July 30, 2009

Internal Audit Report 2009-08
Information Technology Business Continuity Plan
Information Technology Department

Introduction. The Municipality depends heavily on technology and automated information systems, and their disruption for even a few days could have a severe impact on critical resources and affect essential services. The continued operations of the Municipality depend on management's awareness of potential disasters and ability to develop a plan to minimize disruption of daily operations. A business continuity plan is a comprehensive statement of consistent actions to be taken before, during, and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster.

The Municipality has a mainframe server that contains a variety of applications and records including PeopleSoft Financials which includes fixed asset management, PeopleSoft Human Resources which includes payroll, Computer Assisted Mass Appraisal for property assessment, and a tax system for tax billing and processing of payments for real and personal property tax. In addition, more than 200 other servers run a variety of applications such as the Municipality's e-mail system, the geographical information system, permit application data, and so forth.

Objective and Scope. The objective of this audit was to determine if a comprehensive plan had been developed and tested to ensure the continuity of operations in the event of a disaster. Specifically, we determined whether the Information Technology (IT) Department had identified the critical systems that must be continued without interruption in the event of a disaster, if systems and other resources required to support the critical services had been identified, and if a plan was updated as new systems and applications are developed and implemented. We did not include distributed computer hardware and software at Anchorage Water and Wastewater Utility, Municipal Light and Power, Anchorage Police Department, and so forth.

The audit was conducted in accordance with generally accepted government auditing standards, except for the requirement of an external quality control review, and accordingly, included tests of accounting records and such other auditing procedures as we considered necessary in the circumstances. The audit was performed during April 2009.

Overall Evaluation. The Municipality does not have a business continuity plan in the event of a disaster. We found that a business continuity disaster recovery plan had not been developed and implemented. As a result, the Municipality could face a variety of problems such as loss of critical data, inability to pay vendors, and penalties if it fails to pay employees on time. In addition, the handling and storage of back-up data tapes could be improved.

FINDINGS AND RECOMMENDATIONS

1. IT Business Continuity/Disaster Recovery Plan Not Developed.

a. **Finding.** A business continuity plan had not been developed and implemented. A business continuity plan helps ensure the Municipality's business continues without interruption if a disaster occurs, helps prevent confusion, reduces the chance of human error, prevents disruption of critical business functions, and minimizes potential economic loss and legal liability. The Municipality could face a variety of problems without a business continuity plan. For example, one union contract assesses a penalty if the Municipality fails to pay employees on time. In addition, vendors may not be paid, and tax assessment and real property data could be lost.

Although training manuals and templates were obtained by the IT Department to help develop a business continuity plan, a plan was not developed. Specifically, key components such as critical applications, a recovery site, procurement of replacement equipment, and personnel assignments in the event of a disaster had not been identified. Instead, IT Department staff told us that they have undocumented recovery procedures and just know what to do if a disaster strikes. According to the National Institute of Standards and Technology, "Information technology (IT) and automated information systems are vital elements in most business processes.

Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster."

b. **Recommendation.** The Director of the IT Department, in conjunction with other Municipal agencies, should develop and implement a comprehensive IT disaster recovery/contingency plan to provide continuity of operation of critical municipal applications in case of disaster.

c. **Management Comments.** Management concurred and stated,

"• IT will develop and implement an IT business continuity and disaster recovery plan that meets the requirements outlined in an overall Municipality Business Continuity plan in conjunction with other Municipal agencies. This would need to be approved (sponsored) at the level of the Municipal Manager to ensure all departments participate and meet any timelines outlined for this project.

"• IT agrees that the current business continuity and disaster recovery plans and procedures should be more thoroughly documented and brought up to date. IT will document current practices and procedures and develop detailed recovery plans. Timeline to complete – 1 year.

"• Once the recovery plans are developed IT will periodically test these plans to the extent possible using existing resources.

"• More extensive disaster recovery drills could be conducted if arrangements are made for a hot site. Recovery plans assume the existence of an infrastructure on which to implement the recovery. If the data center were destroyed this infrastructure would need to be partially recreated before recovery could begin. A hot site could substantially simplify and speed recovery in the event of an actual disaster but may be very costly."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

2. **Back-Up Data Tape Storage Could be Improved.**

a. **Finding.** The handling and storage of back-up data tapes could be improved. As discussed below, the IT Department backs up data from the main frame server and other servers.

- ***Main Frame Back-up -*** The primary back-up tapes for the main frame server and duplicate back-up tapes are created on site at the Data Center each day. The primary back-up tapes are stored at the Data Center. The duplicate back-up tapes are transferred to an off-site facility Monday thru Thursday. However, the duplicate back-up tapes made Friday thru Sunday are stored onsite until picked up on Monday. Since all back-up tapes are stored at the same location from Friday to Sunday, in the event of disaster, they could all be lost. In addition, the IT Department had no policies and procedures regarding main frame back-up tapes.

- ***Server Back-ups -*** The back-up tapes for servers are created on-site throughout the Municipality each day at six different facilities. Unlike the mainframe, only one back-up tape is created for each server. These back-up tapes are stored on site and transferred to an off-site facility twice a month. Since all back-up tapes are only moved off site twice a month, in the event of a disaster they could all be lost while stored at the on-site facilities. In addition, the IT Department had no policies and procedures regarding server back-up tapes.

The National Institute of Standards and Technology states that "It is good business practice to store backed-up data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility." It also states that ". . . backup media should be stored offsite in a secure, environmentally controlled facility."

b. **Recommendation.** The Director of the IT Department should develop a policy and procedure to ensure back-up tapes are properly stored offsite.

c. **Management Comments.** Management concurred and stated,

"*Mainframe Backups*

"• IT will develop and publish backup tape handling policies and procedures. Timeline – 3 months.

"• IT will reinstate a Friday pickup at the data center to transport mainframe backup tapes to offsite storage in addition to the transfers that currently occur Monday through Thursday. Timeline – immediately.

"• As long as backups are written to tape, there will be a lag between the time the backup tapes are taken, and the time the backup tapes are moved off site, therefore some vulnerability for data loss will always exist.

"• In lieu of pulling and transporting tapes over the weekend we will investigate the feasibility of electronically transferring key critical backups to a file system residing at another location.

"• Through the Business Continuity planning process we will evaluate our server backup and tape rotation policies and procedures to align them with business recovery requirements.

"*Distributed Server Backups*

"• IT will document and publish our current backup and tape handling policies and procedures. Timeline – 3 months

"• IT moves backup tapes for distributed servers off-site twice every month. To mitigate the vulnerability of data loss during the two week period where data is on-site, ITD plans to move the existing disk based backup to alternate locations. Disk based backups are currently performed in conjunction with tape based backups and are performed twice per day with a thirty (30) day retention cycle. Data for key sites will be protected with disk based backups from the Emergency Operations Center (EOC) and Dimond Data Center (DDC). In the event of a disaster, disk based backups provide the ability to access data quickly and with a minimum of data loss. ITD staff plan to relocate the existing disk based backup systems to the EOC and DDC once the current power and infrastructure upgrade projects are completed. Timeline - Based upon the current status of these projects the relocation should be completed within the next four months."

d. **Evaluation of Management Comments.** Management comments were responsive to the audit finding and recommendation.

Discussion With Responsible Officials. The results of this audit were discussed with appropriate Municipal officials on June 11, 2009.

Audit Staff:

Scott Lee