INTERNAL AUDIT REPORT

2013-01

Information Technology Business Continuity Plan Follow-Up

Information Technology Department

January 31, 2013

MUNICIPALITY OF ANCHORAGE
Internal Audit Department
632 W 6th Avenue, Suite 600
P.O. Box 196650
Anchorage, Alaska 99519-6650
www.muni.org/departments/internal_audit

INTERNAL AUDIT DEPARTMENT
Peter Raiskums, CIA, CFE, CGFM
Director
Phone: (907) 343-4438
Fax: (907) 343-4370
E-Mail: raiskumspw@muni.org

MUNICIPALITY OF ANCHORAGE

Internal Audit Department
632 W. 6th Ave., Suite 600

Phone: 907-343-4438
Fax: 907-343-4370

Mayor Dan Sullivan

January 31, 2013

Honorable Mayor and Members of the Assembly:

I am pleased to present **Internal Audit Report 2013-01, Information Technology Business Continuity Plan Follow-Up, Information Technology Department** for your review. A brief summary of the report is presented below.

In accordance with the 2012 Audit Plan, we have completed a follow-up audit of the Information Technology Business Continuity Plan. The objective of this audit was to conduct a follow-up audit to determine the effectiveness of corrective actions taken by the Information Technology Department on the deficiencies contained in Internal Audit Report 2009-08. Specifically, we determined whether the Information Technology Department had developed a business continuity/disaster recovery plan.

Based on our review, we determined that Management action taken in response to the 2009 audit did not fully correct the findings. Our follow-up audit revealed that action taken by Information Technology Department personnel had corrected one of the two deficiencies. However, we found that the Information Technology Department still had not developed a business continuity plan to facilitate the recovery of business operations in case of a disaster.

There was one finding in connection with this audit. Management was responsive to the finding and recommendation.

Peter Raiskums, CIA, CFE
Director, Internal Audit

MUNICIPALITY OF ANCHORAGE

Internal Audit Department
632 W. 6th Ave., Suite 600

Phone: 907-343-4438
Fax: 907-343-4370

Mayor Dan Sullivan

January 31, 2013

Internal Audit Report 2013-01
Information Technology Business Continuity Plan Follow-Up
Information Technology Department

Introduction. In 2009 we performed an audit of the business continuity plan of the Information Technology Department (IT) and issued Internal Audit Report 2009-08 dated July 30, 2009. To assess the effectiveness of corrective action, we have performed a follow-up audit. This report contains the result of our follow-up audit.

The Municipality of Anchorage (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 operation of the Municipality depends on management's awareness of potential disasters and ability to develop a plan to minimize the 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. With the recent implementation of the Kronos Workforce Management System and the upcoming implementation of SAP Enterprise Resource Planning System, having an effective business continuity plan is more important than ever.

The Municipality has a mainframe server that contains a variety of applications and records including financial management and human resource systems (PeopleSoft), Computer Assisted Mass Appraisal (CAMA) for property assessment, and a tax system for tax billing and processing of payments for real and personal property tax. In addition, more than 300 other servers run a variety of applications including the Municipality's time keeping system, e-mail system, the geographical information system, and permit application data.

Objective and Scope. The objective of this audit was to conduct a follow-up audit to determine the effectiveness of corrective actions taken by IT on the deficiencies contained in Internal Audit Report 2009-08. Specifically, we determined whether IT had developed a business continuity/disaster recovery plan.

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 October 2012.

Overall Evaluation. Management action taken in response to the 2009 audit did not fully correct the findings. Our follow-up audit revealed that action taken by IT personnel had corrected one of the two deficiencies. However, we found that IT still had not developed a business continuity plan to facilitate the recovery of business operations in case of a disaster.

AUDIT FINDINGS FOLLOW-UP

1. **Prior Finding: IT Business Continuity/Disaster Recovery Plan Not Developed.** A business continuity plan had not been developed and implemented.

    a. **Corrective Action.** Our audit revealed that IT still had not developed a business continuity plan to facilitate the recovery of business operations in case of a disaster. As a result, there is a risk of costly service interruptions. Although a draft plan was provided to us for review, it appears to have not been worked on since February 2012 and was incomplete. For example, the draft plan did not include recovery procedures for PeopleSoft and CAMA. In addition, the draft plan made no mention of the

Municipality's implementation of the SAP system which impacts critical Municipal functions such as Finance, Employee Relations, Budget, Procurement, Grants Management, and Project Management.

Moreover, our review found that the draft plan was prepared with a copyrighted template. However, IT staff was unable to provide proof that the copyrighted template was legally obtained.

A business continuity plan helps ensure that if a disaster occurs the Municipality's business continues without interruption. In addition, it helps prevent confusion, reduces the chance of human error, helps prevents the disruption of critical business functions, and minimizes potential economic loss and legal liability. The National Institute of Standards and Technology Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, stated that "Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption."

b. **Evaluation of Corrective Action.** Not effective.

c. **Recommendation.** The IT Director, 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.

d. **Management Comments.** Management stated, "ITD concurs with this finding. ITD also concurs with the sub-finding that a copyrighted template was used to start the Draft Systems Continuity Plan.

"Actions that were taken:

"1. ITD began development of a Systems Continuity Plan in August 2009. The approach was to develop a high-level plan to include all services IT provides MOA and the resources required to recover in the event of a disaster; details of recovery for each service was to follow once the high-level plan was complete.

"2. ITD updated the draft Plan in early 2012 to reflect changes in ITD staffing, positions, contact information, etc.. Detailed documentation of service recovery remained incomplete due to both the imminent changes due to Kronos and SAP implementations, and the priority of Kronos and SAP resourcing.

"3. Extensive planning has been performed for High Availability or Disaster Recovery for both Kronos and SAP as part of those implementations, and related Processes and Procedures are key deliverables for those critical enterprise projects.

"4. ITD continues to actively participate with Emergency Management and MOA Public Safety agencies in all Business Continuity and related exercises and tests. We recently assumed management control over power infrastructure at the EOC in order to update critical infrastructure and establish maintenance contracts covering critical devices.

"5. Through rigorous application of enterprise-wide IT standards, and an aggressive program of consolidation and virtualization of MOA servers, ITD has greatly simplified our production operating environment. This is viewed as a critical precursor activity to finalization of the Systems Continuity Plan.

"6. In Q4 2012 MOA developed and began implementation of new network management systems and processes and procedures covering critical network communications infrastructure and servers.

"Actions planned to be taken:

"1. In conjunction with other Municipal agencies and business units, ITD will complete and implement the comprehensive Systems Continuity Plan. (Q2 2014)

"2. ITD will work with Purchasing [*sic*] to validate proper procurement of any commercial product used to support our operations. (Q1 2013)

"3. Deployment of the new Network Management Systems will soon be complete. (Q1 2013)"

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

2. Prior Finding: Back-Up Data Tape Storage Could be Improved. The handling and storage of back-up data tapes could be improved.

a. **Corrective Action.** Our audit revealed that IT had made improvements in the handling and storage of back-up data tapes.

b. **Evaluation of Corrective Action.** Effective.

c. **Recommendation.** Not required.

Discussion With Responsible Officials. The results of this audit were discussed with appropriate Municipal officials on November 15, 2012.

Audit Staff:
Scott Lee