INTERNAL AUDIT REPORT

2019-07

Information Technology Business Continuity Plan

Office of Information Technology

August 8, 2019

MUNICIPALITY OF ANCHORAGE
Internal Audit Department
632 W 6th Avenue, Suite 710
P.O. Box 196650
Anchorage, Alaska 99519-6650
www.muni.org/departments/internal_audit

INTERNAL AUDIT DEPARTMENT
Michael Chadwick, CIA, CICA
Director
Phone: (907) 343-4438

E-Mail: michael.chadwick@anchorageak.gov

Municipality of Anchorage

Ethan Berkowitz, Mayor

Internal Audit Department

August 8, 2019

Honorable Mayor and Members of the Assembly:

I am pleased to present for your review **Internal Audit Report 2019-07, Information Technology Business Continuity Plan, Office of Information Technology**. A brief summary of the report is presented below.

In accordance with the 2019 Audit Plan, we have completed an audit of the Information Technology Business Continuity Plan. The objective of this audit was to determine if a comprehensive business continuity plan has been developed and tested to ensure the Municipality of Anchorage's continuity of operations in the event of a disaster. To accomplish our objective, we determined whether the Office of Information Technology had identified the critical systems that must be continued without interruption in the event of a disaster, if systems and other resources to support the critical services had been identified, and if a plan was updated as new systems and applications were 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, etc.

Our audit revealed that the Municipality of Anchorage has not fully developed and implemented a business continuity plan in the event of a disaster. A similar condition was reported in previous Internal Audit Report 2009-08 and Internal Audit Report 2013-01.

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

Michael Chadwick

Michael Chadwick, CIA, CICA
Director, Internal Audit

Municipality of Anchorage

Ethan Berkowitz, Mayor

Internal Audit Department

August 8, 2019

Internal Audit Report 2019-07
Information Technology Business Continuity Plan
Office of Information Technology

Introduction. 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 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. Currently, the Municipality's Enterprise Resource Planning System, SAP, is hosted on the SAP Hana Enterprise Cloud (HEC) environment (i.e. out-of-state). The Office of Information Technology (OIT) plans to bring SAP back to the Municipality to be hosted at the Municipality's Data Center. At the time of this audit, this plan had not yet been finalized.

With the recent implementation of SAP and the Municipality's plan to change the SAP hosting from the HEC environment to the Municipality's Data Center, having an effective business continuity plan is more important than ever.

The Municipality has a mainframe computer that supports the Computer Assisted Mass Appraisal (CAMA) for property assessment and tax system for billing and processing of payments for real and personal property tax. In addition, almost 400 virtual servers run a variety of applications such as the Municipality's e-mail system, telephone system, budgeting system, and numerous databases essential for Municipality's daily operations.

Objective and Scope. The objective of this audit was to determine if a comprehensive business continuity plan has been developed and tested to ensure the Municipality's continuity of operations in the event of a disaster. Specifically, we determined whether OIT had identified the critical systems that must be continued without interruption in the event of a disaster, if systems and other resources to support the critical services had been identified, and if a plan was updated as new systems and applications were 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, etc.

We conducted this performance audit in accordance with generally accepted government auditing standards, except for the requirement of an external quality control review. Those standards require that 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit was performed during the period of April through June 2019.

Overall Evaluation. The Municipality has not fully developed and implemented a business continuity plan in the event of a disaster. A similar condition was reported in previous Internal Audit Report 2009-08 and Internal Audit Report 2013-01.

FINDING AND RECOMMENDATION

1. Business Continuity Plan Not Fully Developed.

a. **Finding.** A business plan to facilitate the continuity and recovery of business operations in case of a disaster had not been fully developed and implemented. Since there was not a functioning business continuity plan, there has been no testing, training, and simulated exercises to validate the Municipality's recovery capabilities and identify planning gaps for future plan improvement. As a result, there is a risk of costly service interruptions. The Municipality could face a variety of problems without a business continuity plan. For example, disruption of the Municipality's email and telephone systems will impair its daily operations. In addition, vendors may not be paid, and tax assessments and real property data could be lost.

Although OIT management provided a draft "Disaster Recovery & Business Continuity Plan," (Plan) it did not include some key components. For example, conducting a business impact analysis and recovery procedures for applications that impact critical municipal functions, such as the Municipality's CAMA database for real and business personal property, were not covered in this draft Plan.[1] Plan development got stalled when an employee who oversaw it left the Municipality, and this position was eliminated due to a reorganization of OIT.

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. National Institute of Standards and Technology Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, states that "Information systems are vital elements in most mission/business processes. 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." A similar condition was reported in previous Internal Audit Report 2009-08 and Internal Audit Report 2013-01.

[1] One of the key assumptions of the Plan is that SAP will not be affected by the various scenarios addressed in the Plan since SAP is accessible via a contractor's cloud location. However, the Plan did not address the contractor's recovery procedures, nor did it address the Municipality's strategy to host SAP locally within Anchorage, which has not yet been finalized.

b. **Recommendation.** The Chief Technology Officer, in conjunction with other Municipal agencies, should finalize the draft "Disaster Recovery & Business Continuity Plan" and implement it to ensure the operational continuity of critical municipal applications in the event of a disaster.

c. **Management Comments.** Management stated, "After review, the Office of Information Technology is in concurrence with the singular finding of which the Business Continuity Plan requires further development. A plan of action will be taken to correct this deficiency and finalize the Disaster Recovery & Business Continuity Plan. This plan will include testing, training and analysis to ensure that our team will properly support the Municipality in the event of a disaster.

"As always, the protection of Municipal resources, information, and citizens is the highest priority for the Office of Information Technology."

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 July 11, 2019.

Audit Staff:
Scott Lee