IT Audit Risk Assessment: Phase 1
Special Advisory Service

December 2010

Dennis J. Gallagher
Auditor

The **Auditor** of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver's government. He also chairs the City's Audit Committee and oversees the City's Comprehensive Annual Financial Report (CAFR)

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City's finances and operations, including the integrity of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Dennis Gallagher, Chair	Robert Bishop
Maurice Goodgaine	Robert Haddock
Jeffrey Hart	Bonney Lopez
Timothy O'Brien	

Audit Staff

Audrey Donovan, Deputy Director, CIA
Stephen E. Coury, IT Audit Supervisor, CISA
Robert Pierce, Lead IT Auditor, CISA

You can obtain free copies of this report by contacting us at:

Office of the Auditor

201 West Colfax Avenue, Department 705 ⬥ Denver CO, 80202

(720) 913-5000 ⬥ Fax (720) 913-5026

Or download and view an electronic copy by visiting our website at:

www.denvergov.org/auditor

City and County of Denver

201 West Colfax Avenue, Department 705 • Denver, Colorado 80202 • 720-913-5000 •
FAX 720-913-5247 • www.denvergov.org/auditor

Dennis J. Gallagher
Auditor

December 13, 2010

Ms. Molly Rauzi, Chief Information Officer
Technology Services
City and County of Denver

Dear Ms. Rauzi:

Attached is the Auditor's Office Audit Services Division's special advisory service report for their Information Technology (IT) Audit Risk Assessment: Phase 1. The purpose of the IT audit risk assessment was to assist in our audit planning process to ensure resources are applied to auditing the highest risk IT areas. Results from this first phase were included in the Office of the Auditor's 2011 Audit Plan.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5029.

Sincerely,

Dennis J. Gallagher
Auditor

DG/sec

cc: Honorable John Hickenlooper, Mayor
        Honorable Members of City Council
        Members of Audit Committee
        Mr. Jack Finlaw, Chief of Staff
        Ms. Erin Trapp, Deputy Chief of Staff
        Mr. Claude Pumilia, Chief Financial Officer
        Mr. David Fine, City Attorney
        Mr. L. Michael Henry, Staff Director, Board of Ethics
        Ms. Lauri Dannemiller, City Council Executive Staff Director
        Ms. Beth Machann, Controller
        Mr. Chuck Fredrick, Deputy Chief Information Officer
        Mr. Ethan Wain, Deputy Chief Information Officer

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people. We will monitor and report on recommendations and progress towards their implementation.

City and County of Denver

201 West Colfax Avenue, Department 705 ● Denver, Colorado 80202 ● 720-913-5000

FAX 720-913-5247 ● www.denvergov.org/auditor

Dennis J. Gallagher

Auditor

AUDITOR'S REPORT

We have completed the special advisory service for Information Technology (IT) Audit Risk Assessment: Phase 1. The purpose of the IT audit risk assessment was to assist in our audit planning process to ensure resources are applied to auditing the highest risk IT areas. Results from this first phase were included in the Office of the Auditor's 2011 Audit Plan.

This report summarizes part of our planning process and is a non-audit service, and as such, is exempt from the rigors of test work as directed by government auditing standards. No agency response is required for this report and there are no audit findings requiring resolution and audit follow-up.

We extend our appreciation to the personnel who assisted and cooperated with us during this assessment.

Audit Services Division

Kip Memmott, MA, CGAP, CICA
Director of Audit Services

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people. We will monitor and report on recommendations and progress towards their implementation.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction

This special advisory service report completes the first phase of an Information Technology (IT) audit risk assessment. The purpose of this assessment was to assist in our annual audit planning process to ensure we apply our resources to auditing the highest risk IT areas. Our risk assessment model includes ranking both technical process maturity and qualitative factors. We ranked the risk of the critical business applications, IT processes, IT facilities, and IT infrastructure that are supported by Technology Services. The results of the assessment identified specific IT audits which were incorporated into the Auditor's 2011 Audit Plan.

Phased Approach

City agencies utilize a large number of information systems which are supported by multiple technology organizations. In order to conduct the risk assessment most efficiently, it was organized into three phases:

- Shared (or consolidated) services under the direct management of the City's Technology Services department;

- IT services not under the direction of Technology Services, excluding the Denver International Airport (DIA); and

- The IT services managed directly by divisions at DIA.

As noted above, the results from the first phase were included in the 2011 audit plan. The results from subsequent phases will be merged into our knowledge base to support continued audit planning.

Observation

As we identified and ranked the risk for various audit areas, we observed that several City agencies utilize vendors for World Wide Web services. We also noted that the responsibility for managing the City's presence on the World Wide Web does not clearly reside with Technology Services or with any of the City's other technology organizations.

Upon viewing the various agency web sites we noticed inconsistencies in both the appearance of web pages and their respective web addresses, making it unclear whether the City has an official web presence. Ambiguities in web presence could be exploited to mislead the Citizenry on how to obtain City services or where to direct payments. This confusion could also lead to identity theft or loss of City revenues. See the Exhibits section of this report for examples
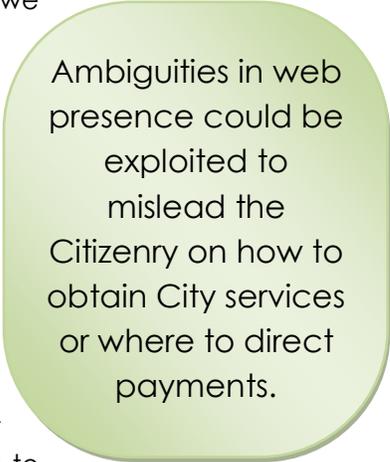
> Ambiguities in web presence could be exploited to mislead the Citizenry on how to obtain City services or where to direct payments.

of various City web appearances and addresses. Although the risk of an inconsistent web presence has been entered into our knowledge base, it did not rank high enough for inclusion in the Office of the Auditor's 2011 Audit Plan.

Conclusion

Results from the IT audit risk assessment identified specific IT audits which were included in the Office of the Auditor's 2011 Audit Plan. The plan includes the following three IT audits in addition to standard audit follow-up work:

- DIA Network Security,
- OASIS/CAMA IT General Controls, and
- OSI IT General Controls and Performance Audit.

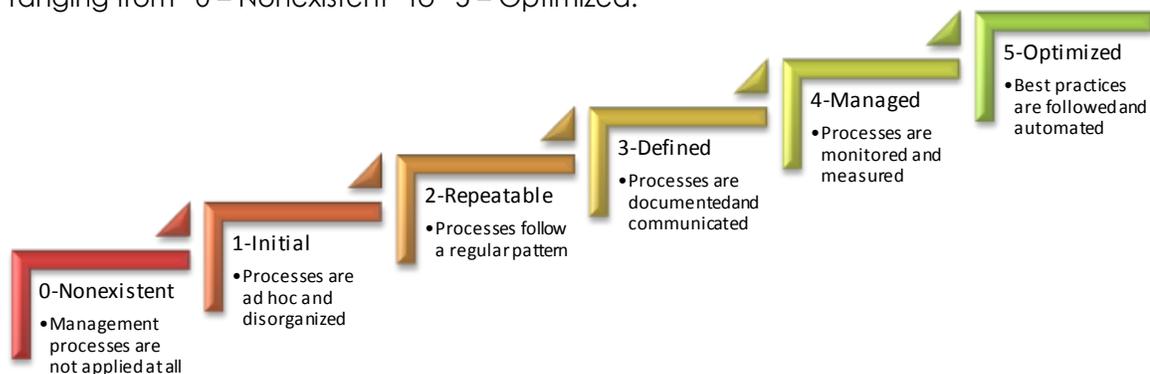See the following report for more details about the above IT audits.

INTRODUCTION & BACKGROUND

Technology Services

Technology Services is the central information technology and telecommunications department supporting the City and County of Denver. Technology Services provides project management, business analysis, data network, telephone, application development, software support, and electronically delivered communication services for internal and external customers. Technology Services supports 338 application systems and 64 IT equipment facilities.

COBIT Maturity Model

COBIT[1] is a widely accepted IT governance framework. As illustrated below, the model establishes a method for ranking IT process maturity according to a six point scale ranging from "0 – Nonexistent" to "5 – Optimized."

5-Optimized
- Best practices are followed and automated

4-Managed
- Processes are monitored and measured

3-Defined
- Processes are documented and communicated

2-Repeatable
- Processes follow a regular pattern

1-Initial
- Processes are ad hoc and disorganized

0-Nonexistent
- Management processes are not applied at all

SCOPE

This risk assessment is a special advisory service and provides information based on a limited review. This report summarizes part of our planning process and is a non-audit service, and as such, is exempt from the rigors of test work as directed by government auditing standards.

The IT audit risk assessment is designed to gather information necessary for planning both short-term and long-term IT audit plans. The assessment is not a business impact analysis that would be used for contingency planning. Our work was conducted during the period of March 30, 2010 through August 2, 2010.

---

[1] Control Objectives for Information and related Technology (COBIT) 4.0, IT Governance Institute, http://www.itgi.org

OBJECTIVE

The purpose of the IT audit risk assessment was to assist in our audit planning process to ensure resources are applied to auditing the highest risk IT areas.

METHODOLOGY

In developing our approach for the IT audit risk assessment we incorporated the Control Objectives for Information and related Technology (COBIT) framework as published by the IT Governance Institute.[2] COBIT is a leading IT governance framework and identifies generally understood IT controls. We also utilized guidance from the Institute of Internal Auditors.[3]

We developed a data collection tool in Microsoft Excel which includes criteria for ranking risk according to the process maturity of technical COBIT areas, as well as qualitative factors.

The COBIT technical areas included:

- restricted access,
- change control,
- computer operations,
- backup, and
- recovery.

Qualitative factors included:

- compliance with regulations,
- public health and safety,
- past audit findings,
- auditor judgment,
- fraud potential, and
- management request.

The evidence gathering and analysis techniques used to meet our audit objectives included, but were not limited to:

- Interviewing personnel in Technology Services;
- Ranking the risk of selected IT areas; and
- Reviewing results with management.

---

[2] COBIT 4.0, IT Governance Institute, http://www.itgi.org
[3] Institute of Internal Auditors, Global Technology Audit Guide #11, Developing the IT Audit Plan

RESULTS

Risk assessing all 338 application systems would have proved to be an unwieldy undertaking and would have caused a heavy burden on Technology Services personnel. As an alternative to reviewing each application, we worked with managers to identify the most critical business systems, as well as, those with the least mature support processes. This led to ranking the risk of a sample of 36 critical business applications, IT processes, IT facilities, and IT infrastructure for risk ranking.

The results of this first phase of our IT audit risk assessment process were incorporated into the Office of the Auditor's 2011 Audit Plan. The following table is reflected in the plan's Attachment A: Listing of Planned Audits.[4]

Audit Title	Department	Audit Type	Audit Objective
DIA Network Security	Denver International Airport	Internal Controls	To assess the efficiency and effectiveness of overall network infrastructure security management including but not limited to: firewall and router configuration and patch management, intrusion prevention and detection, logging and event correlation and monitoring, and wireless access configuration management.
OASIS/CAMA IT General Controls	Technology Services	Internal Controls	To assess the effectiveness of the IT General Controls supporting the City's property tax system including but not limited to: server operating system security (privileged access), server patch management, antivirus controls, change management, user access, vendor support, and system supportability.
OSI IT General Controls and Performance Audit	Technology Services / Denver Police Department	Economy and Efficiency	To assess the efficiency and effectiveness of the IT General Controls supporting the Denver Police Department's Office of Safety Information (OSI) System including but not limited to: server operating system security (privileged access), server patch management, antivirus controls, change management, user access, vendor support, and system supportability. The audit scope will include an assessment of National Incident Based Reporting System (NIBRS) for police crime statistics.
Audit Follow-up	Citywide	N/A	Past audits are followed-up to ensure agreed upon audit findings and recommendations are being implemented in a timely and effective manner. Although several IT audits may be due for follow-up, they are not specifically called out in the 2011 Audit Plan.

---

[4] City and County of Denver Office of the Auditor 2011 Audit Plan, http://www.denvergov.org/auditor

EXHIBITS

Samples of Denver's Web Presence
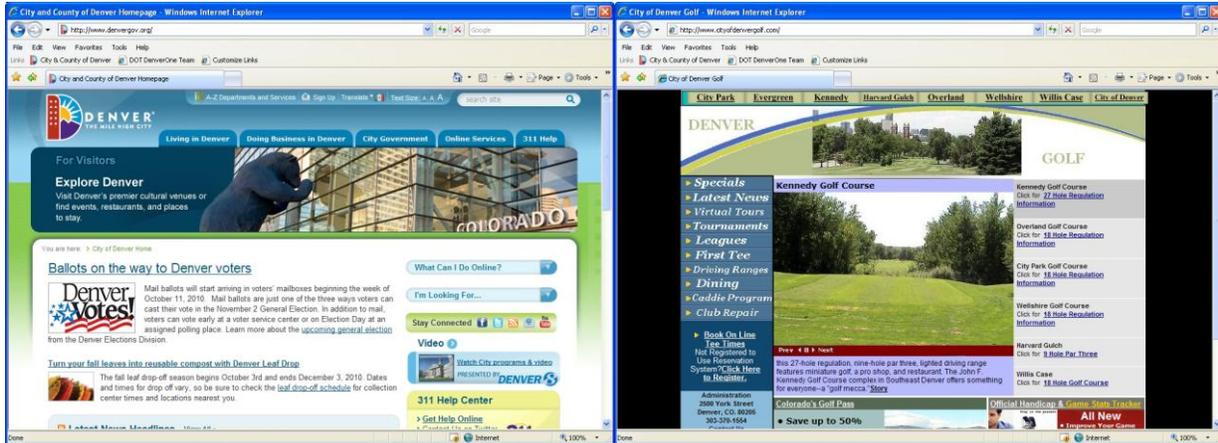
Above: www.denvergov.org

Managed by Technology Services

Above: www.cityofdenvergolf.com

Vendor: North American Golf Experience

Above: www.denverpvb.com
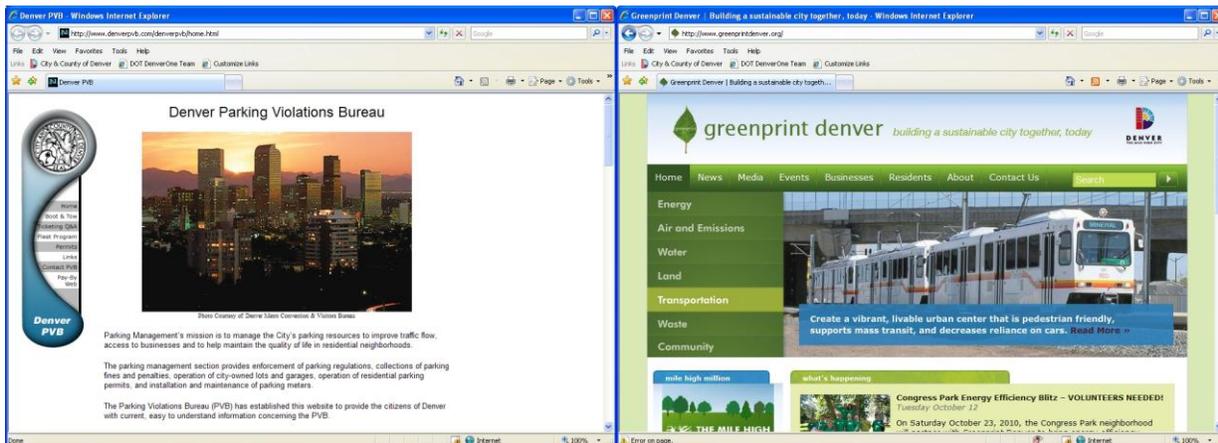
Vendor: ACS State and Local Solutions

Above: www.greenprintdenver.org

Vendor: Viawest