City of Chattanooga

Stan Sewell
Director

INTERNAL AUDIT
City Hall
Chattanooga, Tennessee 37402

Ron Littlefield
Mayor

May 14, 2009

Mayor and City Council
City of Chattanooga
Chattanooga, TN 37402

RE: Post Audit Review of IT Disaster Recovery, Audit 08-07

Dear Mayor Littlefield and Council Members:

On October 20, 2008, the Internal Audit Division released an audit on the Information Services Disaster Recovery Plan. We performed certain procedures, as enumerated below, with respect to activities of Information Services in order to render a conclusion on the status of the recommendations made as a result of that audit.

This Post Audit Review consisted principally of inquiries of City personnel and examinations of various supporting documentation. It was substantially less in scope than an audit in accordance with generally accepted government auditing standards.

The evidence obtained provided a reasonable basis for our conclusions; however, had an audit been performed, other matters might have come to our attention that would have been reported to you and our conclusions may have been modified.

The conclusions of Audit 08-07 were that:

1. The IS Disaster Recovery plan needs updating and enhancement.
2. The IS Disaster Recovery plan is not regularly tested.
3. Some City computer facilities need upgrading and relocating.
4. The IS data backup procedures are not documented.

OFFICE: (423) 425-6202 • FAX: (423) 425-6204

The audit contained five (5) recommendations that addressed the audit's findings. Based on the review performed, we concluded that recommendation #4 was implemented, recommendation #1 was partially implemented and recommendations #2, #3, and #5 were not implemented.

Recommendations Implemented, #4

We recommended (Recommendation 4) that the IS department use the computer facility leased from Airnet to set the standard for all the City's computer facilities in regards to the security, fire protection, and climate monitoring at the minimum in order to protect all the City's computer equipment and sensitive data. This may involve additional funding.

The IS department has purchased a new building and is in the process of moving the main computer facility that is leased from Airnet and the equipment located at the DRC building to the new location. The new location will be outfitted with the proper equipment such as a fire suppression system, environmental monitoring, and a security system.

Recommendations Partially Implemented, #1

We recommended (Recommendation 1) that based upon control practices within COBIT[1], to ensure continuous service of the IS department is to first develop an IS plan which would help reduce the impact of a major disruption on key business functions and processes. The plan should include, but not be limited to, identification of critical resources, setting priorities for restoring critical business functions, identifying key personnel and maintaining a current contact list, alternative processing locations, the procedures for backup and recovery, and requiring annual testing and maintenance of the plan. We also recommend that when the City's divisions start the process to establish their own business continuity plan that the IS department work in coordination with them to help set the priorities when restoring the City's critical systems.

The IS department has updated some areas in their Disaster Recovery plan and they are currently working on detailing out the critical resources in the systems. However, detailing out these critical systems is dependent upon the ability and cooperation of City departments working with IS in identifying these systems and setting priorities.

Recommendations Not Implemented, #2, #3, #5

We recommended (Recommendation 2) that based upon control practices set by COBIT, testing the disaster recovery plan should be scheduled and conducted on a regular basis, at least annually. The results of the test should be documented and the plan should be updated as needed. The IS disaster recovery plan should set requirements for periodic testing of the plan.

---

[1] IT Governance Institute has established standards issued in COBIT (Control Objectives for Information and related Technology). COBIT enables clear policy development and good practice for IT control throughout organizations. (www.tigi.org)

Per the IS department, a test of the Disaster Recovery plan has not yet occurred. This is due to the lack of available "spare" hardware to physically test the plan. They are currently in the process of purchasing new equipment which would help alleviate this problem.

We recommended (Recommendation 3) that the offsite storage location be relocated to a more secure site. We recognize that the site has to be located in an area where IS can still maintain the regular rotation of the media efficiently. The site must also be secure and not comprise the preservation of the media. This may involve additional funding and new technology to improve the security and reliability of the data.

The IS department has investigated new solutions for better off-site storage of data. However, a new site or solution has not been implemented for the data storage.

We recommended (Recommendation 5) that the IS department develop a full set of procedures that addresses the entire process of backing up data, retrieving it and securely storing it. This also includes periodic monitoring of this process to ensure it is being properly followed. We also recommended that IS management work with City management to determine an agreeable risk level set for the acceptable loss of data due to a disaster when setting their procedures for data backup (cost vs. benefit analysis).

The IS department has met with their staff who handle their collection of backup data and restated their practice on the collection and storage process. However, formal written policy and procedures have not been fully completed at this time.

We thank the personnel in IS department for their assistance in conducting this review. We will consider this report to be final unless directed to continue our review.

Sincerely,

Stan Sewell, CPA, CGFM
Director of Internal Audit

cc: Dan Johnson, Chief of Staff
Mark Keil, Chief Information Officer