributed to:

Members of the National Legislative Program Evaluation Society

Members of the Colorado General Assembly

National Association of State Auditors, Comptrollers and Treasurers

Report Control Number 1182