



FOLLOW-UP REVIEW OF THE IT FUNCTION

-Prepared by Audit & Review Division-

April 21, 2008

FOLLOW-UP REVIEW OF THE IT FUNCTION

Table of Contents

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

FOLLOW-UP REVIEW OF THE IT FUNCTION

April 21, 2008

EXECUTIVE SUMMARY

The Audit & Review Division conducted a follow-up review of the internal controls of the RTA's Information System, which is managed by the Information Technology (IT) Division. The overall objectives of the original 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.

The original review resulted in eleven recommendations to improve the internal controls of the RTA's Information System and the operational efficiency of the IT Division. Our follow-up review found that four of the recommendations have been fully implemented with the remaining recommendations scheduled for full implementation by June 30, 2008.

Catherine M. Clark
Senior Auditor, Audit & Review Division

FOLLOW-UP REVIEW OF THE IT FUNCTION

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, for which a report was issued on June 12, 2007, 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.

The review resulted in 11 recommendations to improve the effectiveness and efficiency of the IT Division. The purpose of the follow-up review is to determine whether the recommendations have been implemented and are achieving their intended purpose.

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, a permanent replacement is being sought for the Manager of Information Technology position. While the search is being conducted to fill the position, management of the IT Division is being performed by the Acting Manager of Information Technology. The IT Division is also staffed by a Programmer Analyst, Senior Network Administrator (currently vacant), Help Desk/LAN Technician (currently vacant), Computer Systems Web Designer, Telecommunications Specialist, and the TIC Systems Administrator.

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 follow-up review was limited to the observations set forth in the original report. The follow-up report is not intended to expand upon the observations of the initial review, but rather to determine the current status of the recommendations included in that report. Within this scope, we interviewed the Acting Manager of Information Technology, the Director of HR, and the Procurement Manager who had the responsibility to implement the recommendations.

STATUS OF ORIGINAL OBSERVATIONS AND RECOMMENDATIONS

This section summarizes the original observations, recommendations, and responses from our first report, as well as the current status of those recommendations.

1. Update the IT Contingency Plan

Previous 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.

Previous 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.
- 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.

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been partially implemented. The Acting Manager of Information Technology has updated the IT Contingency Plan, however, it may need to be revised further upon review by the individual who fills the Manager of Information Technology position. Therefore, Audit & Review will follow-up with the individual hired as the Manager of Information Technology to determine the changes, if any, which need to be made to the IT Contingency Plan before it can be implemented.

2. Update IT Policy and Procedures Manual

Previous 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.

Previous 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.

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

Status of Previous Recommendation: This recommendation has been partially implemented. The Acting Manager of Information Technology, along with input from the applicable RTA staff, has updated the IT Policy and Procedures Manual. However, the IT Policy and Procedures Manual may need to be revised further upon review by the individual who fills the Manager of Information Technology position. Therefore, Audit & Review will follow-up with the individual hired as the Manager of Information Technology to determine the changes, if any, to be made to the manual. Once all changes are complete, RTA staff should be informed and the IT Policy and Procedures Manual should be posted to the RTA intranet for easier accessibility.

3. Maintain IT Access Request Forms

Previous Observation: We obtained a listing of all employees hired in 2006 and 2007 from HR and 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.

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

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been partially implemented. The Acting Manager of Information Technology was able to locate the four IT Access Request Forms that could not be located during the original IT audit. Of the two employees that were hired at the RTA since June 2007, an IT Access Request Form was completed and on file. However, the current IT Access Request Form utilized by the IT Division may need to be revised further by the individual who is hired in the Manager of Information Technology position. Therefore, Audit & Review will follow-up with the individual hired as the Manager of Information Technology to determine if this current form should be revised to better capture the resources that are issued to new employees.

4. Document the Holders of Keys to Secured Areas

Previous 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.

Previous 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.

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

Status of Previous Recommendation: This recommendation has been partially implemented as follows:

- It has been determined that the Manager of Information Technology (which is being filled temporarily by the Acting Manager of Information Technology) will maintain a key to access the server room only in those instances when the keycard system is malfunctioning. It has also been determined that the key to the server room on the 2nd floor will be shared by the TIC Systems Administrator and the Telecommunications Specialist and utilized only in those instances when the keycard system is malfunctioning. All other keys to the server rooms located on the 2nd and 15th floors were retrieved from the remaining IT staff members. In regards to the IT supply room, this room can only be accessed with a key. It was determined that it was only necessary for three of the members of the IT Division to retain a key to the IT supply room. All other keys to the IT supply room were retrieved from the remaining IT staff members.
- Procurement management has begun updating its records of the keys that were issued to RTA staff. Procedures are being developed that will state the process that Procurement and HR will follow when issuing and collecting keys. This recommendation will be fully implemented by June 30, 2008.

- The Director of HR developed a form entitled ‘Receipt of Keys’ that details the keys issued to employees. This use of this form began with those employees hired in 2008.

5. Deactivate Access Rights of Terminated Employees/Contractors

Previous 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.

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

Previous Response: The Director of HR agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been implemented.

6. Improve Controls over Tracking Computer Equipment

Previous 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. As stated in the IT Policy and Procedures Manual, the IT Division is to maintain an inventory of all IT equipment, software, and applications.

Previous 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.

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been partially implemented. The Acting Manager of Information Technology has compiled a complete inventory listing that includes the location of all IT equipment (both hardware and software). However, the Procurement Division has not completed their annual physical inventory of RTA assets. Because of that, no reconciliation can be performed to compare Procurement’s records with that of the IT Division. Per discussion with the Procurement Manager, the physical inventory process should be completed

by June 30, 2008. At that time, the records of the Procurement and IT Divisions should be compared and any discrepancies should be properly investigated and the necessary changes made to the inventory records.

7. Dispose of Unused Computer Equipment

Previous 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.

Previous 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.

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been implemented.

8. Improve Controls over IT Loaner Equipment

Previous 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.

Previous 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.

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: This recommendation has been implemented.

9. Document Training for New Employees

Previous 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.

Previous 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.

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

Status of Previous Recommendation: This recommendation has been partially implemented. The Acting Manager of Information Technology developed a checklist to document the training provided to new employees. However, since the Manager of Information Technology position is yet to be filled, the form that is currently being utilized may need to be revised. Audit & Review will follow-up on this recommendation with the individual that is hired as the Manager of Information Technology to ensure that adequate training is being given to new employees and that it is properly documented.

10. Improve Controls over Help Desk Requests

Previous 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.

Previous 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.

Previous Response: IT management agrees with the recommendation.

Status of Previous Recommendation: Audit & Review conducted another survey with a different set of randomly selected employees to determine if the level of service provided by the Help Desk function has improved. Overall, RTA employees are satisfied with the service received from the Help Desk. However, employees continue to state that they are not provided status updates by IT staff during the period when the Help Desk request is being processed and that requests are not always resolved in a timely manner. A factor to consider is that during the period we reviewed, the IT Division was understaffed which may be a contributing factor to the issues faced by the RTA employees who were surveyed. We will continue to monitor this situation on at least an annual basis and share the feedback with the individual that fills the Manager of Information Technology

position to ensure that the Help Desk request system is a benefit to all RTA employees. For the purposes of the follow-up review, the recommendation is considered to be implemented.

11. Update Job Description of TIC Systems Administrator

Previous 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.

Previous 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.

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

Status of Previous Recommendation: This recommendation has been partially implemented. The management reporting structure of the TIC Systems Administrator was changed where the employee reports only to the Manager of Information Technology. The job description for the position will be finalized by the individual selected to fill the Manager of Information Technology position.

Catherine M. Clark
Senior Auditor, Audit & Review Division
April 21, 2008