Audit Report

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Audit of the City's Backup and Disaster Recovery Processes

Report #1515 ***September 1, 2015***

Preamble

We have elected to issue a public report presenting at a summary level the results of our audit of the City's backup and disaster recovery planning processes. Details of certain aspects and characteristics of the City's information technology (IT) systems, for which disclosure may be in violation of state statutes (based on rapidly evolving interpretations of provisions of Chapter 281, Florida Statutes) and good business practices, have intentionally not been included in this report. To facilitate corrective measures and actions based on our audit, a separate, confidential report containing those details has been prepared and issued to appropriate City officials, management, and staff. Management has developed an action plan to address the issues and related recommendations in that confidential report. We will follow up and report to appropriate City officials and management on the efforts of applicable City staff in completing the established action plan steps as part of our periodic follow-up process.

Executive Summary

Overall, we concluded the City's data is being backed up appropriately and, for the most part, in accordance with best practices. We concluded that, overall, there are plans and preparations for disaster recovery for most systems. For appropriate areas, we made recommendations to further enhance the City's IT backup and disaster recovery processes.

The information technology (IT) resources of the City and its departments include servers (computers), operating systems, applications, and large amounts of unique, irreplaceable data. These resources support and facilitate the daily operations of the City, and their loss would significantly impair the City's ability to serve its citizens. One of the means commonly used to protect IT resources from loss is to periodically backup (i.e., create and save copies of) IT operating systems, applications, and data. To ensure the continuing ability to operate with IT resources, it is also common practice to have in place IT disaster recovery plans that describe the processes to be followed in order to resume IT operations after a significant interruption in IT system services. Based on our audit, we concluded the City's data is being backed up appropriately and, for the most part, in accordance with best practices. Additionally, we concluded that, overall, there are plans and preparations for disaster recovery (in accordance with best practices) for most systems. For appropriate areas, we made recommendations to further enhance and improve the City's IT backup and disaster recovery processes.

Audit Purpose and Objectives

The purpose of this audit was to evaluate the effectiveness of the City's information technology (IT) system backup and disaster recovery planning processes. Our objective was to answer the following questions:

1) Are City IT systems being backed up appropriately and in a manner consistent with best practices?
2) Are the plans and preparations for IT disaster recovery reasonable, appropriate, and consistent with best practices?

Audit Scope

The scope of the audit included; (1) identifying and evaluating City policies and selected department processes and procedures relating to the backup of IT systems (to include a comparison to best practices) and a review and analysis of the IT system backups, and (2) identifying and evaluating City policies and departmental procedures and processes relating to disaster recovery planning, as well as a comparison of the disaster recovery planning processes implemented to best practices.

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

Overview of Audit Results. Based on the results of our audit, we concluded the City's data is being backed up appropriately and, for the most part, in accordance with best practices. Additionally, we concluded that, overall, there are plans and preparations for disaster recovery (in accordance with best practices) for most City IT systems. During the course of the audit we identified areas and issues which, if addressed, should enhance or improve the City's processes for backing up data. We also identified areas where improvements should be made to existing disaster recovery plans.

Objective No. 1 – Determine if City IT systems are backed up appropriately and in a manner consistent with best practices.

<u>Best Practices and City Administrative Procedures.</u> Our audit showed that, although the City and its departments had implemented backup processes which were consistent in several respects with best practices, those City processes and/or the related City administrative procedures (Administrative Procedure 809) should be revised to:

- Include the Department of Management and Administration's Information System Services division (ISS), in addition to the applicable department managers, in decisions regarding the specifics as to what, when, and how backups should occur.
- Provide more specificity with respect to when the various backup types (e.g., full, differential, and incremental) and frequencies (e.g., daily, weekly, monthly, etc.) should be used/applied.
- Require periodic and documented tests of the integrity of backup files.
- Require the conduct and documentation of system recovery tests using the backed up files.

<u>Backup of City IT Systems</u>**.** For some City servers, we noted the frequency and types of backup used were reasonable and appropriate. We also found that the retention process and periods

utilized for these server backups were sufficient and provided adequate protection for City data.

For other City servers, we concluded the frequency and types of backups used were reasonable and appropriate. We did note, however, that the retention period utilized for these other server backups may not be sufficient and, as a result, recommend that management consider the adoption of a longer backup retention period to better protect the applicable data.

For certain City servers backed up to cassette tapes we also recommend security enhancements for the cassette tapes.

While an informal monitoring process was used for monitoring the results of the backup process, we determined establishment of a more formal monitoring process was appropriate. Accordingly, we recommend ISS develop for all City servers a formal process for reviewing and testing the results of backups and reporting and resolving the issues detected. Documentation of those monitoring efforts should be retained.

Objective No. 2 – Determine if plans and preparations for IT disaster recovery were reasonable, appropriate, and consistent with best practices.

City Policy and Procedure. Our audit efforts showed that although IT disaster recovery plans had been developed, there is currently no citywide policy or administrative procedure addressing disaster recovery planning for City IT system operations. We recommend a comprehensive City administrative policy or procedure be developed that gives consideration to incorporating applicable best practices.

Disaster Recovery Plans for City IT Systems. A disaster recovery plan (DR plan) should be comprehensive and address all areas relevant to the restoration of IT operations. Our review showed a reasonably comprehensive DR plan has been developed for City IT systems. For the most part, that DR plan is appropriately detailed and addresses areas such as roles and responsibilities of staff, pre-disaster preparation procedures, actions necessary in response to an emergency, the various alert levels in anticipation of an emergency, emergency assembly points for staff after a disaster, response procedures, and checklists. However, we did identify areas where improvements should be made. To address those areas, we recommend:

- Relevant staff identified in the DR plan are provided hard copies of the plan and informed as to the file location of electronic versions of the plan.
- A formal business impact analysis be prepared and documented to help ensure appropriate IT systems are addressed in the DR plan. Additionally, the DR plan should be revised as appropriate based on that formal business impact analysis.
- The DR plan be revised to either include relevant supporting documentation (e.g., manuals, configuration details, checklists) or references to specific locations where such documentation is retained. This supporting documentation should be treated as a part of the DR plan (i.e., with copies of the supporting documentation, in both electronic and hard copy format, provided to key personnel).
- The DR plan be amended to more directly and clearly identify computer hardware and infrastructure requirements so that, in the event replacement is necessary, information and specifications are readily available.
- Pre-approval be obtained for the emergency acquisition of computer hardware, applications, and other IT related items that may be necessary to restore critical IT systems designated in the DR plan. We also recommend this pre-approval be limited such that it is valid only in the event of an emergency, as declared by an appropriate City official (for example, the Mayor or City Manager).

- Consideration be given to the identification and/or verification of the City's critical applications, with appropriate update to the DR plan as a result.
- The DR plan be reviewed and updated as needed, with future, reviews/updates conducted on a regular basis.
- A schedule be developed for the periodic testing of the DR plan and such testing conducted.
- Consideration be given to relocating the alternate restoration site for most City IT systems to a different secured facility (resulting in potential annual savings of approximately $40,000).
- Consideration be given to establishment of an alternate restoration site for certain unique City IT systems for which an alternate restoration site has not been established.
- Because of their unique nature and requirements, separate DR plans that incorporate best practices be developed for certain City IT systems.
- Consideration be given to adding backup air conditioning capability, a high temperature alarm, a fire suppression system, and a fire/smoke alarm at a certain backup location where IT systems are located.

We would like to thank applicable City staff for their assistance during this audit.

Appointed Official's Response

City Manager:

I appreciate the work done by the City Auditor on the Backup and Recovery Planning Processes report. I am pleased that the City Auditor's report found that overall the City's data is being backed up in accordance with best practices. In addition, ISS has plans for disaster recovery for most systems. I am confident that all action items and recommendations will be addressed by their respective target date. I would like to thank the City Auditor and DMA/ISS for their efforts in this audit

Copies of this audit report #1515 may be obtained from the City Auditor's website (http://talgov.com/auditing/index.cfm) or via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (Office of the City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

Audit conducted by:

Dennis R. Sutton, CPA, Audit Manager
T. Bert Fletcher, CPA, CGMA, City Auditor