REVIEW OF THE INTERNAL CONTROLS OF THE RTA's INFORMATION SYSTEM

-Prepared by Audit & Review Division-

June 12, 2007

REVIEW OF THE INTERNAL CONTROLS OF THE RTA's INFORMATION SYSTEM

Table of Contents

REVIEW OF THE INTERNAL CONTROLS OF THE RTA's INFORMATION SYSTEM

June 12, 2007

EXECUTIVE SUMMARY

The Audit & Review Division conducted a review of the internal controls of the RTA's Information System, which is managed by the Information Technology (IT) Division. The objectives of the review were to evaluate the IT Division's:

- Management and security of IT resources, equipment, and information system.
- IT Policy and Procedures for adequacy, completeness, and ease of use.
- IT Contingency Plan for adequacy and completeness.
- Controls in place to account for all RTA computer equipment.

Our review resulted in the following eleven recommendations to improve the internal controls of the RTA's Information System and the operational efficiency of the IT Division:

1. Update the IT Contingency Plan
2. Update IT Policy and Procedures Manual
3. Maintain IT Access Request Forms
4. Document Holders of Keys to Secured Areas
5. Deactivate Access Rights of Terminated Employees/Contractors
6. Improve Controls over Tracking Computer Equipment
7. Dispose of Unused Computer Equipment
8. Improve Controls over IT Loaner Equipment
9. Document Training for New Employees
10. Improve Controls over Help Desk Requests
11. Update Job Description of TIC Systems Administrator

RTA management has accepted and agreed to implement each of the recommendations. We thank and appreciate the complete cooperation of the entire IT Division staff.

Paul G. Neuhauser
Manager, Audit & Review Division

REVIEW OF THE INTERNAL CONTROLS OF THE RTA's INFORMATION SYSTEM

INTRODUCTION

Under the direction of the Senior Deputy Executive Director, Finance and Administration, the Information Technology (IT) Division provides strategic direction to the RTA staff for the RTA's information resources and technology needs. The IT Division is responsible for the following activities:

- Maintaining an agency contingency plan to ensure continued operations in case of loss or disruption and testing the plan annually.
- Providing support to RTA employees utilizing IT resources (computer equipment, centralized network, internet and email systems, keycard security system, telephone and voicemail system, and the Travel Information Center).
- Participating in the selection of IT resources to meet user needs and obtain information technology in accordance with RTA procurement procedures and regulations.
- Obtaining, installing, distributing, and maintaining software and hardware.
- Creating and maintaining information security and privacy policies.
- Maintaining a test environment where software may be evaluated before procurement decisions are made and software problems may be resolved before impacting system users.

The specific objectives of this review were to evaluate the IT Division's:

1. Management and security of IT resources, equipment, and information system.
2. IT Policy and Procedures for adequacy, completeness, and ease of use.
3. IT Contingency Plan for adequacy and completeness.
4. Controls in place for the recording, disposing, and inventorying of RTA computer equipment.

BACKGROUND

The IT Division is responsible for overseeing the RTA's information resources and technology needs, which is monitored by the Manager of Information Technology under the authority of the Senior Deputy Executive Director of Finance and Administration (SDED). Currently, the Manager of Information Technology position is vacant and the SDED of Finance and Administration is performing that function. The IT Division is also staffed by a Programmer Analyst, Senior Network Administrator, Help Desk/LAN Technician, and a Computer Systems Web Designer. Because of certain IT responsibilities in connection with the Travel Information Center, the Telecommunications Specialist and the TIC Systems Administrator, who are under the direction of the Director of Regional Services, also report on technology issues to the Manager of Information Technology.

The IT Division is responsible for the security, purchase, installation, maintenance, and repair of network equipment, printers, computers, and software. The RTA computer network is composed of the following:

- Network servers which maintain the corporate applications and databases.
- The distribution system which includes wiring, switches, hubs, and routers.
- Desktop computers, printers, and other peripherals.

The network servers are a critical part of the IT environment. The loss of a server for any reason would impair the ability of the RTA to perform essential mission tasks. The servers are connected to Uninterruptible Power Supplies (UPS), which will maintain the server in an operation status during short interruptions of power supply. The RTA utilizes 36 servers to operate its Information System.

Desktop computers are in place for the support of all RTA employees. The units are all Intel or compatible processor systems running the Windows 2000 or XP operating systems. There are also notebook computers assigned to the RTA senior staff and other employees as well. The primary software applications loaded on the desktop and laptop computers is MS Office 2003. These systems are also running Norton Anti Virus software (Corporate Edition) to guard against computer viruses which can interfere with computer operation.

SCOPE OF REVIEW

The scope of the review included the following activities:

- Interviewed IT Division staff.
- Reviewed existing job descriptions on file with HR. (See Observation #11)
- Reviewed the training provided by the IT Division to RTA staff. (See Observation #9)
- Reviewed the IT Contingency Plan. (See Observation #1)
- Reviewed the IT Policy and Procedures Manual. (See Observation #2)
- Reviewed the RTA Information System Inventory listing. (See Observation #2)
- Reviewed the back-up tape schedule and off-site storage location. (See Observation #1)
- Reviewed the documentation related to the latest recovery testing. (See Observation #1)
- Reviewed the process for issuing/deactivating user access rights. (See Observations #3 & #5)
- Reviewed the process for obtaining IT loaner equipment. (See Observation #8)
- Performed physical inventory verification of IT equipment. (See Observation #6)
- Reviewed fixed assets disposed of and purchased in 2006 and 2007. (See Observation #7)
- Surveyed employees who submitted help desk requests. (See Observation #10)

The review scope also examined the following activities which were found to be in compliance:

- Physical and logical security controls utilized to protect IT equipment.
- Local area network security controls utilized to ensure the RTA's Information System is properly monitored and protected.
- Adequate insurance coverage for the computer equipment.
- Adequate physical controls (secured room, video surveillance, etc.) are in place in the server rooms to protect IT equipment.
- All alarms and other electronically controlled security devices are connected to a back-up power source that would allow them to function in the event of a power failure.
- Video surveillance cameras are utilized to monitor the activity surrounding and inside the server rooms.
- Adequate environmental controls (fire alarms, temperature and humidity controllers, etc.) installed in the server rooms to protect IT equipment (both on the 2nd and 15th floors).
- Standalone Uninterruptible Power Supply (UPS) is utilized for the servers.
- Adequate password policies and procedures are in place.
- Internet security controls utilized to ensure the RTA's Internet system is properly monitored and protected.
- Adequate Internet policies and oversight are in place to monitor staff activities.
- Adequate Internet firewalls are in place to protect the RTA's Information System.
- Log is in place that tracks access to the RTA's Information System.
- Written policies and procedures in place to process software changes and upgrades.
- RTA's Information System protected from computer viruses or other security threats.
- Monitoring procedures in place to ensure that the RTA's Information System is not accessed by outsiders.
- Encryption techniques in place within the LAN network.

OBSERVATIONS AND RECOMMENDATIONS

Overall, we found that the IT Division carries out its responsibilities efficiently and effectively. However, we do offer the following eleven recommendations to strengthen the internal controls of the RTA's Information System and improve the operational efficiency of the IT Division.

1. Update the IT Contingency Plan

Observation: The objective of any contingency plan is the identification of risk factors and the preparation of plans to ensure the ability of the entity to recover its data and the infrastructure required to continue operations. The current IT Contingency Plan details how the server system will be restored in the event of hardware and software failures; however, it does not detail how the IT Division will react to restore RTA operations if a disaster were to occur that prohibits the RTA from operating at its current location. We understand that it is not possible to plan for every possible emergency event that may occur, but having a guide to assist in dealing with certain emergencies is essential.

Also, addressed in the current IT Contingency Plan is a regular schedule of computer backup tapes. Backup tapes are prepared daily, but are not sent to an off-site until the end of the week. Further, the off-site location for the storage of the tapes is at the Northern Trust Bank, less than three blocks from the RTA offices.

Recommendation: The following areas should be reviewed for inclusion in the IT Contingency Plan or updated as necessary:

- Development of the Business Continuity Plan to allow essential elements of the RTA to continue operation in the event of a disaster. First, departmental contingency plans would have to be developed to identify those areas that are critical to the RTA and the systems that should resume operations in a timely manner if a disaster were to occur. As stated in the IT Contingency Plan, and as was performed in 2006, testing of the contingency plan should be performed on an annual basis. This should include testing to ensure the RTA system can be restored based on mock emergencies as well as ensuring equipment, such as back-up power sources, is working properly.
- IT management should re-examine its computer back-up tape policy of sending those tapes off-site daily, rather than weekly, and to consider an off-site storage location outside of the immediate downtown area rather than its present location less than three blocks from the offices of the RTA.
- The documentation that details the results of the testing performed to ensure operations are restored in accordance to plans should be expanded to include the system(s) tested, the individuals who participated in the test, and the results of the testing performed.

Response: IT management agrees with the recommendation.

2. Update IT Policy and Procedures Manual

Observation: The IT Policy and Procedures Manual, which is distributed to all employees, needs to be updated. The manual was last updated on November 22, 2006. Since that time, there have been a number of changes to the policies and procedures related to the administration of IT resources that should be documented.

Recommendation: The IT Policy and Procedures Manual should be updated to reflect the current policies and procedures to be followed and the documentation to be utilized. Some key areas that should be updated or reviewed for inclusion are as follows:

- Employees permitted to have IT equipment at their homes to perform work-related tasks. This policy should be carefully scrutinized with the assistance of Human Resources (HR) because any non-exempt employee that is working both at the office and at home and exceeds 40 hours in a week is eligible for overtime pay.
- Employees that are eligible to be distributed IT equipment such as cell phones, laptops, and wireless personal digital assistants (BlackBerrys). BlackBerrys can send and receive email and other data, browse the web over a cellular network, and function as a cellular telephone.

- Establish a policy for moving data out of the RTA's infrastructure by the RTA staff, utilizing such means as email, iPods, and USB flash drives.
- Instructions on how IT staff is to send and track files sent to vendors to correct software applications.
- The RTA Information System Inventory listing should include the software purchased by the RTA, names of employees who are currently responsible for the RTA databases, and the number of software licenses the RTA purchased.
- Process for initiating and canceling access rights for employees/contractors/interns.
- Proper usage of email distribution lists.

An updated procedures manual will ensure that formal guidelines are on file that can be consistently applied and referred to as needed by the staff.

Response: IT management and the Director of HR (see first bullet point) agree with the recommendation.

3. Maintain IT Access Request Forms

Observation: We obtained a listing of all employees hired in 2006 and 2007 from HR and determined if an electronically submitted IT Access Request Form was on file detailing the access rights (for computers, email, telephones, voice mail, on-line services, internet, keycards, etc.) given to each employee. We could not locate the IT Access Request Form for four of the 23 employees hired in 2006. As stated in the IT Policy and Procedures Manual, IT is to maintain an electronic record of all access requests.

Recommendation: IT management should ensure that a record of all access request forms are maintained in an electronic file.

Response: IT management agrees with the recommendation.

4. Document the Holders of Keys to Secured Areas

Observation: We noted from discussions with IT staff that six employees have been issued keys that allow them to access the server rooms located on the 2nd and 15th floors and the IT supply room. However, the log that Procurement maintains of the employees that have been issued those keys has not been updated to include the names of all of the current key holders.

Recommendation: We recommend the following:

- Since the sensitive areas mentioned above can also be accessed utilizing a keycard, Procurement management recommends that there be a single point of control, rather than multiple means of entering these areas that are controlled by different divisions. Since the keycard records the entry in the Kastle system, there should be no keys issued for these areas and the master key should be used only when the card reader fails. Any other keys to these rooms should be collected from the current holders.

- Procurement management should ensure the log that is maintained of the keys that RTA employees are issued, especially master keys that access sensitive areas such as the server rooms and the IT supply room, is updated as needed to include current key holders.
- The form that HR maintains that details the resources that RTA employees have been issued should be updated to include a line item to note that keys were issued to the employees. Upon termination, HR can reference the Procurement key log to ensure that all keys have been returned.

Response: Procurement management, IT management, and the Director of HR agree with the recommendation.

5. Deactivate Access Rights of Terminated Employees/Contractors

Observation: The IT staff is required to deactivate electronic access rights upon notification from HR that an employee is no longer employed by the RTA. We reviewed the reports detailing active user identifications and active keycard holders and noted the following:

- An employee that retired in January 2007 still has access rights to the RTA system.
- A temporary employee that was terminated in April 2007 appears on the listing of active keycard holders.

Per discussion with the IT staff, the above employees were not removed from the active lists because they were not advised to do so by HR.

Recommendation: HR should inform IT Division of each terminated employee so that the necessary access rights can be immediately deactivated.

Response: The Director of HR agrees with the recommendation.

6. Improve Controls over Tracking Computer Equipment

Observation: We could not locate six of the 25 items selected for physical inventory verification. The value of the missing items totaled $27,700, and consisted, for the most part, of outdated monitors, computers, and other miscellaneous items. IT staff could offer no explanation why the disposition of these items was not recorded, but believe that the items, which have little or any value at this time, had been legitimately disposed of earlier. Furthermore, in order to select the items for physical inventory verification, records maintained by both the Procurement and the IT Divisions had to be reviewed since there is not one central location where all IT equipment (both hardware and software) is tracked. As stated in the IT Policy and Procedures Manual, the IT Division is to maintain an inventory of all IT equipment, software, and applications.

Recommendation: IT management should maintain a complete inventory listing that includes the location of all IT equipment (both hardware and software). This listing should be compared to Procurement's records of fixed assets. Any discrepancies noted between Procurement's and IT's inventory records should be properly investigated and any necessary changes made to the inventory records.

Response: IT management agrees with the recommendation.

7. Dispose of Unused Computer Equipment

Observation: We found unused computer equipment stored in the IT staff office as well as outside of the office in the hallway. Computer equipment that is not being used by the RTA should be properly disposed of so that assets are not misappropriated.

Recommendation: IT management should ensure that computer equipment that is not being used by the RTA is properly disposed. If the computer equipment is not operable, it should be properly discarded. If the computer equipment is still operable, it should be either sold or donated to the appropriate non-profit organization and stored in a secured area until disposition.

Response: IT management agrees with the recommendation.

8. Improve Controls over IT Loaner Equipment

Observation: We noted during our review of IT Resource Request Forms that RTA employees were allowed to request IT loaner equipment (for RTA work related purposes) without the approval of their immediate supervisor. As stated in the IT Policy and Procedures Manual, managers must authorize the use of a loaner by completing the IT Loan Request Form. In addition, it was found that the IT staff does not track whether the loaner IT equipment is returned by the date stated on the request form and does not record the date the equipment was actually returned.

Recommendation: IT management should ensure that requests for IT loaner equipment are initiated and approved by the employee's immediate supervisor. In addition, for better control over this equipment, the IT Division should ensure that it is returned by the due date and that should be noted in the records.

Response: IT management agrees with the recommendation.

9. Document Training for New Employees

Observation: We noted during our review that the Help Desk/LAN Technician is responsible for providing training to new employees concerning how to utilize IT equipment (such as computers, faxes, printers, telephones, etc.) and the policies related to computer usage. However, the areas to be covered with the new employee are not documented which would help to ensure that all pertinent information is covered.

Recommendation: For the training that IT staff gives to new employees, a checklist should be prepared to document the areas to be covered. This checklist should be signed by the employee and the IT staff member performing the training and should be forwarded to HR to be maintained in the employee's personnel file as evidence of the training provided.

Response: IT management and the Director of HR agree with the recommendation.

10. Improve Controls over Help Desk Requests

Observation: We surveyed ten randomly selected RTA employees who completed Help Desk requests during the first six months of 2007, regarding the quality and timeliness of service received as well as any suggestions for improving the Help Desk function. Overall, RTA employees are satisfied with the quality of service received from the Help Desk, but did provide the following comments to improve the process:

- Help Desk request forms, which are accessible via the intranet, are not user friendly.
- There is no timetable provided as to when the Help Desk request will be completed by the IT staff member handling the request. This would be especially helpful when an urgent or high priority level is selected. Because this information is not provided, RTA employees are more inclined to contact IT staff directly for urgent requests which defeats the purpose of having an on-line Help Desk request system.
- No status updates are provided by IT staff during the period when the Help Desk request is being processed.
- RTA employees are not always informed that their Help desk request has been completed.

Recommendation: IT management should take into consideration the comments provided by RTA staff concerning the service provided by the Help Desk function and determine the appropriate actions to take to ensure the Help Desk function is an adequate resource for the RTA.

Response: IT management agrees with the recommendation.

11. Update Job Description of TIC Systems Administrator

Observation: The TIC Systems Administrator's job description was last updated in 1997, when that position reported exclusively to the Manager of Regional Services. Currently, while the incumbent directly reports to the Director of Regional Services, he also reports on technology issues to the Manager of Information Technology.

Recommendation: The TIC Systems Administrator's job description should be updated by the Director of Regional Services with assistance as necessary from the Manager of Information Technology to reflect the changes made to the position since the last update.

Response: The Director of Regional Services will work with IT management and HR to update the TIC System Administrator's job description.

June 12, 2007

Paul G. Neuhauser
Manager, Audit & Review Division