PERFORMANCE AUDIT

STATE DATA CENTER
COMPREHENSIVE CONTINUITY PLANNING AND
MAINFRAME SECURITY ADMINISTRATION

From The Office Of State Auditor
Claire McCaskill

The State Data Center comprehensive continuity planning is not complete. Mainframe security weaknesses increase risk for unauthorized system use or modification.

Report No. 2003-113
November 26, 2003
www.auditor.state.mo.us

Office of
Missouri State Auditor
Claire McCaskill

November 2003

YELLOW SHEET

Comprehensive continuity plan for the State Data Center needs to address risks and responsibilities

This audit reviewed the State Data Center's comprehensive continuity plan and security administration. The Office of Administration, Division of Information Services established the State Data Center, which processes mainframe data, stores data, and backs up state data systems. Without a complete continuity plan, there is limited assurance information technology processing could be promptly resumed after a disaster or other disruptive event. Security control weaknesses put mainframe data at risk for unauthorized use or modification. The following highlights the findings:

Data center recovery plans missing key items

The comprehensive continuity plan is used to restore the state's operating system to recover critical state agency applications during a disaster. Auditors found some necessary information was not included in the recovery plan. Examples include: guidelines on how to use the plan; assumptions used for developing the plan; different procedures for various recovery scenarios from minor to total loss of processing capability; identification of the plan's limitations; an order of succession to follow for decisions; and procedures or objectives for testing the plan. (See page 3)

Plan lacks enough detail for data center recovery teams

Division officials' plans for two of the three recovery teams rely on the teams reacting to disasters without a detailed response plan, which could be detrimental to successful recovery. Standards state a detailed plan is necessary for recovery personnel who will respond, recover capabilities, and/or return the system to normal operation. These personnel need to clearly understand each step they are to execute and how their team relates to other teams. (See pages 4 and 5)

Access to the recovery plan has not been sufficiently restricted

Weaknesses in establishing access rights to the recovery plan allowed at least 1,000 OA employees to receive unnecessary plan access. Officials have not developed formal procedures to evaluate access rights to the confidential portion of the data center's disaster recovery plan. OA officials took immediate action to remove the unnecessary plan access. (See page 6)

Contract procedures for alternate facility are not adequate

The initial data center contract for an alternate facility, necessary in the event the data center cannot be used, was to have ended with fiscal year 1999 and was not re-bid until over two years later. Bids were then solicited for configuration settings that would not be used. (See page 7)

Mainframe and customer security control weaknesses increase risk

Management practices and the data center customer procedures manual do not provide sufficient computer security procedures for agencies, or require agency mainframe security to be monitored. At April 30, 2003, 38 percent of over 45,000 active data center IDs had some security weakness including: no password change interval, not accessed for more than 90 days or never accessed, and no assigned or associated user name. (See pages 10 and 11)

All audit reports are available on our website: www.auditor.state.mo.us

STATE DATA CENTER
COMPREHENSIVE CONTINUITY PLANNING AND
MAINFRAME SECURITY ADMINISTRATION

TABLE OF CONTENTS

CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden, Governor
and
Jacquelyn D. White, Commissioner
Office of Administration
Jefferson City, MO 65102

The State Auditor's Office audited the State Data Center's (data center) comprehensive continuity planning preparedness and administration of security controls for information and data stored on data center resources. The objectives of this audit were to evaluate if the Office of Administration's data center management had (1) defined and implemented a comprehensive continuity plan to recover state computer processing operations in case of a disaster or other unexpected interruptions and (2) established adequate administration procedures over security controls to ensure the integrity, confidentiality, and availability of data and information on the mainframe.

We concluded the current comprehensive continuity plan had several missing items and access to the confidential portions of the plan was not appropriately restricted. In addition, data center management needs to monitor agency system security as well as develop internal policies.

We conducted the audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such tests of the procedures and records as were considered appropriate under the circumstances.

Claire McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	William D. Miller, CIA
Assistant Director of Audits:	Jon Halwes, CPA, CGFM
Information Systems Audit Manager:	Jeff Thelen, CPA
In-Charge Auditor:	Tara Shah, CPA
Audit Staff:	Frank Verslues
	Lori Melton, CPA

224 State Capitol • Jefferson City, MO 65101

Truman State Office Building, Room 880 • Jefferson City, MO 65101 • (573) 751-4213 • FAX (573) 751-7984

RESULTS AND RECOMMENDATIONS

1. Comprehensive Continuity Plan Needs To Address Risks and Responsibilities

Although State Data Center (data center) officials have developed a comprehensive continuity plan, our audit noted a risk for disruptions still exist because officials have not:

- Identified and developed all necessary contents of a continuity plan and analyzed potential risks and threats.
- Adequately restricted access to the current comprehensive continuity plan.

The data center processes mainframe data, stores data, and backs up state data systems. Without a complete continuity plan, there is limited assurance information technology processing could be promptly resumed after a disaster or other disruptive event. Unnecessary access to the plan increases the risk of compromising data center operations. Since data center operations are crucial to state business operations, recovery preparedness must be as complete as possible. The plan's missing items resulted from data center officials being unable to identify standards specific to a mainframe environment and the lack of an overall recovery framework by the Office of Administration (OA). In addition, data center officials had not reviewed disaster plan access rights since it was developed.

Description of comprehensive continuity planning

An organization must take steps to ensure it is adequately prepared to cope with a loss of operational capability. An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information maintained electronically. Three main classes of events might affect an organization's ability to continue business operations: an unplanned incident or accident such as an explosion or fire, a natural disaster such as a tornado or earthquake, or a deliberate act.

An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity plan. Comprehensive continuity planning includes business continuity and information technology recovery. With business continuity planning, an organization is ensuring the availability of all business resources and supporting information technology necessary to continue/resume business processes. For information technology recovery planning, the organization is ensuring the availability of information technology resources required to support the continuity or recovery of business processes. A comprehensive continuity plan specifies emergency responses, backup operations, and restoration procedures to ensure the availability of critical resources and facilitate the continuity of operations. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a continuity plan should be periodically tested in disaster simulation exercises and employees should be trained and familiar with its use.

Criteria used to evaluate the data center's comprehensive continuity planning

No state regulations currently require agencies to develop, implement, and maintain a comprehensive continuity plan. However, federal, national and international comprehensive continuity planning standards exist. For our review of comprehensive continuity planning, we used accepted standards from the following sources:

- National Institute of Standards and Technology
- American Institute of Certified Public Accountants
- Canadian Institute of Chartered Accountants
- Information Systems Audit and Control Association
- United States General Accounting Office

The OA, Division of Information Services established the data center which provides: technical and operational support, network services, and information security management. The data center disaster recovery coordinator, who is developing the comprehensive continuity plan, is assigned to the Information Security Management Office, established in August 2001.

Standards state organizational policies should require a continuity planning framework to ensure consistency in continuity plans and inclusion of all necessary items in the plans. OA officials have not established an office-wide outline guiding division management to the general issues needed in the plan.[1] The framework should define the roles, responsibilities, and the risk-based approach/methodology to be adopted, the rules and structures to document the plan, and the approval procedures. *See Appendix II, page 17, for key terms and definitions used in the report.*

Recovery plans missing key items

The data center comprehensive continuity plan has a public access section and 10 confidential appendixes. The plan is applicable to the data center operations and how personnel plan to restore the state's operating system to support the recovery of critical state agency applications during a disaster. Audit results showed the plan does not include the following necessary data:

- Guidelines on how to use the plan.
- The assumptions used for developing the plan.
- Different procedures for various recovery scenarios from minor to total loss of processing capability.
- Identification of the plan's limitations. For example, a statement that the plan does not include evacuation procedures.
- An order of succession to follow for decisions.
- Procedures or objectives for testing the plan.
- Determination of team availability and organization of schedules.
- Detailed individual and team responsibilities.
- Salvage and media reclamation procedures.

[1] Reported in report number 2003-108, *Comprehensive Continuity Planning and Information Resource Security Management of the State's Accounting System (SAM II)* issued October 23, 2003.

- Restoration planning for the alternate site including plans for: hardware, software, connectivity, communications, security, and applications and support.
- Security and control requirements for operations when alternate processing methods and/or facilities are used.
- Procedures to clean the alternate site, especially of sensitive materials.

These missing items partially resulted from the OA not having a continuity planning framework. Data center officials also said they were unable to identify standards specific to a mainframe environment. Accepted national and international standards provide informative descriptions of items, such as those listed above, that need to be considered and documented in recovery planning for all types of systems including mainframes.

Standards also state criteria necessary to activate the plan should be clearly documented. The recovery coordinator has documented criteria which states, "in the event of a disaster, the SDC Disaster Recovery Plan will be initiated…" and has defined the term "disaster." The definition is a general listing of common disasters. However, the listing of disasters is so broad the disaster recovery plan would be initiated for unnecessary events, such as a general electrical power outage. This weakness suggests the criteria to activate the plan needs to be more detailed.

The plan does not provide enough detail for data center recovery teams to carry out their responsibilities.

Division officials' plans for two of the three recovery teams rely on the teams reacting to disasters without a detailed response plan which could be detrimental to successful recovery. The plan notes three recovery teams: disaster recovery management, administrative, and enterprise (which includes technical support, operations, and network operations units). These units will be responsible for reestablishing the operating system, connections, and a workable environment between the data center, users, and the alternative site. The disaster recovery coordinator explained detailed response plans will be developed for the enterprise team units but no response plans will be developed for the other two recovery teams. This can be problematic. As an example, the disaster recovery management team has to determine the degree of facility and/or computer equipment disability. Team members have no guidance on what procedures they are to perform or conclude. Standards call for detailed procedures for damage assessment. These procedures should include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of information technology equipment functionality and inventory, including items to be replaced; and estimated time to repair services to normal operations. Standards state any recovery personnel who will respond to the disaster event, recover capabilities, and/or return the system to normal operation need to clearly understand each step they are to execute and how their team relates to other teams.

Tolerable down time needs to be evaluated periodically

The timeline for obtaining and packaging off-site media, transporting it to the hotsite,[2] loading the tapes into the machine, and restoring the operating system is not based on specific agency outage limitations. Standards require management to determine a maximum tolerable outage time for critical business functions. In 2000, data center officials met with user agency representatives and presented different recovery options and the associated costs. According to data center officials, user agency representatives decided their operating system recovery preferences were not affordable and accepted the data center's current recovery plans for an outage period of up to 5 days. However, since these decisions were made 3 years ago, data center officials should evaluate the current customer requirements and assess risks to determine a tolerable outage time. This outage tolerance should be used in the planning process to meet customer needs.

Equipment replacement responsibilities and sources are not clear

The continuity plan's listing of all system hardware does not clearly state who is responsible for replacing damaged or destroyed hardware in a disaster. The listing includes hardware, which is owned by other state agencies. The coordinator explained this listing is to be used to ensure the environment of the data center can be reconstructed. However, he stated the data center would only be responsible for replacing hardware purchased and owned by the data center.

Vendor information contained in the plan does not identify the equipment or software available from the vendors and any applicable contract numbers. Without necessary vendor information readily available during a disaster situation, it will be difficult for personnel to timely purchase replacement equipment.

There is no documentation of business supplies, furniture, and personal computers and related peripheral equipment needed to maintain operations at an alternate site. For example, the current draft action plans of the enterprise team state it would need 10 personal computers at the alternative local site for restoration procedures; however, these computers are not provided for in the plan.

Configurations of the alternative site are not supported

There is no documentation to support the specific configurations outlined in the alternate facility contract that will be used in case of a disaster where the data center site is not available. The contract configurations are much lower than the current operational capacity of the data center. Data center officials stated technical support personnel instinctively know what configuration is required to support the hotsite readiness and that knowledge is used to determine contract parameters. However, without documentation supporting these configurations, it is unclear if the capacity limits are sufficient to restore applications. Table 1.1 shows the total operational capacity of the data center and the current contracted capacity at the hotsite.

[2] See Appendix II, page 17, for key terms and definitions used in the report.

Table 1.1: Capacity Comparison State Data Center and Hotsite

Capacity	Processing Capacity	System Storage	Direct Access Storage Device	Internet Connectivity
Per Contract	690 MIPS[1]	16 GB[2]	10.00 TB[3]	10 Mbps[4]
Current Operations	3,716 MIPS	38 GB	9.16 TB	47 Mbps
Difference	(3,026) MIPS	(22) GB	0.84 TB	(37) Mbps

Source: Data center officials and disaster recovery contract

[1] MIPS - Millions of instructions per second
[2] Gigabytes
[3] Terabytes
[4] Megabits per second

Standards state that management should ensure information technology recovery plans and arrangements are based on current needs. The data center customer procedures manual states: "A hardware configuration similar to what is available in the current data center will be provided at the alternate computer facility. The CPU and peripherals are sufficient to support the current production workload." This statement would infer that 100 percent of the current operational capacity will be provided in a disaster even though this is not the capacity planned for. The inconsistency could result in agency confusion over the applications to be restored.

Access to the recovery plan has not been sufficiently restricted

Weaknesses in establishing access rights to the recovery plan allowed at least 1,000 OA employees to receive unnecessary plan access. Data center officials indicated shortcuts taken by personnel in establishing access rights caused this problem. Officials have not developed formal procedures to evaluate access rights to the confidential portion of the data center's disaster recovery plan. Recovery plan access would not be necessary for most OA employees working outside of the data center. Also, some data center personnel have access rights to the plan individually and within a user group. The network administrator in charge of establishing access rights stated individual access was not necessary if access was already available through a user group. After discussion of these issues with data center officials, plan access for OA personnel outside the data center was removed and one official stated the access rights for the remaining users will be reviewed.

Officials need to evaluate the impact of risks or threats

Data center officials do not have procedures to analyze the impact of various disruptive events. According to accepted standards, potential risks and exposures should be updated on an ongoing basis. A business impact analysis would consider different types of risks and threats and their corresponding impact on business functions. Potential business interruptions as well as maximum tolerable down times should be identified. This analysis will allow officials to identify how long a critical function may be down, the impact on other business functions if it is out longer than anticipated, and what alternatives should be considered to resume business operations. Standards state the continuity plans should address disasters of varying degrees, and an impact analysis would provide the means to consider different scenarios.

Various strategies are available for recovering business operations. The appropriate strategy balances preventive and recovery costs against the business impact of possible outages. This business impact analysis would allow officials to select the most appropriate alternative to resume operations based on the risks identified.

Backup and off-site storage procedures are not adequately documented

Personnel cannot readily identify all the files and data being backed up, how often the backup is performed and how long the backup files are retained off-site. These weaknesses occur because these items are not documented or only documented in the job control language of the computerized backup job.

Accepted standards state backup and off-site storage plans should:

- Document backup procedures for data files and software.
- Document procedures for off-site storage, or availability of all material which would be required to restore and recover critical business functions within their identified maximum outage time.
- Ensure appropriate retention cycles have been established for critical off-site storage documentation based on the business needs and risks.
- Ensure information technology management approves backup and off-site storage procedures.

Standards state backup tapes should be retrieved on a regular basis from off-site storage and tested. The testing should ensure data required to resume/recover critical business processes are being stored correctly and the files may be retrieved without errors or lost data. Data center personnel do not routinely test backup systems and data outside of the annual recovery test. An October 1999 study performed by IBM stated the data center should increase the frequency of disaster recovery testing. IBM stated business continuity plans may fail while being tested because of incorrect assumptions, oversights, or changes in equipment or personnel.

Contract procedures for alternate facility are not adequate

The initial data center contract for an alternate facility was not re-bid timely and request for proposal (RFP) documents for the re-bid contract did not include appropriate configuration settings. The data center has a contract to provide an alternate computer facility in the event the data center cannot be used. In a disaster situation, data center officials will activate the disaster recovery plan and resume processing from the alternate computer facility. The alternate computer facility agreement for fiscal year 1996 was extended over 2 years past its contractual 3-year renewal period, which was to have ended with fiscal year 1999. The contract's procurement officer noted he mistakenly allowed the first year extension to occur, but stated the last year and a half extension occurred because the next new contract was under development. State data center officials stated the contract bidding was delayed due to extensive discussions with the legislature and user agencies over funding available for disaster recovery preparedness.

When the contract was re-bid, bids were solicited for configuration settings that would not be used. Data center personnel explained they did not use current system settings in the RFP because they did not expect those same settings to be relevant when the contract was finalized. The RFP included three configurations: the bare minimum production, full production without Internet capability, and full production with Internet capabilities, none of which were put into place once the contract bid was accepted. There is less assurance the data center is getting the best costs possible without re-bidding contracts timely and using actual specifications in the bidding process.

Conclusions

Data center officials have taken significant steps in development of a comprehensive continuity plan; however, the current plan still lacks several items. Officials have not performed an analysis of the risks the data center is susceptible to and the likelihood of the risks. Data center operations face significant risks without a completed comprehensive continuity plan, an impact analysis, and adequately documented and tested backup procedures. In addition, data center officials had not taken sufficient steps in restricting access to the confidential sections of the plan until we reported access problems to them.

Recommendations

We recommend the Commissioner, Office of Administration:

1.1 Complete development and implementation of a detailed comprehensive continuity plan which will support the data center's recovery strategy that ensures critical information systems processing functions can continue in the event of a significant disruption to normal computer operations. Procedures and objectives of testing the plan should be incorporated.

1.2 Establish a formal maximum tolerable outage time for the data center's operations.

1.3 Review the current access rights to the recovery plan to ensure they are appropriate and necessary as well as prepare procedures for establishing future access to the plan.

1.4 Develop procedures to incorporate a periodic impact analysis process to monitor the ongoing requirements of recovery plans.

1.5 Develop and document backup and off-site storage procedures for critical data files to support the recovery and resumption of business processes and system operations.

1.6 Test off-site backup files more frequently than during the state's annual recovery test.

1.7 Improve contract procedures, which should include ensuring planned specifications are used in soliciting bids and re-bidding contracts once renewal options have expired or sooner if warranted.

Office of Administration Comments

1.1 We agree that a detailed comprehensive continuity plan is desirable. However, since our primary objective is to provide critical services to our customers during a disaster, our first priority is a complete disaster recovery plan. We believe that very little of our critical recovery strategy would be covered in a continuity plan. Once we have developed an adequate disaster recovery plan, we will evaluate what is necessary in the continuity area.

1.2 The State Data Center is governed by a steering committee comprised of all our customers. In the past, we have presented to the committee different disaster recovery options that include outage times and costs associated with changing those outage times. The committee agreed to the current contract's outage times and associated costs are reasonable in the event of a disaster. However, since this has not been reviewed recently, we will present it for review by the steering committee to be sure that it is still acceptable to the agencies.

1.3 This recommendation has currently been implemented. System access has been reviewed and restricted to authorized personnel within the State Data Center.

1.4 We agree that an impact analysis would provide additional helpful information to help improve our recovery plans. However, at this time the State Data Center does not have any resources to dedicate to this effort or the money to outsource it.

1.5 We have developed procedures and made the documentation an integral part of the disaster recovery plan.

1.6 We agree that having the ability to test the off-site backup files more frequently than once a year would be optimal, however, our current contract only allows for once a year testing. We do not believe the state could afford to do it more frequently. We have however created a section of the mainframe to allow agencies to test applications on a limited basis as often as they desire.

1.7 We have implemented new bid procedures through the Division of Purchasing.

2. Mainframe Security Control Weaknesses Increase Risk

Management practices do not provide sufficient computer security procedures for agencies, or require agency mainframe security to be monitored. Other management weaknesses include:

- Lack of security policies and procedures for system administration within the data center.
- Lack of documentation of life-cycle changes for the mainframe security program.
- Inadequate segregation of duties.

Data center officials said the data center operates as a customer service function rather than a policy maker and enforcer. As a result, the state mainframe data integrity, confidentiality and availability are at risk for unauthorized use or modification.

Background

Data center officials safeguard information and data stored on data center resources. The state uses the IBM application Resource Access Control Facility (RACF) as the utility for computer security. The data center is the system administrator of computer access for 14 state entities. The remaining 22 state entities with mainframe access have approximately 250 system administrators within their information systems sections that are responsible for managing access to mainframe resources through RACF. The data center has 5 system administrators with system-wide access and 19 system administrators with access to data center IDs. As of April 2003, there were approximately 45,000 active user IDs on the mainframe system, including 301 IDs of data center staff.

In October 1999, IBM performed a security review and noted there was a lack of uniform security policies and standards which should be implemented by all sections of state government. IBM recommended establishing an information security officer position to act as a central focus for information security issues that could promote and enforce information security for all state information technology functions. The data center responded by creating the Information Security Management Office to coordinate work with steering committees, advisory boards, and the Office of Information Technology to establish "best practices," guidelines, and policies for all state agencies.

Customer security procedures need to be expanded

The data center customer procedures manual does not require agencies to (1) establish a password change interval for all user IDs, (2) periodically review inactive user IDs, (3) review for IDs with expired passwords that were reset and never used again, (4) include the user's name with the ID information, (5) segregate administrator and auditor functions, or (6) obtain and review security violation reports. As a result, 38 percent (17,341 of 45,331) of all active data center user IDs as of April 30, 2003 had some weakness which included:[3]

[3] Includes data center staff further discussed on page 11. Some user IDs had more than one weakness.

- 3,996 IDs had no password change interval established. A password interval notifies the system how often the ID's password must be changed. These IDs will remain active without a periodic password change.
- 9,651 IDs that had been signed onto at least once had not been accessed for 90 days. An additional 3,696 IDs had never been accessed.
- 5,226[4] IDs had not been signed onto since the password had been reset. 4,139 of these IDs are part of the 9,651 IDs noted above, which have been inactive for at least 90 days. An expired password indicates the user ID's password had been reset, but not used after the reset. Such IDs pose more of a security risk because when the passwords are reset, the reset defaults to an easily determinable password unless over-ridden by the system administrator.
- 6,622 IDs did not have an assigned and associated user name.
- 11 IDs have access to perform both system administrator and auditor functions.

Data center staff do not monitor the system security actions or established controls of the entities delegated authority to manage their user IDs. For the entities where the data center handles ID administration, data center employees do not automatically prepare security reports for agency staff to review unless requested by the agency. As the system and security administrator of the RACF program, the data center has the ultimate responsibility to ensure system security of the mainframe and its data. Standards state management should assume full responsibility for developing and maintaining a framework policy, which establishes the organization's overall approach to security and internal control to establish and improve the protection of information technology resources and system integrity. The data center needs to establish more detailed security policies for agency system administrators to follow and monitor compliance with those policies to provide better protection to the state's computerized data.

Security policies and procedures for the data center being developed

Data center officials stated until fall 2002, there were no security policies for administration of their staff's mainframe access or the manpower available to monitor IDs. At that time, unofficial security guidelines were created which are still waiting management's approval. A data center employee has been given the responsibility to monitor user access, but has not fully implemented all monitoring procedures. As a result, data center staff access weaknesses still exist.

User IDs need to be properly managed

Data center officials currently do not review user ID access after it is granted and also allow more than one ID to be assigned to a data center employee. As a result, during April 2003:

- 59 active user IDs for data center staff had no password interval established.
- 104 users had their passwords reset but were never logged on.
- 58 data center staff had been assigned 127 user IDs.

[4] Of these 5,226 user IDs, 817 were reset within a week of the April 30, 2003 report date and all but 14 of those IDs had been logged onto as of June 30, 2003.

The system administrators stated the extra IDs are assigned as a backup in case the employee's main ID is not functional. Although a few of the IDs are used for test purposes, we noted 5 of these IDs were never used and 23 had not been logged on for 90 days or more. In addition to these 28 user IDs, we identified 65 other active mainframe user IDs assigned to data center staff that had not been used for over 90 days. At our request, data center officials reviewed some of these user IDs and deleted access for 19. Officials stated they would review the access for the remaining inactive user IDs as well as the extra user IDs.

Access and security violations are not sufficiently monitored

Data center officials have not taken sufficient steps to ensure system security controls are functioning properly. The first step in establishing effective security is developing procedures for logging appropriate security-related events, monitoring specific access, and investigating apparent security violations. Currently, security features are activated to create an auditing log which includes all RACF command violations for all user IDs on the system, all commands issued by privileged IDs, and all failed actions to critical resources, such as protected datasets.

There are system tools to summarize and analyze the information in the auditing log; however, they are not used. Potential violations are brought to the attention of management by personnel once the concern is noted rather than through periodic review of this log. Documented procedures are not in place to investigate and take necessary action. Accordingly, unauthorized changes to critical security controls could go undetected without routinely reviewing the log. In addition, access to confidential data is not monitored to detect failed attempts or unusual patterns of successful access to such information. Routinely monitoring the access activities of employees can help identify significant problems and deter employees from inappropriate activities.

A security monitoring program should include (1) identifying sensitive system files, programs, and data files on computer systems and networks, (2) using the audit trail capabilities of security software to document both failed and successful access to these resources, (3) defining normal patterns of access activity, (4) analyzing audit trail information to identify and report on access patterns that differ significantly from defined normal patterns, (5) investigating potential security violations, and (6) taking appropriate action to discipline perpetrators, repair damage, and remedy the control weaknesses that allowed improper access.

System administrators' changes were not properly reviewed

Data center officials fail to review the use of privileged accounts. There are five system administrators with global rights over the entire data center computer system, but no policy for monitoring their operations. Accepted standards require effective supervision and review by management and formal operating procedures to help prevent or detect unauthorized or erroneous personnel actions. The security log maintains a record of changes made by the system administrators, but these logs are not reviewed.

Documentation is lacking in system security changes

RACF system security settings were changed but not documented. When the RACF program was installed, there were features a purchaser could customize. Also, since installation, officials indicated some other changes have been made to the RACF settings. These changes occurred without complying with any change management procedures; therefore, management cannot ensure they were made properly. Data center officials stated they felt the system settings themselves were adequate documentation of the changes. No documentation showed these officials approved the changes. Standards state procedures should be implemented to ensure system software changes are controlled with the organization's change management procedures, which should include a formal evaluation and approval by management.

Responsibilities for auditing and system security need to be properly segregated

Staff duties are not properly segregated. Three technical support personnel have privileged IDs with access rights that allow them to perform administration functions as well as auditing functions, including turning on and off system logging. The staff explained the auditing function has access rights to systematically run special reports that two of the technical support personnel need to use during off-peak times and the other staff person needs the auditing function to control the auditing logs. Data center officials feel the administrators need such rights to perform their job function. Standards recommend a division of roles between data security and audit. Officials should review other means of running the reports or implement compensating controls to mitigate this control weakness.

Conclusions

The data center does not have sufficient mainframe security procedures for system users to follow for the administration of RACF user IDs. Data center personnel are not monitoring state entities to determine if they have proper control procedures in place to ensure the information and data on the state's mainframe is secure. Data center system administrators follow no procedures concerning management of data center staff system IDs. The RACF program is not properly controlled through change management procedures. There is a lack of segregation of duties between access rights allowing security and auditing functions within the system.

Recommendations

We recommend the Commissioner, Office of Administration:

2.1 Establish security guidelines and procedures for the state entities to ensure adequate controls of access to data.

2.2 Establish and perform oversight controls for the RACF system to be used to monitor state entities.

2.3 Implement internal security procedures and controls regarding access of data center personnel to ensure the protection of information technology resources and integrity of information technology systems for the state. These procedures should include:

- Performing documented periodic reviews of user access rights to determine if they remain appropriate.
- Routinely reviewing security-related events, monitoring access, investigating apparent security violations, and taking appropriate remedial action.
- Reviewing the actions of privileged accounts.

2.4 Perform and document a review of current RACF system security settings to ensure they are appropriate and establish procedures to ensure future changes to system security settings are documented and approved.

2.5 Ensure system security duties are properly segregated from auditing duties and access rights are limited to essential job functions. If proper segregation cannot be done, implement compensating controls to limit any resulting control weaknesses.

Office of Administration Comments

2.1 We have security guidelines and procedures in place to ensure adequate controls of access to data. We have reviewed them and made updates necessary to maintain that control.

2.2 We believe that the current controls in place for RACF for state agencies are adequate. Currently each agency has a RACF administrator who is responsible for the specific data access for their employees. The State Data Center does not have the resources to perform the requested oversight and monitor each state agency. This is currently not within our scope of services and we believe there is no security risk with our current process.

2.3 Currently the State Data Center does have internal security procedures and controls regarding access of data center personnel. We did perform a review of these procedures and made appropriate changes and improved the current documentation.

2.4 We have performed a review of the system settings and made changes in the documentation process to better track changes to the system.

2.5 We have reviewed system security duties and made corrections in limiting the access for each job function as recommended.

Auditor's Comment

2.2 Thirty-eight percent of RACF user IDs having some type of security weakness at April 2003 does not support OA's statement that there is no security risk with current processes. Data center officials have developed new suggested user ID security procedures for data center customers that they anticipate will be added to the customer procedures manual in November 2003. These procedures address most of the weaknesses discussed on page 10. As the system and security administrator of the RACF program, the data center has the ultimate responsibility to ensure system security of the mainframe and its data. Data center officials need to monitor compliance with these new procedures once implemented to better ensure the integrity of the state's computerized data.

APPENDIX I

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate if the Office of Administration's (OA) data center management had (1) defined and implemented a comprehensive continuity plan to ensure recovery of business and computer processing operations in case of a disaster or other unexpected interruptions and (2) established appropriate administrative controls over the state's mainframe security application.

Scope and Methodology

Auditors conducted fieldwork during March 2003 through June 2003. The audit included:

- Review of applicable federal, national, and international standards related to comprehensive continuity planning and information resource security controls.
- Review of IBM's RACF manuals.
- Discussion with department personnel involved in comprehensive continuity planning and information resource security controls.
- Review of department records related to comprehensive continuity planning and RACF administration.
- Analysis of user ID information with RACF access.
- Evaluation of management controls pertinent to comprehensive continuity planning and information resource security through RACF.

The audit reviewed the data center's practices and procedures for comprehensive continuity planning and administration of RACF resource security controls. We did not fully evaluate all computer controls and we did not perform any penetration testing.[1]

During the audit, we provided OA officials with specific detail on security concerns noted for their immediate consideration.

[1] A test of a network's vulnerabilities by having an authorized individual actually attempt to break into the network. The tester may undertake several methods, workarounds and "hacks" to gain entry, often initially getting through to one seemingly harmless section, and from there, attacking more sensitive areas of the network.

APPENDIX II

DEFINITION OF TERMS

Some key terms and definitions accepted by the organizations noted on page 3 that have developed national and international standards for computer security include:

Application: Any of a class of "programs" or "software," which causes a computer to perform some useful function such as data entry, update or query.

Business Continuity: The discipline of planning for the recovery of business operations in the event that normal business resources, such as office space, terminals, microcomputers, office machines, terminals and networks, are made unavailable following a disaster. The term normally does not include the separate, but closely related, discipline of disaster recovery planning for information technology resources.

Dataset: A data file or collection of interrelated data. The term is used in a mainframe environment, whereas file is used almost everywhere else.

Hotsite: A disaster recovery facility that contains computers and equipment that an organization can use immediately.

Framework: A management level outline of the issues that need to be addressed in a comprehensive department-wide computer security plan. Provides background and rationale for information technology security, evaluation, certification and system accreditation.

Job Control Language: A command language for operating systems used to control run routines in connection with performing tasks on a computer.

Mainframe: A multi-user computer designed to meet the computing needs of a large organization.

Operating System: The master control program that runs the computer. It is the first program loaded when the computer is turned on and must reside in memory at all times. It sets the standards for all application programs that run in the computer.

Recovery: The ability to resume processing without irreparable loss of system data after an error or malfunction in software or hardware.

Security Administrator: The person(s) responsible for managing the security for computer facilities, computer systems and/or data that is stored on computer systems or transmitted via computer networks.

System Administrator: The person(s) responsible for administering use of a multi-user computer system, communications system, or both.

APPENDIX III

REFERENCES

American Institute of Certified Public Accountants

AICPA/CICA SysTrust: Principles and Criteria for Systems Reliability, Version 2.0, January 2001.

Auerbach Publishers

Information Technology Control and Audit, Frederick Gallegos, Daniel P. Manson and Sandra Allen-Senft, 1999.

Standard for Auditing Computer Applications, Martin A. Krist, 1999.

Canadian Institute of Chartered Accountants

Information Technology Control Guidelines 3rd Edition, July 1998.

Federal Chief Information Officers Council

Federal Information Technology Security Assessment Framework, November 28, 2000, http://www.cio.gov.

Information Systems Audit and Control Foundation

Control Objectives for Information and Related Technology (COBIT), 3rd Edition, July 2000, http://www.isaca.org.

Certified Information Systems Auditor (CISA) Review Manual, 2002, http://www.isaca.org.

International Organization for Standardization / International Electrotechnical Commission

ISO/IEC 17799:2000(E), *Information Technology – Code of Practice for Information Security Management,* December 2000, http://www.iso.ch.

McAtte, Bryan

Introduction to Information Technology Auditing, 2002.

Missouri Office of Administration - Division of Information Systems State Data Center

Customer Procedures Manual, Section IX, January 2002.

National Institute of Standards and Technology

Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995, http://csrc.nist.gov.

Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996, http://csrc.nist.gov.

Special Publication 800-18, *Guide For Developing Security Plans For Information Technology Systems,* December 1998, http://csrc.nist.gov.

Special Publication 800-26, *Security Self-Assessment Guide For Information Technology Systems,* November 2001, http://csrc.nist.gov.

Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002, http://csrc.nist.gov.

APPENDIX III

U.S. Office of Management and Budget

Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, November 2000, http://www.whitehouse.gov/omb/circulars/index.html.

U.S. General Accounting Office

Federal Information System Controls Audit Manual: GAO/AIMD-12.19.6, January 1999, http://www.gao.gov.

Warren Gorham & Lamont/RIA Group

Handbook of IT Auditing, 2001 Edition.