AUDIT REPORT

Public Works Asset Management Software Applications

Department of Public Works and Technology Services Agency

January 2020

Office of the Auditor
Audit Services Division
City and County of Denver
Timothy M. O'Brien, CPA
Denver Auditor

Audit Team

Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director
Brenda Berlin, CPA, IT Audit Supervisor
Karin Doughty, CISA, Lead IT Auditor
Joe Ebiziem, CISA, Senior IT Auditor

Audit Management

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ♦ Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at: www.denverauditor.org.

Cover photo by Auditor's Office staff.

Timothy M. O'Brien, CPA
Auditor

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202
(720) 913-5000 • Fax (720) 913-5253 • www.denverauditor.org

January 16, 2020

AUDITOR'S LETTER

The objective of our audit of the Department of Public Works' asset management software applications was to determine whether the information technology general controls are effective for two of the asset management software applications managed by Public Works and the city's Technology Services agency. I am pleased to present the results of this audit.

The audit revealed the city needs to establish citywide policies for information technology general controls and spreadsheet controls and both Public Works and Technology Services need to improve their oversight of cloud-based vendors. The controls over information technology contracts need strengthening, and Technology Services needs to improve its customer service. Additionally, Public Works needs to formalize its strategy for managing its infrastructure assets.

Creating standardized citywide information technology policies, improving the contracting processes for technology purchases, and strengthening vendor oversight will create a stronger cybersecurity approach for protecting the city's data. Developing a best practice to establish spreadsheet controls will protect critical financial and operational data. Improving the way Technology Services supports other city agencies will lower costs and help streamline overall operations. Finally, formalizing Public Works' infrastructure asset management will prevent wasted efforts and provide leadership with meaningful data to improve services provided to Denver's residents. Our report lists several related recommendations.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, "General Powers and Duties of Auditor," and was conducted in accordance with 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.

We extend our appreciation to the Public Works and Technology Services personnel who assisted and cooperated with us during the audit. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

Public Works Asset Management Software Applications

January 2020

Objective

To evaluate the design and the operating effectiveness of the information technology general controls, specific application controls, and financial reporting for infrastructure assets tracked in the Cartegraph and dTIMS asset management systems. Also, to assess the shared responsibility between the Department of Public Works and the city's Technology Services agency to define and implement information technology general controls.

Background

The Department of Public Works uses asset management application software to track and report on the city's $2.8 billion investment in streets, alleys, traffic signals, sewers, and other related infrastructure assets it manages. The city's Technology Services agency provides technical support services to keep these applications fully functional.

REPORT HIGHLIGHTS

Highlights

The Lack of Formal Citywide Policies for Information Technology Processes to Guide Agency Procedures Creates Cybersecurity and Operational Risks

- Technology Services does not have the explicit authority to create and enforce citywide information technology policies.
- The lack of documented information technology controls places the Department of Public Works' infrastructure asset data at risk.
- The lack of a formal citywide best practice for spreadsheet controls results in errors in Public Works' fixed asset accounting and reporting data.

Poor Vendor Oversight Puts Asset Management Data at Risk

- There is no effective review of cloud-based vendors' information technology general controls.
- Public Works did not obtain and review vendors' insurance coverage for dTIMS and Cartegraph.

The City's Contracting Process Failed to Include Technology Services' Required Review and Approval of a Technology Purchase

- Technology Services did not review the Cartegraph contract, which resulted in the city purchasing unneeded licenses.
- The Cartegraph contract did not clearly specify who is responsible for backup of city data in line with best practices.

Technology Services Should Expand its Existing Business Relationship Management Program to Include the Public Works Department to Provide Better Customer Service

- Technology Services failed to respond to requests from Public Works to ensure appropriate security processes were established.
- Technology Services has not communicated the process for updating citywide geographic information system data.

The Public Works Department Does Not Have a Formal Strategy for Asset Management

Public Works identified the need to expand its asset management plan, but it lacks a comprehensive asset management plan.

For a copy of this report, visit www.denverauditor.org or contact the Auditor's Office at (720) 913-5000.

TABLE OF CONTENTS

BACKGROUND 1

FINDING 1 7

The Lack of Formal Citywide Policies for Information Technology Processes to Guide Agency Procedures Creates Cybersecurity and Operational Risks

Technology Services Does Not Have the Explicit Authority to Create and Enforce Citywide Information Technology Policies 7

The Lack of Documented Information Technology Controls Places the Department of Public Works' Infrastructure Asset Data at Risk 10

The Lack of a Formal Citywide Policy for Spreadsheet Controls Results in Errors in Public Works' Fixed Asset Accounting and Reporting Data 15

FINDING 2 18

Poor Vendor Oversight Puts Asset Management Data at Risk

There Is No Effective Review of Cloud-Based Vendors' Information Technology General Controls 20

Public Works Did Not Obtain and Review Vendors' Insurance Coverage for dTIMS and Cartegraph 23

FINDING 3 26

The City's Contracting Process Failed to Include Technology Services' Required Review and Approval of a Technology Purchase

FINDING 4 29

Technology Services Should Expand its Existing Business Relationship Management Program to Include the Public Works Department to Provide Better Customer Service

Technology Services Failed to Respond to Requests from Public Works to Ensure Appropriate Security Processes Were Established 29

Technology Services Has Not Communicated the Process for Updating Citywide Geographic Information System Data 31

FINDING 5 33

The Public Works Department Does Not Have a Formal Strategy for Asset Management

RECOMMENDATIONS 37

TABLE OF CONTENTS, continued

AGENCIES' RESPONSES TO AUDIT RECOMMENDATIONS **45**

OBJECTIVE, SCOPE, AND METHODOLOGY **64**

BACKGROUND

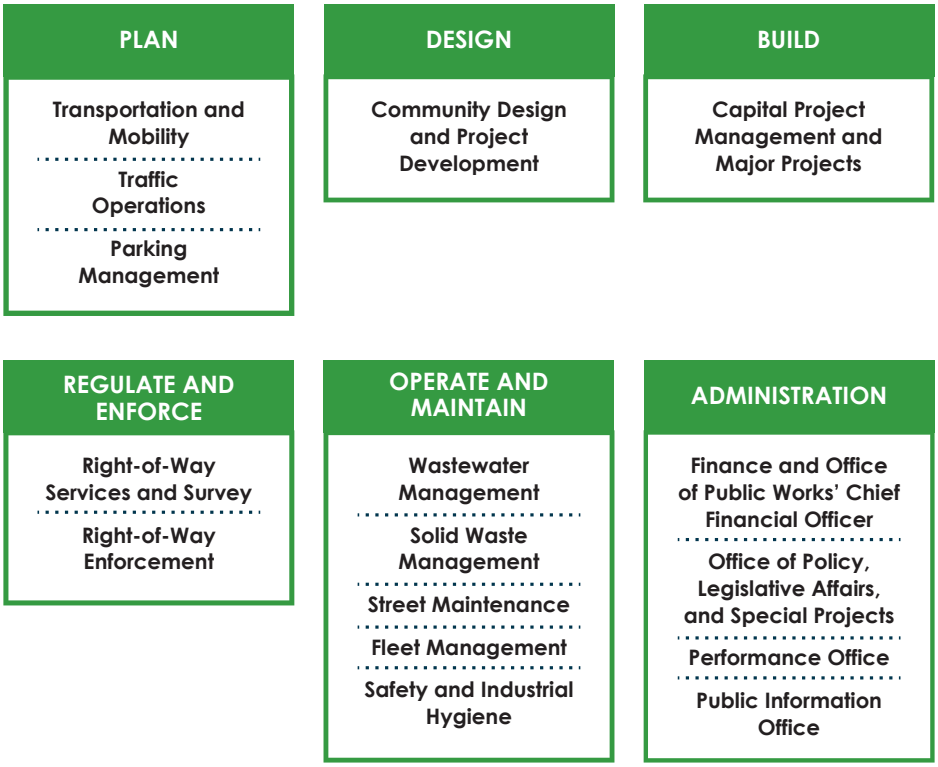
The Department of Public Works

The Department of Public Works is responsible for:

- Road maintenance and repair;
- Collection of residential trash, recycling, and compost;
- Design and construction of streets, bridges, public buildings, and storm and sanitary sewers;
- Mobility and parking services; and
- Oversight and regulation of the use of public rights of way.

Public Works is organized around six primary services as noted in Figure 1. These are: planning, design, building, regulation and enforcement, operation and maintenance, and administration.

FIGURE 1. Public Works Department Primary Services



Source: Department of Public Works.

To provide these services in 2019, the department received a budget of over $321 million. In addition to this operating budget, Public Works had over $353 million in ongoing capital projects for 2019, as shown in Table 1.[1]

TABLE 1. Ongoing Capital Projects in 2019

Budgeted Capital Project Categories	Recommended 2019 Budget
Capital Improvements	$109,245,949
Bond Project Funds	$184,650,739
Grant and Other Capital Funds	$16,989,000
Wastewater Management	$42,737,796
TOTAL	**$353,623,484**

Source: Mayor's 2019 Budget.

As of Dec. 31, 2018, Public Works managed $2.8 billion in infrastructure assets, as shown in Table 2 on the following page. These assets include the city's roads, alleys, bridges, sewers, storm drains, and traffic signals. They make up the underlying infrastructure for the city. All city operations — from the location of homes and businesses to the roads residents drive on — depend on the existence and function of these critical infrastructure assets.

Public Works uses asset management software applications designed to track, report, and manage infrastructure assets throughout the assets' life cycle, from acquisition to disposal. These software applications allow Public Works to track the condition of assets — from streets to sewers — and to help identify when they require maintenance or repairs. The department uses the following six asset management systems:

1. IPS – manages parking meters
2. Cartegraph – manages street signals, signage, and the city's fiber optics network
3. INFOR – manages city-owned bridges
4. Lucity – manages sewer and stormwater systems
5. dTIMS – manages streets, alleys, curbs, gutters, and curb ramps
6. FASTER – manages Public Works' fleet management operations

[1] City and County of Denver, Mayor's 2019 Budget (2019), accessed Oct. 21, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/344/documents/Budget/2019/2019_Budget%20Book_V2-OnlineVersion-compressed.pdf.

TABLE 2. Total Acquisition Cost of Infrastructure Assets Managed by the Department of Public Works, 2017 and 2018

Asset Type	Dec. 31, 2017	Dec. 31, 2018
Transportation Assets		
Alleys	$81,748,632	$82,276,549
Street Network	$854,259,606	$901,009,164
Bridges	$517,328,994	$518,517,635
Traffic Signals	$186,446,252	$192,594,492
Dynamic Message Signs	$1,302,298	$1,302,298
Subtotal	**$1,641,085,783**	**$1,695,700,137**
Wastewater Assets		
Land and Construction in Progress	$100,211,000	$115,349,000
Buildings and Improvements	$17,975,000	$17,975,000
Sewer and Stormwater Lines	$834,944,000	$969,110,000
Machinery and Equipment	$15,165,000	$14,629,000
Intangible Assets	$6,125,000	$6,375,000
Subtotal	**$974,420,000**	**$1,123,438,000**
GRAND TOTAL	**$2,615,505,783**	**$2,819,138,137**

Source: 2017 and 2018 comprehensive annual financial reports and the Department of Public Works.

Public Works started using Cartegraph in 2017 to manage the city's traffic control devices — including traffic signs and 11,300 traffic signals — and the fiber optics network that connects them. It provides the specific location and details for each asset.

For example, Cartegraph has a built-in catalog of all standard traffic control devices, so Public Works personnel can select a specific traffic sign and automatically load all related data such as size, shape, and an image of the sign. This provides consistent and accurate data on the city's traffic signage.

dTIMS tracks the condition of the city's 2,000 miles of streets and 463 miles of alleys. Working with the software vendor, Public Works created specific software applications capable of running on city-owned tablets, which are used to conduct surveys to report on the condition of the 2,500 miles of streets and alleys.

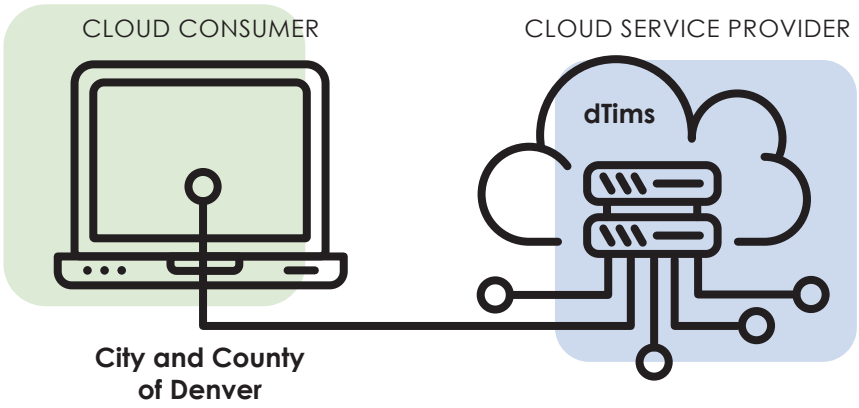
Using this data, dTIMS creates a digital model of the condition of the transportation infrastructure. Management then uses this digital model to project and prioritize the future repair and replacement needs for the city's streets and alleys. Current construction activity is tracked in dTIMS, including the location of the work, type of work performed, and the cost to repair or replace the street or alley. dTIMS also provides the new transportation asset costs, which are included in the city's Comprehensive Annual Financial Report.

Technology Services

The city's Technology Services agency is responsible for providing support for technology infrastructure including software development, technical support, and technology solutions to all city departments including Public Works. This includes providing information technology support services ranging from providing email and computer support to providing project management services for implementing new software applications.

Technology Services assisted Public Works in moving Cartegraph and dTIMS to cloud-based systems in 2017. As illustrated in Figure 2, cloud-based systems provide access and support for software systems without requiring the city to invest in new computer hardware.

FIGURE 2. Representation of Cloud-Based Service Model



Source: Image designed by Auditor's Office staff.

In the case of Cartegraph and dTIMS, the specific type of cloud-based service is called "hosted services." In hosted services, the vendor provides the hardware required to run the software at the vendor's locations. Public Works uses the internet to access these systems.

The benefit of hosted services includes the ability of a vendor to ensure the hardware and software are always up to date. In addition, the city does not have to maintain any additional hardware or hire and train

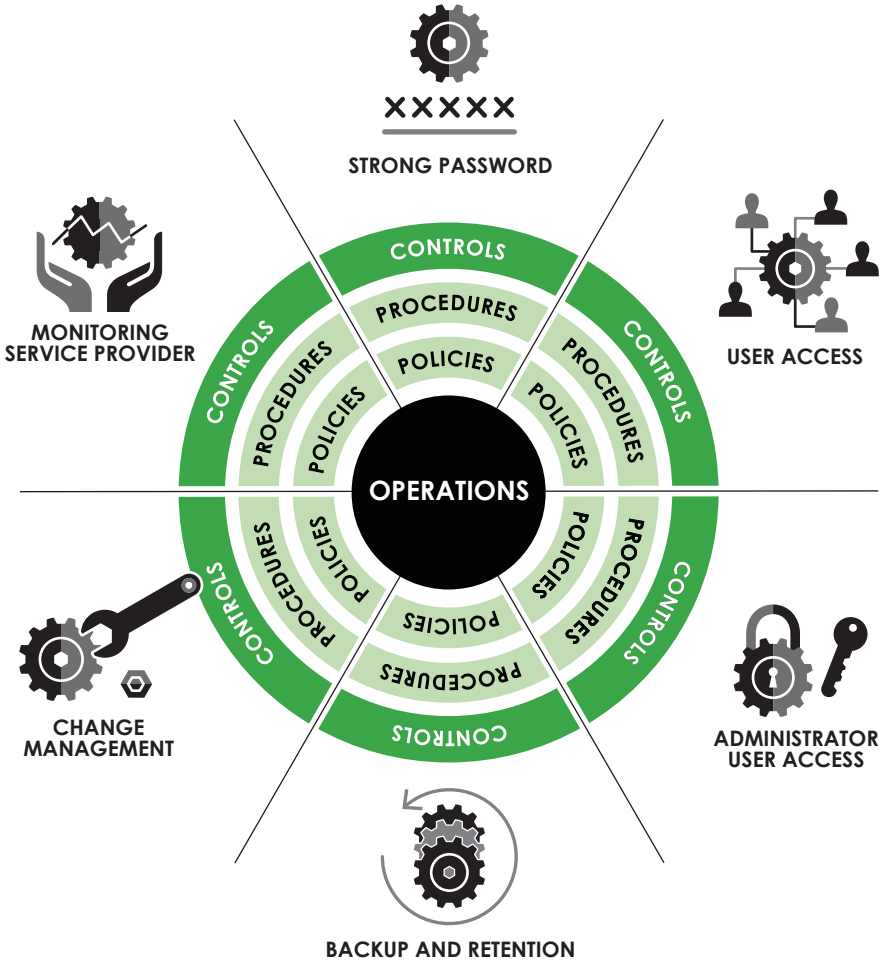
technology personnel to provide the specific support needed to keep these software systems running.

Shared Responsibility Between the Public Works Department and the Technology Services Agency

Because both Cartegraph and dTIMS are hosted by their respective vendors, there is a shared responsibility between Technology Services and Public Works to ensure the appropriate information technology general controls are in place and working.

All organizations should have their own unique set of internal controls to ensure the organization's objectives are achieved in the most efficient and effective way while still complying with laws, regulations, and policies.[2] This includes information technology general controls, as shown in Figure 3.

FIGURE 3. Representation of Information Technology General Controls



Source: Image designed by Auditor's Office staff.

[2] U.S. Government Accountability Office, GAO-14-704G, "Standards for Internal Control in the Federal Government" (2014), accessed July 17, 2019, https://www.gao.gov/assets/670/665712.pdf. These standards help government entities establish internal control systems to ensure efficiency, the effectiveness of operations, and compliance with laws and regulations.

"Information technology general controls" are part of the overall internal controls that need to be in place for Public Works to meet its objectives. Information technology general controls create the foundation for the effective, secure operation of all city-run software applications. These controls should be in place for all critical city software applications.

The National Institute of Standards and Technology, a laboratory and nonregulatory federal agency within the U.S. Department of Commerce, has defined the information technology general controls that should be in place, as described in Table 3.[3]

TABLE 3. Description of Information Technology General Controls

Type	Description
Password	User passwords should require at least eight characters made up of a combination of upper- and lowercase letters, numbers, and special characters such as "#" or "$". The password should be changed every 90 days. New passwords should not be the same as the prior five passwords and should not include common words or phrases.
User Access	User access controls should require review and approval of all new users and should specify the type of access a user needs to the software application. These controls should define how often periodic user access reviews should be performed and how quickly user access should be removed when no longer needed.
Administrator User Access	System administrators have access to perform all the functions in software systems. Because of this complete access to the application functions, controls need to be in place to monitor administrative actions to ensure unauthorized transactions or actions are identified and reviewed by management.
Monitoring Service Providers	When the city is using a third-party service provider, controls need to be in place to ensure the services being provided are complying with contractual requirements.
Change Management	All changes to the actual software programming need to have controls to ensure only approved, tested, and agreed-upon changes are made to the software.
Backup and Retention	Because of the possibility of damage to the software application data, the city needs to ensure all city data is backed up regularly and retained in a manner that will allow the data to be fully recovered.

Source: National Institute of Standards and Technology.

Public Works is responsible for maintaining the appropriate level of information technology general controls to preserve the integrity of the city's data, and Technology Services must provide technical support to keep dTIMS and Cartegraph operational.

[3] National Institute of Standards and Technology, Special Publication 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations," (2013), accessed Aug. 23, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

FINDING 1

The Lack of Formal Citywide Policies for Information Technology Processes to Guide Agency Procedures Creates Cybersecurity and Operational Risks

In 2005, the mayor's Executive Order 18 established the authority and function for Technology Services as the city agency responsible for "oversee[ing] the technology service delivery functions of the city government."[4] However, the executive order is vague, outdated, and does not give Technology Services the explicit authority to create and enforce policies for information technology general controls across city agencies.

Lacking guidance on information technology general controls, Public Works did not have any formal policies or procedures in place to implement these critical controls for the two asset management systems we tested. We also found that Public Works is using spreadsheets for critical financial reporting without effective controls to safeguard the accuracy of the data.

The audit focused on two of Public Works' six asset management systems: dTIMS and Cartegraph. As discussed in the Background section, Public Works is responsible for the required information technology general controls to protect these software systems, detailed previously in Table 3. Because of the lack of direction from Technology Services requiring Public Works to identify and implement information technology general controls, Public Works did not implement these basic information technology general controls for these asset management systems and for the spreadsheets used to track financial data.

Technology Services Does Not Have the Explicit Authority to Create and Enforce Citywide Information Technology Policies

The need to develop and implement information technology general controls cannot be overemphasized. Information technology general controls form the foundation of an effective and efficient cybersecurity program and technology operations.

When Technology Services was created in 2005, the technology environment was radically different. For example, the term "cloud computing" was coined in 2006, and the Apple iPhone was first

[4] Exec. Order No. 18, City and County of Denver (2005), accessed Oct. 24, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/exectiveorders/18-Establishment-of-Techonology-Services.pdf.

Technology Services does not have the authority to establish citywide policies for information technology security processes.

introduced in 2007.[5] In that time, computers and networks have become more complex, and the city is much more dependent on information systems to provide all its services and to process large amounts of data. Mobile computing, smartphones, and access to high-speed Wi-Fi are now a common part of providing technology services, yet none of these existed when the executive order establishing Technology Services was issued.

Executive Order 18 emphasizes technology service delivery, stating "the chief information officer *may organize* the city's various technology operations *as necessary to deliver the most effective service*."[6] The only mention of security is that Technology Services is responsible for "ensuring that city information technology systems, data, and networks are secure and available."

Executive Order 18 does not define what "may organize" or "deliver … effective service" mean. Absent the definition of these key phrases, it is unclear if Technology Services has the authority to establish the citywide information technology policies needed to address today's technology environment. We concluded Technology Services has not created or implemented citywide policies because of this vagueness.

Without the guidance of Technology Services, all city agencies are responsible for creating their own policies and procedures to implement information technology general controls. However, they do not have the necessary technical knowledge to create these controls.

We tested two of the six Public Works asset management systems and found the majority of the expected information technology general controls were not in place.

Lacking these controls creates a higher cybersecurity risk, because a weakness in an asset management system may allow a hacker access to this system. Once a hacker has access to a system connected to the city's network, the hacker can access

WHAT IS A RANSOMWARE ATTACK?

Ransomware is a type of cybersecurity attack where a malicious hacker infects a subject computer with software that encrypts all of the computer's data. Until a ransom is paid, the computer's owner cannot access any data or use the computer.

[5] Antonio Regalado, "Who Coined 'Cloud Computing,'" MIT Technology Review, Oct. 31, 2011, accessed Nov. 15, 2019, https://www.technologyreview.com/s/425970/who-coined-cloud-computing/; "Timeline of Computer History," Computer History Museum, accessed Nov. 21, 2019, https://www.computerhistory.org/timeline/2007/.

[6] Exec. Order No. 18, City and County of Denver (2005), accessed Oct. 24, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/exectiveorders/18-Establishment-of-Techonology-Services.pdf, emphasis added.

the entire city network because they can bypass a number of security controls. This places the entire city at risk of a ransomware attack or loss of city data.

Allowing each city agency to create its own information technology general control policies creates a new set of cybersecurity risks.

The National Institute of Standards and Technology addresses this risk with its cybersecurity framework that identifies the need to establish consistent policies to ensure all systems and functions running in the same network have the same set of information technology general controls and cybersecurity controls.[7]

It is unlikely each city agency would create and adopt the same set of technology policies. Having differences in technology policies, such as the minimum requirements for passwords, creates gaps in the controls that can be exploited by malicious hackers.

Given that we tested only two of the six Public Works asset management systems, it is very likely a significant number of the 493 software applications that Technology Services supports also do not have the appropriate information technology general controls in place.

Establishing standardized policies is essential because it would help in ensuring appropriate, consistent controls are in place for maintaining efficient and secure operations. This is also a requirement of the National Institute of Standards and Technology, which stipulates that organizations should develop policies and procedures for their information systems.[8]

Giving Technology Services the clear authority to establish and enforce technology-related policies would mimic the process the Controller's Office uses to establish required financial controls for the city. The Controller's Office does this by issuing Fiscal Accountability Rules all agencies must follow. This process ensures all agencies are accounting for items the same way.

Providing the same type of direction for technology-related areas will also help create a more consistent and secure method of providing technology-related services across the city.

[7] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (2018), accessed Nov. 15, 2019, https://www.nist.gov/cyberframework/framework, 25-26.

[8] National Institute of Standards and Technology, Special Publication 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations" (2013), accessed Aug. 23, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

RECOMMENDATION 1.1

Update Necessary Laws – The Technology Services agency should have the necessary laws updated as soon as possible to enable the agency to establish and enforce standardized citywide information technology policies.

Agency Response: Agree, Implementation Date – April 15, 2020

RECOMMENDATION 1.2

Create Information Technology Policies – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should create citywide information technology policies and establish the means to ensure all city agencies are complying with these policies.

Agency Response: Agree, Implementation Date – July 15, 2020

The Lack of Documented Information Technology Controls Places the Department of Public Works' Infrastructure Asset Data at Risk

As noted, the city does not have formal documented information technology policies that are enforceable across all city agencies. As such, Public Works did not have any guidance on the need to create and implement policies and procedures for information technology general controls. Instead, the department relied on existing informal and undocumented processes.

We were unable to evaluate or test the design and effectiveness of the information technology general controls for the Cartegraph and dTIMS asset management systems because there were no formal controls in place. Specifically, we found:

Lack of User Access Controls – We identified a lack of a formal approval process for providing, reviewing, and removing user access. Even though there was an informal process of granting access via email, Public Works was unable to provide the email approval documentation.

According to the National Institute of Standards and Technology, controls should be established for adding new users, changing users' account access, and removing users when they no longer need access.[9]

[9] Ibid.

Lack of Administrator User Access Controls – We identified a lack of a formal approval process for providing and reviewing administrator user access. Users with administrator access can perform all functions in a software application, meaning they can bypass any controls built into the software. Because of the risks caused by administrator access, we tested all administrator user accounts and found every one of them lacked evidence of formal approval prior to being granted access.

Even though there was an informal process of granting access via email, Public Works was unable to provide the email approval upon request. There is a pressing need to establish a formal approval process, because accounts without proper authorization could lead to unauthorized access to the system.

According to the National Institute of Standards and Technology:

> "The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access."[10]

Lack of Unpaid Intern User Access Controls – Public Works regularly hires student interns during the summer to help with pavement and alley data collection projects using dTIMS. Depending on the task assigned to these interns, Public Works requests Workday and email accounts for them, but the department was unaware it needed to develop procedures to remove the interns' access to dTIMS and Workday once their internships ended. As a result, we found one student intern still had active Workday and email accounts 90 days after leaving the city.

The National Institute of Standards and Technology requires organizations to notify account managers "when accounts are no longer required, when users are terminated or transferred,

WHAT IS WORKDAY?

Workday is the city's accounting and personnel software system. For the city to establish an email account for any city employee or intern, that employee or intern needs to have a Workday account. Creating an email account also adds the user to the Technology Services user management process.

[10] Ibid.

and when individual information system usage or need-to-know changes."[11]

As an example of the risk created by having user accounts active when no longer needed, Michelle Cawthra embezzled $11 million from the Colorado Department of Revenue by using other users' accounts and inactive accounts to bypass the controls around processing Colorado taxpayers' tax returns.[12]

Lack of System Administrator Succession Planning – Public Works does not have a formal succession plan for dTIMS' and Cartegraph's administrator roles. We found there was no formalized documentation and cross-training.

As a result, when the Cartegraph system administrator left the city at the start of our audit in July 2019, there was no one with the knowledge to keep Cartegraph running effectively. The current Cartegraph interim administrators are undergoing a massive effort, first, to learn how to administer the system and, second, to eventually return the system's full functionality. For dTIMs, Public Works relies on the vendor to provide these critical administrator roles.

The Cartegraph system administrator left the city in July 2019, which was at the start of our audit.

Guidance from the U.S. Government Accountability Office stipulates that one of the elements of good internal controls is that "management defines succession plans for key roles, chooses succession candidates, and trains succession candidates to assume the key roles."[13] The city's Fiscal Accountability Rules also require that Public Works should have a complete system of internal controls, which would include items like succession plans.[14]

Lack of User Access Reviews – During our audit, we found Public Works does not have a process to periodically review user access. Such reviews are necessary to ensure user access is appropriate. For dTIMS, we were informed that because of the limited number of users, Public Works was aware of staffing changes that would require access updates. However, the department did not have any formal process to review user access.

The department's interim administrators for Cartegraph confirmed they had performed only one user access review since assuming

[11] Ibid.

[12] "Randell Convicted in $11M Theft from Colorado Revenue Department," Denver Business Journal, July 20, 2009, accessed Oct. 16, 2019, https://www.bizjournals.com/denver/stories/2009/07/20/daily20.html; Dan Boriface, "Former Employee 'Not Surprised' by Alleged Tax Scheme," 9News, May 2, 2007, accessed Nov. 18, 2019, https://www.9news.com/article/news/local/former-employee-not-surprised-by-alleged-tax-scheme/73-343782328.

[13] U.S. Government Accountability Office, GAO-14-704G, "Standards for Internal Control in the Federal Government" (2014), accessed Oct. 21, 2019, https://www.gao.gov/assets/670/665712.pdf.

[14] City and County of Denver, Rule 1.1 – Accounting Principles and Standards, Fiscal Accountability Rules (revised 2008).

responsibility for the application. This review, which occurred in July 2019, was not a regular process and resulted in the discovery of users who needed to be removed and of some users who did not have the access needed to perform their jobs.

The National Institute of Standards and Technology requires that organizations develop, document, and disseminate access control policies and procedures that include reviewing and updating accounts that "are no longer required, when users are terminated or transferred, [and] when individual information system usage or need-to-know changes occur.[15]

Public Works officials acknowledged the need for a formal process for user access review. They also agreed that the lack of a periodic review of user access could lead to unauthorized individuals gaining access to critical data.

Without Controls, Public Works' Asset Management Systems Are Vulnerable to Cybersecurity Attacks

Without effective controls over the city's software systems, there is a risk that city data may be lost or compromised, such as through a cybersecurity attack. As an example, there have been many governments, including the City of Baltimore, that have suffered cybersecurity attacks resulting in their data being encrypted and thus not available. Baltimore spent over $18 million in recovering from such an attack.[16]

The ability for hackers to be able to access and encrypt data on city systems can also be limited by implementing strong controls over user access.

To ensure the asset management systems are secure, available, and proving accurate data, Public Works — with the assistance of Technology Services — should create procedures to ensure required information technology general controls are developed and implemented.

[15] National Institute of Standards and Technology, Special Publication 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations" (2013), accessed Aug. 23, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[16] Ian Duncan, "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," Baltimore Sun, May 29, 2019, accessed Oct. 25, 2019, https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

RECOMMENDATION 1.3

Develop User Access Process – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible to grant, change, and remove user system access.

Agency Response: Agree, Implementation Date – June 30, 2020

RECOMMENDATION 1.4

Develop Administrator User Review Process – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible for approving administrator user accounts.

Agency Response: Agree, Implementation Date – June 30, 2020

RECOMMENDATION 1.5

Develop an Access Removal Process – The Department of Public Works should develop a process to notify Workday administrators to remove user access for all users, including unpaid interns, when their employment or internship is completed.

Agency Response: Agree, Implementation Date – June 30, 2020

RECOMMENDATION 1.6

Develop User Access Review – The Department of Public Works, working with the Technology Services agency, should develop a process as soon as possible to establish periodic user access review listings to ensure user access remains appropriate for all applications and that appropriate segregation of duties is maintained.

Agency Response: Agree, Implementation Date – June 30, 2020

RECOMMENDATION 1.7

Develop Succession Plan – The Department of Public Works, with guidance from the Technology Services agency, should ensure there is a succession plan as soon as possible for all system administrator roles.

Agency Response: Agree, Implementation Date – March 31, 2020

The Lack of a Formal Citywide Policy for Spreadsheet Controls Results in Errors in Public Works' Fixed Asset Accounting and Reporting Data

The Department of Public Works uses spreadsheets to track financial information for infrastructure assets. This is because Public Works did not implement Cartegraph to meet any requirements for financial reporting. dTIMS provides the detail for the current year's additions to streets and alleys. Although dTIMS has the ability to report on the original cost of the streets and alleys as required by financial accounting standards, Public Works does not use this capability. The Controller's Office said Workday, the city's accounting system, is not being used to record the infrastructure assets and there are no plans to do so.

Because these two asset management systems and Workday are not fully used for tracking financial details, Public Works defaulted to using spreadsheets for infrastructure asset financial reporting. Lacking any guidance on required controls for spreadsheets, these critical spreadsheets did not have controls in place to ensure the accuracy and availability of the data they are tracking.

Four spreadsheets are used by Public Works to record and report on the city's streets, alleys, and signalized intersections. We tested these and determined only one spreadsheet had error-checking built-in. However, this error check did not detect an existing error in one row of data — demonstrating one of the weaknesses with using this method to track data. We also identified a data error related to the number of traffic signals that were removed in 2018, which resulted in a $345,000 error in the amount reported in the 2018 Comprehensive Annual Financial Report.

According to global accounting firm PwC:

> "A proliferation of [the use of] spreadsheets can inevitably increase the risk of mistakes and make errors harder to detect. Some of the main risks associated with spreadsheets actually stem from their flexibility and ease

of use. This includes making it hard to pick up changes to functionality or data."[17]

The firm goes on to say that "reducing dependence on spreadsheets should therefore be a key priority" and "similarly, the user guidance for spreadsheets tends to be less well documented than for an [information technology] system."

Data Accuracy and Reliability Is Diminished without Proper Controls over Spreadsheet Data

The risks of using spreadsheets as a primary tracking and control device include errors in calculations or data entry and the possibility of using an out-of-date version of the file. There is also the potential for inexperienced users to use spreadsheets incorrectly or that an unauthorized employee will have inappropriate access to files through shared networks. The use of spreadsheets also increases an organization's dependence on key personnel who could leave at any time.

According to the National Institute of Standards and Technology, the recommended controls for spreadsheets would include access controls, configuration management, backup contingency planning, and authentication.[18]

Public Works is required to establish a system of internal controls in compliance with the city's Fiscal Accountability Rules.[19] Because Public Works uses spreadsheets as the main accounting system to record and report on the city's infrastructure assets, these spreadsheets must have the same types of controls that should be in place in any accounting software system.

[17] PwC, "Managing Spreadsheet Risks" (2011), accessed Oct. 25, 2019, https://www.pwc.com/gx/en/insurance/solvency-ii/pdf/pwc-countdown-june-11-managing-spreadsheet-risks.pdf.

[18] National Institute of Standards and Technology, Special Publication 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations" (2013), accessed Aug. 23, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[19] City and County of Denver, Rule 1.1 – Accounting Principles and Standards, Fiscal Accountability Rules (revised 2008).

RECOMMENDATION 1.8

Create Spreadsheet Best Practice – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should establish standard citywide best practices for key spreadsheet controls that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed
5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agency Response: Agree, Implementation Date – April 15, 2020

RECOMMENDATION 1.9

Implement Spreadsheet Controls – Working with the Technology Services agency, the Department of Public Works should, as soon as possible, move to a solution with appropriate information technology controls or implement spreadsheet control procedures that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed
5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agency Response: Agree, Implementation Date – 180 days after completion of Recommendation 1.8

FINDING 2

Poor Vendor Oversight Puts Asset Management Data at Risk

Vendor management for cloud service providers is a critical part of the city's overall cybersecurity control environment. Cloud service providers store city data in their systems, and without appropriate security controls, the city's data is at risk.

We found that the city's Technology Services agency and the Department of Public Works are not providing oversight of cloud-based vendors' information technology controls. In addition, Public Works did not confirm two of its vendors were properly insured. Proper insurance coverage reduces liability to the city in the event of a cybersecurity attack.

Effective Technology Vendor Management Is Important to Help Ensure Data Security

One part of ensuring an effective technology vendor management process is to obtain and review vendors' System and Organization Controls for Service Organizations, or SOC, report. These reports provide a description of how effective the critical internal controls are for vendors providing the city with accounting or operational services. Such a report provides the city with the information to make sure the service provider is not putting the city's data at risk.

Because of the nature of the contractual relationship between a vendor and the city, there is a shared responsibility to ensure the city's data is properly handled, processed, and protected. Because of this shared responsibility, the vendor's System and Organization Controls for Service Organizations report also provides a list of controls that the city needs to implement to make sure city data is accurate and secure. For example, the city would be responsible for ensuring only authorized people have access to the asset management systems, and the vendor would be responsible for backing up the asset management data.

Another important control is for the city to confirm whether the vendor has implemented the "Cloud Security Alliance" controls."[20] However, this is not being done on a regular basis. The Cloud Security Alliance provides fundamental security principles to cloud vendors to help ensure a secure cloud environment.

[20] "About," Cloud Security Alliance, accessed Oct. 25, 2019, https://cloudsecurityalliance.org/about/.

THE CLOUD SECURITY ALLIANCE

The Cloud Security Alliance is a not-for-profit group composed of leading technology and security organizations that was founded to provide security control best practices for cloud-based services. The organization developed "The Cloud Security Controls Matrix," which maps cloud-specific security controls to leading standards, regulations, and industry best practices.

A Lack of Vendor Management Can Be Expensive

According to required controls from the National Institute of Standards and Technology, the City and County of Denver should actively monitor third-party compliance with enterprisewide information security policies, standards, and information security requirements.[21]

When software vendors and third-party cloud service providers lack adequate controls, unauthorized access, data loss, or weak configuration settings could adversely affect the security, integrity, and availability of city data. According to the Wall Street Journal: "Poor security practices, complicated controls, and rushed technology programs are causing a rash of data breaches stemming from the use of cloud services, experts say. Both users and cloud providers could be doing more to prevent them."[22]

There have been numerous security breaches in recent times. For example, when Capital One suffered a security breach that exposed 100 million customers' personal data, it cost an estimated $100 million.[23] Equifax also experienced a data security breach of customer data, and that cost over $600 million.[24] These breaches may have been prevented if these companies had established security monitoring processes to evaluate the cloud service providers, such as by requesting and reviewing System and Organization Controls for Service Organizations reports to determine the design and effectiveness of the service provider's information technology environment.

According to the National Institute of Standards and Technology: "Organizations placing sensitive and regulated data into a public

[21] National Institute of Standards and Technology, Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing" (2011), accessed Oct. 23, 2019, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[22] James Rundle, "Human Error Often the Culprit in Cloud Data Breaches," The Wall Street Journal, Aug. 27, 2019, accessed Oct. 16, 2019, https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203.

[23] Fred Imbert, "Capital One Shares Dive after Data Breach Affecting 100 Million," CNBC, July 30, 2019, accessed Oct. 25, 2019, https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html.

[24] Stacy Cowly, "Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement," The New York Times, July 29, 2019, accessed Oct 21. 2019, https://www.nytimes.com/2019/07/22/business/equifax-settlement.html.

cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure."[25]

In addition, the city's Executive Order No. 18 makes Technology Services responsible for "reviewing and approving all technology purchases made by city" and "ensuring that city information technology systems, data, and networks are secure and available to the city's internal and external customers."[26]

There Is No Effective Review of Cloud-Based Vendors' Information Technology General Controls

During our review of dTIMS and Cartegraph, we found that neither Technology Services nor Public Works requests and reviews the System and Organization Controls for Service Organizations reports or other assurance documentation from either vendor.

The only review of the cloud-based vendors' compliance with Cloud Security Alliance controls was performed by Technology Services before the services were first purchased in 2014 for Cartegraph and in 2017 for dTIMS. Our testing of these reviews identified gaps, unanswered questions, and a lack of support for Technology Services' conclusion that these vendors were compliant with the Cloud Security Alliance security controls.

Prior to our audit, Technology Services identified the need to strengthen its vendor management program and purchased a new module in ServiceNow — the city's software for technology support services — that allows Technology Services to request documentation, document the review, and support the recurring review of vendor reports. However, because of the amount of work required, this module is not fully implemented.

WHAT IS SERVICENOW?

ServiceNow is a software application designed to assist technology support services. ServiceNow tracks vendor compliance with System and Organization Controls for Service Organizations reports and submission of Cloud Security Alliance security controls. ServiceNow also provides other support services.

An effective review process of information technology general controls is similar to the controls required by the city controller. According to the city's Fiscal

[25] National Institute of Standards and Technology, Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing" (2011), accessed Oct. 23, 2019, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[26] Exec. Order No. 18, City and County of Denver (2005), accessed Oct. 24, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/exectiveorders/18-Establishment-of-Techonology-Services.pdf.

Accountability Rules, "all independent agencies shall annually certify to the Controller, as to the adequacy of its systems of internal accounting and administrative controls."[27]

In addition, according to an article published by the American Institute of Certified Public Accountants, the city may obtain and review the System and Organization Controls for Service Organizations report as part of the city's assessment of the cloud-based service provider's internal controls.[28]

Vendor Software Changes Not Reviewed – Neither Technology Services nor Public Works reviews the cloud-based vendors' process to make changes to software programming, which may lead to unauthorized changes to dTIMS and Cartegraph. This could create system outages, potential security issues, and undocumented system modifications resulting in incorrect data.

The creation of a formal review process for any changes made to the programming of the application software would ensure changes to dTIMS and Cartegraph are properly documented and approved by appropriate individuals. For these two applications, however, we found that Public Works does not have a formal process to track and approve the changes made by the applications' respective vendors.

The vendors have the responsibility of performing all changes to dTIMS and Cartegraph because the applications are cloud-based. Public Works relies on the vendors' expertise to create and test all changes to the software. Public Works performs some testing of the software changes to dTIMS; however, there is no formal documented process to track and validate the testing performed.

Poor Oversight of System Backup and Recovery – We also reviewed the backup and recovery processes for dTIMS and Cartegraph. Both systems are cloud-based and, therefore, the vendor should be responsible for the backup and recovery of the data.

Public Works officials believe the applications' vendors are meeting the city's backup standards, but the department has not confirmed the frequency and types of backups and recovery being performed by the vendors.

Failure to confirm the frequency and type of backup performed could result in a loss of city data when there are system outages or security issues.

[27] City and County of Denver, Rule 1.1 – Accounting Principles and Standards, Fiscal Accountability Rules (revised 2008).

[28] Audrey Katcher, "Understanding How Users Would Make Use of a SOC2 Report," accessed Oct. 23, 2019, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc2-user-document.doc.

RECOMMENDATION 2.1

Implement Vendor Management System – The Technology Services agency should continue to implement the ServiceNow Vendor Management module to fully document the review process and schedule recurring reviews for System and Organization Controls for Service Organizations, or SOC, reports. The agency should follow up with the vendor on control gaps identified in the report.

Agency Response: Agree, Implementation Date – Dec. 31, 2020

RECOMMENDATION 2.2

Implement Periodic Cloud-Based Vendor Security Reviews – The Technology Services agency should implement a process to review cloud-based vendors' ongoing adherence to the Cloud Security Alliance security controls. If gaps in the vendors' security controls are identified, Technology Services should implement sufficient additional controls to mitigate the lack of security or decommission the noncompliant vendor service until the security issues can be adequately addressed.

Agency Response: Agree, Implementation Date – Dec. 31, 2020

RECOMMENDATION 2.3

Obtain System and Organization Controls for Service Organizations Reports – The Department of Public Works should obtain its vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review to determine whether backups are scheduled and tested on a periodic basis. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

RECOMMENDATION 2.4

Review Vendor Disaster Recovery Controls – The Department of Public Works should obtain the vendor System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the disaster recovery information contained in these reports to ensure the vendors' disaster recovery processes meet Public Works' needs. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

RECOMMENDATION 2.5

Review Vendor Change Management Controls – The Department of Public Works should obtain the vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the change management information contained in these reports to ensure the vendors' change management controls meets Public Works' needs. The department should follow up with the vendors on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

RECOMMENDATION 2.6

Implement Complementary User Controls – The Department of Public Works should ensure it evaluates the complementary user controls as identified in each vendor's System and Organization Controls for Service Organizations, or SOC, report and implements those controls that are feasible.

Agency Response: Agree, Implementation Date – 180 days after receipt of SOC reports

Public Works Did Not Obtain and Review Vendors' Insurance Coverage for dTIMS and Cartegraph

The Department of Public Works is required to ensure all vendors — including those for dTIMS and Cartegraph — maintain agreed-upon insurance coverage. However, Public Works has no clear process to obtain proof on a periodic basis that the vendor is maintaining its compliance with the city's required insurance coverage.

If the city experiences a cyberattack, the costs to remediate the

Without adequate insurance coverage, the vendor might not have the resources to cover the liability incurred.

incident can be expensive. For example, in early 2018, a hacker successfully executed a ransomware attack on the Colorado Department of Transportation. When the ransomware was deployed, it impaired the ability of the Colorado Department of Transportation to provide services.[29] Although the Colorado Department of Transportation did not pay the ransom, the efforts to restore its systems and data files were estimated to cost $1.5 million.[30]

Cybersecurity insurance can provide the necessary coverage to a government entity without having to pass the cost of a security breach on to residents. For this reason, the city should ensure cloud service vendors carry an appropriate amount of cybersecurity insurance.

Current insurance certificates are required to verify whether vendors maintain insurance in the types and amounts specified by the contract. The insurance provisions in city contracts provide coverage to the city should an event occur that would be covered under insurance. Without adequate insurance coverage, the vendor might not have the resources to cover the liability incurred. This could result in negotiations or legal actions to meet any obligations.

Guidance from the U.S. Government Accountability Office states "management should identify, analyze, and respond to risks related to achieving the defined objectives."[31] Risk identification includes looking at external parties to determine risk factors. After identifying the external risks, management should assess the risk and determine the likelihood and impact of the risk. After this has been identified, management should formalize a response, which could include accepting the risk, reducing the risk, or sharing the risk. Management can share the risk with external parties by requiring them to carry insurance.

Also, the city's Executive Order No. 8 specifies that the agency management that requests the contract (called the "initiating authority" — in this case, Public Works) has specific responsibilities for the life of the contract.[32] These responsibilities include ensuring compliance with contract terms, including maintaining insurance for the correct amount and types throughout the life of the contract.

Public Works should determine which of its divisions will be responsible for reviewing insurance renewals by vendors and track compliance.

---

[29] State of Colorado Business Emergency Operations Center, "CDOT After Action Report for the 2018 Cyber Incident," accessed Oct. 21, 2019, https://www.colorado.gov/pacific/cobeoc/news/after-action-report-released-cdot-cyber-incident.

[30] "What Colorado Learned from Treating a Cyberattack like a Disaster," Statescoop, accessed Oct. 21, 2019, https://statescoop.com/what-colorado-learned-from-treating-a-cyberattack-like-a-disaster/.

[31] U.S. Government Accountability Office, GAO-14-704G, "Standards for Internal Control in the Federal Government" (2014) para. 7.01, accessed Oct. 21, 2019, https://www.gao.gov/assets/670/665712.pdf.

[32] Exec. Order No. 8, City and County of Denver (2011), accessed Oct. 21, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/executiveorders/8-Contracts-Other-Written-Instruments-CCD.pdf.

RECOMMENDATION 2.7

Review Insurance Coverage – The Department of Public Works should develop a process to receive, track, and review all insurance coverage certificates from technology vendors to ensure they are maintaining compliance with the city's insurance requirements.

Agency Response: Agree, Implementation Date – June 30, 2020

FINDING 3

The City's Contracting Process Failed to Include Technology Services' Required Review and Approval of a Technology Purchase

The Cartegraph application contract was executed without the required review and approval of the city's Technology Services agency, which resulted in the purchase of 488,000 "citizen-use" licenses that were not, in fact, intended to be used by citizens. In addition, the contract language was unclear as to who is responsible for backing up the city's data.

Contracts represent one of the "highest administrative priorities within the city" and a legal obligation for the city.[33] Because of the importance of contracting, the city established Executive Order No. 8, which provides detailed guidelines for the contract process and for monitoring contract compliance. Executive Order No. 18 establishes the requirement that Technology Services review all technology purchases.

The city developed an automated workflow review and approval system to ensure all relevant agencies and staff review a contract before the final approval. Auditors reviewed the contract workflow for the Cartegraph contract and observed that the "technology review required" flag was set to "NO." With the flag set to "NO," the contract was not routed to a Technology Services staff member for their review.

Technology Services Did Not Review the Cartegraph Contract, which Resulted in Purchasing Unneeded Licenses

The purchase agreement for the Cartegraph contract contains a provision for 488,000 licenses for citizen use, costing $170,800. Because of staff turnover, current Public Works management could not explain the purpose of these licenses.

After discussions with the Cartegraph vendor account manager, auditors learned the citizen licenses were never intended to be used by citizens but, instead, were a means to charge municipalities according to the size of the population. The Cartegraph contract also includes 100 named-user licenses. The Technology Services asset management team, which is responsible for tracking software license compliance for the city, did not have a record of any of the Cartegraph licenses.

[33] Exec. Order No. 8, City and County of Denver (2011), accessed Oct. 21, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/executiveorders/8-Contracts-Other-Written-Instruments-CCD.pdf.

Maintaining accurate counts for licenses is key to contract compliance. Without an accurate software license inventory, the city is at risk of incurring fines and penalties from its software vendors due to underlicensing or other noncompliance.

Current contracting practices did not assure that Technology Services reviewed and approved the technology purchase for Cartegraph, as required by Executive Order 18.[34] Technology Services management relies on the contract review process to ensure they are aware of software licenses and to remain compliant with vendor agreements.

Cybersecurity risks occur when Technology Services' required review is not conducted, because new cloud-based services with weak security controls could be added to the city's network. Because these services are now in the city's network, they would bypass a number of security controls and processes in place to prevent unauthorized access to the city's systems and data. Additionally, without the agency's review, services may be purchased that are already in place. This results in a duplication of services and a waste of taxpayer funds.

The Cartegraph Contract Did Not Clearly Specify Who Is Responsible for Backup of City Data in Line with Best Practices

One section of the Cartegraph contract requires the city to back up and recover data, while another section of the contract states that the vendor is responsible for backup and recovery of data.

Because Technology Services did not review this contract, these contradictory requirements were not identified and addressed.

Without a clear understanding of who is responsible for the backup and recovery of data, there is a risk that the city's data may be lost.

RECOMMENDATION 3.1

Improve Contracting Process – The Technology Services agency should work with all parties involved in the contracting process to improve the contract routing and approval process to ensure Technology Services is included in all technology purchases.

Agency Response: Agree, Implementation Date – July 15, 2020

[34] Exec. Order No. 18, City and County of Denver (2005), accessed Oct. 21, 2019, https://www.denvergov.org/content/dam/denvergov/Portals/executiveorders/18-Establishment-of-Techonology-Services.pdf.

RECOMMENDATION 3.2

Clarify Contract Language – The Department of Public Works should clarify the Cartegraph contract language regarding the responsibility for performing backups and for how frequently those backups should occur.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

FINDING 4

Technology Services Should Expand its Existing Business Relationship Management Program to Include the Public Works Department to Provide Better Customer Service

The Technology Services agency established a business relationship management program in 2017. The program provides dedicated technology resources to an agency to better assist with its technology needs. Technology Services management reported that the business relationship team is not currently assigned to the Public Works Department because the team is working with another agency with a higher priority.

Technology Services is responsible for a vital support function for Public Works. To provide these support services, the agency needs to establish effective and efficient business relationships with Public Works. However, we noted Technology Services has not established a customer service model for Public Works to ensure it fulfills the department's technical needs.

This resulted in problems with password settings for dTIMS, and dTIMS staff were unclear on how to make updates to the city's geographic information system.

Technology Services Failed to Respond to Requests from Public Works to Ensure Appropriate Security Processes Were Established

dTIMS is built to integrate with the city's network. Public Works repeatedly asked Technology Services to add the dTIMS software system to the city's network, which would have provided strong password settings. The department's attempts to work with Technology Services were unsuccessful.

We reviewed seven emails that started in May 2018 and ended in July 2018 directly related to the attempts by Public Works to work with Technology Services to add dTIMS to the network. Technology Services did not respond until Public Works management escalated the issue. As of October 2019, dTIMS had not been added to the network.

As a result, the dTIMS system is at a heightened cybersecurity risk because dTIMS does not have the capability to support strong password requirements. Technology Services' password policy aligns with the National Institute of Standards and Technology's controls,

which state that organizations should enforce information system password-based authentication.[35]

There is a proposed technical workaround initiated by dTIMS' vendor that would allow dTIMS to have strong password settings. However, at the time of this audit, this process had not been reviewed by Technology Services to make sure it does not create some other cybersecurity risks. Therefore, the agency has yet to implement the solutions.

RECOMMENDATION 4.1

Improve Customer Service – The Technology Services agency should improve its customer service for the Department of Public Works' technology issues.

Agency Response: Agree, Implementation Date – Immediately

RECOMMENDATION 4.2

Establish Service-Level Agreements – The Technology Services agency should establish and communicate a standard process with expected response times and escalation path for handling customer requests and disagreements.

Agency Response: Agree, Implementation Date – March 31, 2020

RECOMMENDATION 4.3

Improve dTIMS Password Settings – The Technology Services agency should work with the Department of Public Works to ensure dTIMS meets password security requirements as soon as possible by integrating dTIMS into the city's active directory or ensuring that a vendor-provided solution meets Technology Services' requirements.

Agency Response: Agree, Implementation Date – March 15, 2020

[35] National Institute of Standards and Technology, Special Publication 800-53 (Revision 4), "Security and Privacy Controls for Federal Information Systems and Organizations" (2013), accessed Aug. 23, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Technology Services Has Not Communicated the Process for Updating Citywide Geographic Information System Data

The Department of Public Works routinely reidentifies alleys that no longer exist and that need to be removed from the city's geographic information system.

Public Works noted that the missing alleys are the result of the city converting an existing alley into a single block of land for some city purpose. For example, the Lindsey Flanigan Courthouse located off Colfax Avenue and Fox Street used an existing city block that had had an alley, but because of the size of the building, the entire block was used in construction, including the alley. Because the alley was used for a city purpose, a public approval process was not needed to remove the alley from the city's geographic information system. Without the public approval process, the geographic information system team was unaware of the need to remove the alley.

The dTIMS software application has a tool to track the condition of the city's alleys. The process to review the city's alleys starts with the city's geographic Information system data being loaded into dTIMS. Because of the number of "missing" alleys, dTIMS starts all alley inspections with the question "Does the alley exist?"

According to the International Organization for Standardization, "data error correction shall consist of … the activity that notifies all the responsible parties of the data before and after the correction in order to eliminate any confusion in the data operation."[36]

Notably, Technology Services created a process for city personnel to report changes to the geographic information system database. However, this process was not clearly communicated to Public Works personnel.

Because Public Works was unaware of this process, the missing alleys that department staff identified were not reported or updated in the city's geographic information system. As a result, the city's geographic information system database is not accurate, and the city wastes taxpayer dollars in staff having to reidentify missing alleys.

[36] International Organization for Standardization, "ISO/TS 8000-150 Data Quality – Part 150: Master Data: Quality Management Framework" (2015), accessed Oct. 23, 2019, http://vai.org.vn/docs/iso/8000-150.pdf.

RECOMMENDATION 4.4

Communicate Update Process – The Technology Services agency should, as soon as possible, communicate its process to the Department of Public Works for updating the city's geographic information system database.

Agency Response: Agree, Implementation Date – Jan. 31, 2020

FINDING 5

The Public Works Department Does Not Have a Formal Strategy for Asset Management

Current management in the Department of Public Works had been in place for less than one year when they realized they inherited an ineffective asset management process that consists of six different tracking systems and is driven by individual department needs rather than a comprehensive, integrated solution.

Therefore, in December 2018, the department identified the need to reassess its overall strategy for identifying, tracking, and reporting on its fixed assets. Although Public Works started work on a departmentwide plan for asset management, the current plan was not developed with Technology Services' assistance, it is informal, and it lacks the necessary rigor to provide an effective strategy for combining multiple asset management systems.

Public Works started to address this problem with a "Concept of Operations" whitepaper that identified an informal strategy for asset management across Public Works' divisions. The whitepaper outlined a team structure and the benefits of a coordinated asset management system, such as:

- "Data-driven decision making for annual maintenance programs"
- "Use of economies of scale and optimization of funding"
- "Coordinated multi-year work programs amongst different agencies and asset classes"
- "Ability to optimize cross-asset management principles"
- "Scalable for multiple assets and degree of detail for each asset"
- "Supports One Build concept"[37]

Consolidating asset management systems also supports Public Works' "One Build" initiative. The initiative means maintaining neighborhoods in a systematic way by sequencing construction and maintenance work to minimize conflicts and by completing all planned activities in a reasonable amount of time to minimize impact to residents.

[37] City and County of Denver Public Works Department, "Public Works Asset Management Concept of Operations."

Public Works Identified the Need to Expand its Asset Management Plan

Senior leadership identified the need to expand its current asset management efforts to include:

- Fully assessing each system's functionality in relation to each other;
- Determining how assets identified can be included in Workday; and
- Developing a data management plan to classify and standardize the critical data across all asset management systems.

Public Works has spent almost a year investigating how best to consolidate the existing six asset management systems. However, there will be a need for multiple systems because of the operational needs for the infrastructure asset management systems. As an example, dTIMS provides extensive functionality to assess the status of the city's streets and alleys, which is not available in a standard asset management application. But dTIMS does not provide the functionality of the fleet operations provided by the FASTER asset management system.

Public Works' current stopgap approach is to build a combined database from all the asset management systems to allow a single reporting source. This will require that each of the asset management systems produce a set of standard data that can be combined into a new database.

Public Works has begun discussing with the city's chief data officer, who provides guidance on data management and system implementations, how to create and manage the asset management database. However, nothing formal has been developed.

THE CHIEF DATA OFFICER'S ROLE

The chief data officer is part of the city's Technology Services agency and is responsible for providing guidance on data management and system implementations. This includes the selection and review of data-reporting technology, such as the asset management database.

Public Works Lacks a Comprehensive Asset Management Plan

Without a comprehensive plan for asset management systems, we found problems with Public Works' processes for tracking and reporting

on fixed assets. Specifically, we found:

- Spreadsheets are used as the record for fixed-asset reporting and tracking resulting in data errors.
- Asset tracking systems are developed without formal controls for the operation and maintenance of those systems.
- Contracts contained contradictory provisions and unused licenses.
- Comprehensive policies and procedures are lacking.
- Succession planning for system administrators does not occur, resulting in a single point of failure.
- There are no data standards across asset management systems.

Public Works did not engage with Technology Services for project management assistance. Technology Services provides specific project management support for the implementation of new systems and services to help ensure the success of these projects by following best practices such as those identified by the Project Management Institute.[38] The Project Management Institute published a collection of processes, best practices, terminologies, and guidelines that are accepted as a framework within the project management industry.[39]

Key elements that are included in the project management process are a project charter that defines the objectives and establishes the key stakeholders and their needs and the project plan that maps the specific objectives and deliverables to project resources that complete the objectives. A project plan should include well-defined business cases that will provide guidance during the project and a way to measure the success of the efforts.

Adding these key elements will help the department achieve the goals outlined in its "Concept of Operations" whitepaper.

[38] "A Guide to the Project Management Body of Knowledge," Third Edition (Project Management Institute, 2004), 79-80 and 105-106.

[39] Ibid.

RECOMMENDATION 5.1

Formalize Asset Management Strategy – The Department of Public Works should continue its efforts to develop an asset management strategy by formalizing its asset management approach and:

- Developing a comprehensive charter;
- Creating specific deliverables and objectives;
- Identifying a business case and requirements; and
- Conducting an analysis of stakeholder needs.

Agency Response: Agree, Implementation Date – Sept. 30, 2020

RECOMMENDATION 5.2

Consult with the Chief Data Officer – The Department of Public Works should continue its efforts to develop an asset management strategy by consulting with the chief data officer to leverage their experience in developing data standards to ensure consistency between the various asset management platforms.

Agency Response: Agree, Implementation Date – Ongoing

RECOMMENDATION 5.3

Engage Technology Services – The Department of Public Works should continue its efforts to develop an asset management strategy by engaging the Technology Services agency as soon as possible to assist with the asset management initiative to ensure information technology and project management best practices are followed.

Agency Response: Agree, Implementation Date – Sept. 30, 2020

RECOMMENDATIONS

1.1 **Update Necessary Laws** – The Technology Services agency should have the necessary laws updated as soon as possible to enable the agency to establish and enforce standardized citywide information technology policies.

Agency Response: Agree, Implementation Date – April 15, 2020

Agency Narrative: The mission and functions of Technology Services have evolved over the years, moving beyond the scope of the current Executive Order (XO) No. 18. We will evaluate the options of revising XO No. 18 or consider an alternative form of authority (ex: charter) to provide the requisite power to fulfill our mission and deliver effective services.

1.2 **Create Information Technology Policies** – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should create citywide information technology policies and establish the means to ensure all city agencies are complying with these policies.

Agency Response: Agree, Implementation Date – July 15, 2020

Agency Narrative: When the requisite authority is established, Technology Services will create related citywide policies and control processes to ensure compliance.

1.3 **Develop User Access Process** – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible to grant, change, and remove user system access.

Agency Response: Agree, Implementation Date – June 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will work with Technology Services to create a user access procedure to cover asset management software system access and user privilege modifications. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

1.4 **Develop Administrator User Review Process** – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible for approving administrator user accounts.

Agency Response: Agree, Implementation Date – June 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will work with Technology Services to create an asset management software administrator process and procedure to cover administrator roles and responsibilities. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

1.5 **Develop an Access Removal Process** – The Department of Public Works should develop a process to notify Workday administrators to remove user access for all users, including unpaid interns, when their employment or internship is completed.

Agency Response: Agree, Implementation Date – June 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will work with Workday administrators to create a process for timely and appropriate access removal for all staff (including unpaid interns) with asset management system access. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

1.6 **Develop User Access Review** – The Department of Public Works, working with the Technology Services agency, should develop a process as soon as possible to establish periodic user access review listings to ensure user access remains appropriate for all applications and that appropriate segregation of duties is maintained.

Agency Response: Agree, Implementation Date – June 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will work with Technology Services to create a quarterly asset management software access review to ensure system access is verified. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

1.7 **Develop Succession Plan** – The Department of Public Works, with guidance from the Technology Services agency, should ensure there is a succession plan as soon as possible for all system administrator roles.

Agency Response: Agree, Implementation Date – March 31, 2020

Agency Narrative: The Department of Transportation and Infrastructure will include, in the Office of Asset Management Business Plan, succession planning for all asset management software system administrator roles to include identifying secondary personnel and the provision of cross training.

1.8 **Create Spreadsheet Best Practice** – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should establish standard citywide best practices for key spreadsheet controls that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed

5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agency Response: Agree, Implementation Date – April 15, 2020

Agency Narrative: Microsoft Office 365 is the city's supported productivity suite, which includes Excel as its spreadsheet solution. Office 365 contains extensive native functionality that enables and supports best practices on data management and usage, such as change controls, version controls, access controls and backups. Simply by utilizing Excel as part of our Office 365 suite, Technology Services has already implemented four of the six recommendations (1,2,3, and 6). Recognizing that areas 4 and 5 are intended to establish citywide best practices for key spreadsheets, rather than enforce compliance, Technology Services will develop and communicate these best practices to appropriate agencies and departments.

1.9 **Implement Spreadsheet Controls** – Working with the Technology Services agency, the Department of Public Works should, as soon as possible, move to a solution with appropriate information technology controls or implement spreadsheet control procedures that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed
5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agency Response: Agree, Implementation Date – 180 days after completion of Recommendation 1.8

Agency Narrative: Upon completion of a citywide Policy(s) for key spreadsheet controls by Technology Services as outlined in Finding 1.8, the Department of Transportation and Infrastructure will develop and implement appropriate spreadsheet controls aligned with the policy.

2.1 **Implement Vendor Management System** – The Technology Services agency should continue to implement the ServiceNow Vendor Management module to fully document the review process and schedule recurring reviews for System and Organization Controls for Service

Organizations, or SOC, reports. The agency should follow up with the vendor on control gaps identified in the report.

Agency Response: Agree, Implementation Date – Dec. 31, 2020

Agency Narrative: Technology Services agrees with the recommendation and has implemented the vendor risk assessment module in ServiceNow to document and track vendor assessments related issues. We are also in the process of setting up recurring vendor reviews, which will include both cloud-based vendors and non-cloud-based vendors.

2.2 **Implement Periodic Cloud-Based Vendor Security Reviews** – The Technology Services agency should implement a process to review cloud-based vendors' ongoing adherence to the Cloud Security Alliance security controls. If gaps in the vendors' security controls are identified, Technology Services should implement sufficient additional controls to mitigate the lack of security or decommission the noncompliant vendor service until the security issues can be adequately addressed.

Agency Response: Agree, Implementation Date – Dec. 31, 2020

Agency Narrative: Technology Services agrees with the recommendation and has implemented the vendor risk assessment module in ServiceNow to document and track vendor assessments related issues. We are also in the process of setting up recurring vendor reviews, which will include both cloud-based vendors and non-cloud-based vendors.

2.3 **Obtain System and Organization Controls for Service Organizations Reports** – The Department of Public Works should obtain its vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review to determine whether backups are scheduled and tested on a periodic basis. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation for asset management software vendors. The Department will work with vendors to mitigate risks identified in the audit findings. DOTI will develop and add language to applicable department contracts that establish data standards and include routine contract compliance deliverables such as routine SOC reporting, backup schedules, and backup test results.

The Department will obtain SOC reports or other attestation documentation from Deighton and Cartegraph for those asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020 and incorporate language covering SOC reports as new asset management software contracts (or extensions of existing) are implemented; for Deighton and Cartegraph this will be completed by October 30, 2020.

2.4 **Review Vendor Disaster Recovery Controls** – The Department of Public Works should obtain the vendor System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the disaster recovery information contained in

these reports to ensure the vendors' disaster recovery processes meet Public Works' needs. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation and review for disaster recovery procedures. The Department will establish, with the assistance of Technology Services, a review checklist to identify potential disaster recovery risks, and will work with vendors to mitigate those identified risks.

The Department will obtain SOC report or other attestation documentation from Deighton and Cartegraph asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020. The Department will incorporate language covering SOC reports as new asset management software contracts are implemented; for Deighton and Cartegraph this will be completed by October 30, 2020.

2.5 **Review Vendor Change Management Controls** – The Department of Public Works should obtain the vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the change management information contained in these reports to ensure the vendors' change management controls meets Public Works' needs. The department should follow up with the vendors on control gaps identified in the report and mitigate any risks identified.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation and review for change management controls. The Department will work with vendors to mitigate any risks identified.

The Department will obtain SOC report or other attestation documentation from Deighton and Cartegraph asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020. The Department will incorporate language covering SOC reports as new asset management software contracts are implemented. For Deighton and Cartegraph this will be completed by October 30, 2020.

2.6 **Implement Complementary User Controls** – The Department of Public Works should ensure it evaluates the complementary user controls as identified in each vendor's System and Organization Controls for Service Organizations, or SOC, report and implements those controls that are feasible.

Agency Response: Agree, Implementation Date – 180 days after receipt of SOC reports

Agency Narrative: The Department of Transportation and Infrastructure will identify and implement additional controls based on the assessment of current SOC reports.

2.7 **Review Insurance Coverage** – The Department of Public Works should develop a process to receive, track, and review all insurance coverage certificates from technology vendors to ensure they are maintaining compliance with the city's insurance requirements.

Agency Response: Agree, Implementation Date – June 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will develop a process to ensure acceptable evidence of insurance is provided and renewed for all executed contracts and their amendments to confirm insurance requirements continue to be met during the term of the agreement.

3.1 **Improve Contracting Process** – The Technology Services agency should work with all parties involved in the contracting process to improve the contract routing and approval process to ensure Technology Services is included in all technology purchases.

Agency Response: Agree, Implementation Date – July 15, 2020

Agency Narrative: When the requisite authority is established as noted in the Recommendation 1.1 narrative, Technology Services will work with all parties and define our involvement in the technology procurement process.

3.2 **Clarify Contract Language** – The Department of Public Works should clarify the Cartegraph contract language regarding the responsibility for performing backups and for how frequently those backups should occur.

Agency Response: Agree, Implementation Date – Oct. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will clarify / modify language in the renewed Cartegraph contract to specify back-up protocols and frequency, conforming to Technology Services guidance and policies, to ensure appropriate levels of redundancy.

4.1 **Improve Customer Service** – The Technology Services agency should improve its customer service for the Department of Public Works' technology issues.

Agency Response: Agree, Implementation Date – Immediately

Agency Narrative: Notwithstanding the possibility that Technology Services may disagree from time to time with Public Works' perspective on a technology direction or procurement, the Technology Services Agency strives to communicate effectively and efficiently with Public Works, regardless of the level of agreement. To that end and given this specific example in which Technology Services was considered unresponsive by Public Works, Technology Services will improve our customer service with Public Works.

4.2 **Establish Service-Level Agreements** – The Technology Services agency should establish and communicate a standard process with expected response times and escalation path for handling customer requests and disagreements.

Agency Response: Agree, Implementation Date – March 31, 2020

Agency Narrative: Technology Services is committed to continuously enhancing the customer experience for all our customers. We will evaluate resource capacity within our existing Business Relationship Management Program with intention to improve our specific partnership, communication, and customer service with Public Works.

4.3 **Improve dTIMS Password Settings** – The Technology Services agency should work with the Department of Public Works to ensure dTIMS meets password security requirements as soon as possible by integrating dTIMS into the city's active directory or ensuring that a vendor-provided solution meets Technology Services' requirements.

Agency Response: Agree, Implementation Date – March 15, 2020

Agency Narrative: Technology Services agrees with the final clause of the recommendation in that the vendor-provided solution should meet Technology Services' requirements. The current vendor solution does not meet the city's information security requirements. Technology Services has provided a response and recommendations to Public Works and the vendor. Public Works should work with its vendor to find a solution that complies with the city's established security requirements.

4.4 **Communicate Update Process** – The Technology Services agency should, as soon as possible, communicate its process to the Department of Public Works for updating the city's geographic information system database.

Agency Response: Agree, Implementation Date – Jan. 31, 2020

Agency Narrative: The process for updating the geographic information system (GIS) database is published in the city's intranet, DenverHub. We will launch a communication campaign to increase the awareness of the process.

5.1 **Formalize Asset Management Strategy** – The Department of Public Works should continue its efforts to develop an asset management strategy by formalizing its asset management approach and:

- Developing a comprehensive charter;
- Creating specific deliverables and objectives;
- Identifying a business case and requirements; and
- Conducting an analysis of stakeholder needs.

Agency Response: Agree, Implementation Date – Sept. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure has completed a charter for the Office of Asset Management ("OAM"). Specific deliverables, objectives, business case and requirements will be incorporated into a business plan for the Office of Asset Management. An analysis of stakeholder needs is in progress.

The charter has been completed as of December 31, 2019. The creation of deliverables

and objectives will be finalized by March 31, 2020. The completion of the business case and requirements will be completed by March 31, 2020. An analysis of stakeholder needs will be completed by September 30, 2020.

5.2 **Consult with the Chief Data Officer** – The Department of Public Works should continue its efforts to develop an asset management strategy by consulting with the chief data officer to leverage their experience in developing data standards to ensure consistency between the various asset management platforms.

Agency Response: Agree, Implementation Date – Ongoing

Agency Narrative: The Department of Transportation and Infrastructure will continue ongoing meetings with the Chief Data Officer for coordination of the asset management strategy, tools and systems, data standards and asset management best practices.

5.3 **Engage Technology Services** – The Department of Public Works should continue its efforts to develop an asset management strategy by engaging the Technology Services agency as soon as possible to assist with the asset management initiative to ensure information technology and project management best practices are followed.

Agency Response: Agree, Implementation Date – Sept. 30, 2020

Agency Narrative: The Department of Transportation and Infrastructure will partner with Technology Services in the review of stakeholder needs to establish Information Technology best practices in relation to asset management processes.

The Department will further engage with Technology Services and collaborate on a data collection RFP by March 31, 2020, as well as collaborate with Technology Services regarding contract extensions with Deighton (June 30, 2020) and Cartegraph (September 30, 2020).

AGENCIES' RESPONSES TO AUDIT RECOMMENDATIONS

DENVER
THE MILE HIGH CITY

January 9, 2020

Auditor Timothy M. O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted a performance audit of Public Works Asset Management Software Applications.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on December 16, 2019. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The Lack of Formal Citywide Policies for Information Technology Processes to Guide Agency Procedures Creates Cybersecurity and Operational Risks

RECOMMENDATION 1.3 **Develop User Access Process** – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible to grant, change, and remove user system access.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	June 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 1.3

The Department of Transportation and Infrastructure will work with Technology Services to create a user access procedure to cover asset management software system access and user privilege modifications. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/dotI
Phone: (720) 865 - 8630

311 | POCKETGOV.COM | DENVERGOV.ORG | DENVER 8 TV

DENVER
THE MILE HIGH CITY

RECOMMENDATION 1.4 **Develop Administrator User Review Process** – The Department of Public Works, with guidance from the Technology Services agency, should develop a formal process as soon as possible for approving administrator user accounts.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	June 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 1.4

The Department of Transportation and Infrastructure will work with Technology Services to create an asset management software administrator process and procedure to cover administrator roles and responsibilities. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

RECOMMENDATION 1.5 **Develop an Access Removal Process** – The Department of Public Works should develop a process to notify Workday administrators to remove user access for all users, including unpaid interns, when their employment or internship is completed.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	June 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 1.5

The Department of Transportation and Infrastructure will work with Workday administrators to create a process for timely and appropriate access removal for all staff (including unpaid interns) with asset

management system access. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

RECOMMENDATION 1.6 **Develop User Access Review** – The Department of Public Works, working with the Technology Services agency, should develop a process as soon as possible to establish periodic user access review listings to ensure user access remains appropriate for all applications and that appropriate segregation of duties is maintained.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	June 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 1.6

The Department of Transportation and Infrastructure will work with Technology Services to create a quarterly asset management software access review to ensure system access is verified. Procedure development and documentation will be completed by March 30, 2020 with implementation finalized by June 30, 2020.

RECOMMENDATION 1.7 **Develop Succession Plan** – The Department of Public Works, with guidance from the Technology Services agency, should ensure there is a succession plan as soon as possible for all system administrator roles.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2020	Pat Kennedy (303) 446-3535

DENVER
THE MILE HIGH CITY

Narrative for Recommendation 1.7

The Department of Transportation and Infrastructure will include, in the Office of Asset Management Business Plan, succession planning for all asset management software system administrator roles to include identifying secondary personnel and the provision of cross training.

RECOMMENDATION 1.9

Implement Spreadsheet Controls – Working with the Technology Services agency, the Department of Public Works should, as soon as possible, move to a solution with appropriate information technology controls or implement spreadsheet control procedures that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed
5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	180 Days after completion of recommendation 1.8	Pat Kennedy (303) 446-3535

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/dot
Phone: (720) 865 - 8630

311 | POCKETGOV.COM | DENVERGOV.ORG | DENVER 8 TV

Narrative for Recommendation 1.9

Upon completion of a citywide Policy(s) for key spreadsheet controls by Technology Services as outlined in Finding 1.8, the Department of Transportation and Infrastructure will develop and implement appropriate spreadsheet controls aligned with the policy.

AUDIT FINDING 2
Poor Vendor Oversight Puts Asset Management Data at Risk

RECOMMENDATION 2.3 Obtain System and Organization Controls for Service Organizations Reports – The Department of Public Works should obtain its vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review to determine whether backups are scheduled and tested on a periodic basis. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 2.3

The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation for asset management software vendors. The Department will work with vendors to mitigate risks identified in the audit findings. DOTI will develop and add language to applicable department contracts that establish data standards and include routine contract compliance deliverables such as routine SOC reporting, backup schedules, and backup test results.

The Department will obtain SOC reports or other attestation documentation from Deighton and Cartegraph for those asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020 and incorporate language covering SOC reports as new asset management software contracts (or extensions of existing) are implemented; for Deighton and Cartegraph this will be completed by October 30, 2020.

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/doti
Phone: (720) 865 - 8630

311 | POCKETGOV.COM | DENVERGOV.ORG | DENVER 8 TV

DENVER
THE MILE HIGH CITY

RECOMMENDATION 2.4 Review Vendor Disaster Recovery Controls – The Department of Public Works should obtain the vendor System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the disaster recovery information contained in these reports to ensure the vendors' disaster recovery processes meet Public Works' needs. The department should follow up with the vendor on control gaps identified in the report and mitigate any risks identified.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 2.4

The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation and review for disaster recovery procedures. The Department will establish, with the assistance of Technology Services, a review checklist to identify potential disaster recovery risks, and will work with vendors to mitigate those identified risks.

The Department will obtain SOC report or other attestation documentation from Deighton and Cartegraph asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020. The Department will incorporate language covering SOC reports as new asset management software contracts are implemented; for Deighton and Cartegraph this will be completed by October 30, 2020.

RECOMMENDATION 2.5 Review Vendor Change Management Controls – The Department of Public Works should obtain the vendors' System and Organization Controls for Service Organizations, or SOC, reports or other attestation documentation and review the change management information contained in these reports to ensure the vendors' change management controls meets Public Works' needs. The department should follow up with the vendors on control gaps identified in the report and mitigate any risks identified.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/doti
Phone: (720) 865 - 8630

	(Generally expected within 60 to 90 days)	
Agree	October 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 2.5

The Department of Transportation and Infrastructure will obtain SOC reports or other attestation documentation and review for change management controls. The Department will work with vendors to mitigate any risks identified.

The Department will obtain SOC report or other attestation documentation from Deighton and Cartegraph asset management systems by March 31, 2020. The Department will finalize asset management data standards by June 30, 2020. The Department will incorporate language covering SOC reports as new asset management software contracts are implemented. For Deighton and Cartegraph this will be completed by October 30, 2020.

RECOMMENDATION 2.6
Implement Complementary User Controls – The Department of Public Works should ensure it evaluates the complementary user controls as identified in each vendor's System and Organization Controls for Service Organizations, or SOC, report and implements those controls that are feasible.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	180 Days after receipt of SOC reports	Pat Kennedy (303) 446-3535

Narrative for Recommendation 2.6

The Department of Transportation and Infrastructure will identify and implement additional controls based on the assessment of current SOC reports.

DENVER
THE MILE HIGH CITY

RECOMMENDATION 2.7 **Review Insurance Coverage** – The Department of Public Works should develop a process to receive, track, and review all insurance coverage certificates from technology vendors to ensure they are maintaining compliance with the city's insurance requirements.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	June 30, 2020	Elizabeth Zollo (720) 913-1774

Narrative for Recommendation 2.7

The Department of Transportation and Infrastructure will develop a process to ensure acceptable evidence of insurance is provided and renewed for all executed contracts and their amendments to confirm insurance requirements continue to be met during the term of the agreement.

AUDIT FINDING 3
The City's Contracting Process Failed to Include Technology Services' Required Review and Approval of a Technology Purchase

RECOMMENDATION 3.2 Clarify Contract Language – The Department of Public Works should clarify the Cartegraph contract language regarding the responsibility for performing backups and for how frequently those backups should occur.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 3.2

The Department of Transportation and Infrastructure will clarify / modify language in the renewed Cartegraph contract to specify back-up protocols and frequency, conforming to Technology Services guidance and policies, to ensure appropriate levels of redundancy.

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/doti
Phone: (720) 865 - 8630

311 | POCKETGOV.COM | DENVERGOV.ORG | DENVER 8 TV

DENVER
THE MILE HIGH CITY

AUDIT FINDING 5
The Public Works Department Does Not Have a Formal Strategy for Asset Management

RECOMMENDATION 5.1
Formalize Asset Management Strategy – The Department of Public Works should continue its efforts to develop an asset management strategy by formalizing its asset management approach and

- Developing a comprehensive charter;
- Creating specific deliverables and objectives;
- Identifying a business case and requirements; and
- Conducting an analysis of stakeholder needs.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	September 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 5.1

The Department of Transportation and Infrastructure has completed a charter for the Office of Asset Management ("OAM"). Specific deliverables, objectives, business case and requirements will be incorporated into a business plan for the Office of Asset Management. An analysis of stakeholder needs is in progress.

The charter has been completed as of December 31, 2019. The creation of deliverables and objectives will be finalized by March 31, 2020. The completion of the business case and requirements will be completed by March 31, 2020. An analysis of stakeholder needs will be completed by September 30, 2020.

RECOMMENDATION 5.2
Consult with the Chief Data Officer – The Department of Public Works should continue its efforts to develop an asset management strategy by consulting with the chief data officer to leverage their experience in developing data standards to ensure consistency between the various asset management platforms.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation

	(Generally expected within 60 to 90 days)	
Agree	Ongoing	Brandon Lawrence (720) 913-1760

Narrative for Recommendation 5.2

The Department of Transportation and Infrastructure will continue ongoing meetings with the Chief Data Officer for coordination of the asset management strategy, tools and systems, data standards and asset management best practices.

RECOMMENDATION 5.3 **Engage Technology Services** – The Department of Public Works should continue its efforts to develop an asset management strategy by engaging the Technology Services agency as soon as possible to assist with the asset management initiative to ensure information technology and project management best practices are followed.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	September 30, 2020	Pat Kennedy (303) 446-3535

Narrative for Recommendation 5.3
The Department of Transportation and Infrastructure will partner with Technology Services in the review of stakeholder needs to establish Information Technology best practices in relation to asset management processes.

The Department will further engage with Technology Services and collaborate on a data collection RFP by March 31, 2020, as well as collaborate with Technology Services regarding contract extensions with Deighton (June 30, 2020) and Cartegraph (September 30, 2020).

DENVER
THE MILE HIGH CITY

Please contact Seth Runkle at (720) 865-8707 with any questions.

Sincerely,

Seth Runkle
Chief Financial Officer
Department of Transportation and Infrastructure

cc: Valerie Walling, CPA, Deputy Auditor
Brenda Berlin, CPA, IT Audit Supervisor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director
Dawn Wiseman, CRMA, Audit Director
Eulois Cleckley, Executive Director, Dept of Transportation and Infrastructure
Todd Richardson, Deputy Manager - Operations, Dept of Transportation and Infrastructure
David Edinger, Chief Information Officer
Christine Binnicker, Deputy Chief Information Officer

City and County of Denver Department of Transportation & Infrastructure
201 W Colfax Avenue | Denver, CO 80202
www.denvergov.org/dotI
Phone: (720) 865 - 8630

311 | POCKETGOV.COM | DENVERGOV.ORG | DENVER 8 TV

DENVER
TECHNOLOGY SERVICES

Technology Services
201 West Colfax Avenue
Department 301
Denver, CO 80202

January 8, 2020

Auditor Timothy M. O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted a performance audit of Public Works Asset Management Software Applications.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on December 16, 2019. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The Lack of Formal Citywide Policies for Information Technology Processes to Guide Agency Procedures Creates Cybersecurity and Operational Risks

RECOMMENDATION 1.1 **Update Necessary Laws** – The Technology Services agency should have the necessary laws updated as soon as possible to enable the agency to establish and enforce standardized citywide information technology policies.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	April 15, 2020	David Edinger Chief Information Officer 720-865-9033

Narrative for Recommendation 1.1
The mission and functions of Technology Services have evolved over the years, moving beyond the scope of the current Executive Order (XO) No. 18. We will evaluate the options of revising XO No. 18 or consider an alternative form of authority (ex: charter) to provide the requisite power to fulfill our mission and deliver effective services.

RECOMMENDATION 1.2 **Create Information Technology Policies** – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should create citywide information technology policies and establish the means to ensure all city agencies are complying with these policies.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	July 15, 2020	David Edinger Chief Information Officer 720-865-9033

Narrative for Recommendation 1.2
When the requisite authority is established, Technology Services will create related citywide policies and control processes to ensure compliance.

RECOMMENDATION 1.8

Create Spreadsheet Best Practice – When the laws are updated as noted in Recommendation 1.1, the Technology Services agency should establish standard citywide best practices for key spreadsheet controls that address the following areas:

1. Change controls – develop controls to highlight changes made to the spreadsheet calculations or reporting
2. Version control – set up automated version control of all files when they are updated to allow tracking of changes made
3. Access control – restrict users' access to the folders where the critical files are stored and set up password protection of individual files
4. Input controls – set up "checksum" totals to confirm the accuracy of data entered, and lock cells with formulas to prevent them from being accidentally changed
5. Documentation – create documentation for each spreadsheet to describe its purpose, methodology, source of data, and outputs
6. Backups – ensure folders where spreadsheets are stored are regularly backed up to a different location

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	April 15, 2020	Paul Kresser Chief Data Officer (720) 913-4876

Narrative for Recommendation 1.8

Microsoft Office 365 is the city's supported productivity suite, which includes Excel as its spreadsheet solution. Office 365 contains extensive native functionality that enables and supports best practices on data management and usage, such as change controls, version controls, access controls and backups. Simply by utilizing Excel as part of our Office 365 suite, Technology Services has already implemented four of the six recommendations (1,2,3, and 6). Recognizing that areas 4 and 5 are intended to establish citywide best practices for key spreadsheets, rather than enforce compliance, Technology Services will develop and communicate these best practices to appropriate agencies and departments.

AUDIT FINDING 2
Poor Vendor Oversight Puts Asset Management Data at Risk

RECOMMENDATION 2.1 Implement Vendor Management System – The Technology Services agency should continue to implement the ServiceNow Vendor Management module to fully document the review process and schedule recurring reviews for System and Organization Controls for Service Organizations, or SOC, reports. The agency should follow up with the vendor on control gaps identified in the report.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	December 31, 2020	Julie Sutton Information Security Manager (720) 913-4964

Narrative for Recommendation 2.1
Technology Services agrees with the recommendation and has implemented the vendor risk assessment module in ServiceNow to document and track vendor assessments related issues. We are also in the process of setting up recurring vendor reviews, which will include both cloud-based vendors and non-cloud-based vendors.

RECOMMENDATION 2.2 Implement Periodic Cloud-Based Vendor Security Reviews – The Technology Services agency should implement a process to review cloud-based vendors' ongoing adherence to the City and County of Denver cloud security controls. If gaps in the vendors' security controls are identified, Technology Services should implement sufficient additional controls to mitigate the lack of security or decommission the noncompliant vendor service until the security issues can be adequately addressed.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	December 31, 2020	Julie Sutton Information Security Manager (720) 913-4964

Narrative for Recommendation 2.2
Technology Services agrees with the recommendation and has implemented the vendor risk assessment module in ServiceNow to document and track vendor assessments related

issues. We are also in the process of setting up recurring vendor reviews, which will include both cloud-based vendors and non-cloud-based vendors.

AUDIT FINDING 3
The City's Contracting Process Failed to Include Technology Services' Required Review and Approval of a Technology Purchase

RECOMMENDATION 3.1 **Improve Contracting Process** – The Technology Services agency should work with all parties involved in the contracting process to improve the contract routing and approval process to ensure Technology Services is included in all technology purchases.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	July 15, 2020	David Edinger Chief Information Officer 720-865-9033

Narrative for Recommendation 3.1
When the requisite authority is established as noted in the Recommendation 1.1 narrative, Technology Services will work with all parties and define our involvement in the technology procurement process.

AUDIT FINDING 4
Technology Services Should Expand its Existing Business Relationship Management Program to Include the Public Works Department to Provide Better Customer Service

RECOMMENDATION 4.1 **Improve Customer Service** – The Technology Services agency should improve its customer service for the Department of Public Works' technology issues.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	Immediately	David Edinger Chief Information Officer 720-865-9033

Narrative for Recommendation 4.1
Notwithstanding the possibility that Technology Services may disagree from time to time with Public Works' perspective on a technology direction or procurement, the Technology Services Agency strives to communicate effectively and efficiently with Public Works, regardless of the level of agreement. To that end and given this specific example in which Technology Services was considered unresponsive by Public Works, Technology Services will improve our customer service with Public Works.

RECOMMENDATION 4.2 **Establish Service-Level Agreements** – The Technology Services agency should establish and communicate a standard process with expected response times and escalation path for handling customer requests and disagreements.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2020	Kevin Anthony Director, Application Planning and Customer Engagement (720) 913-4885

Narrative for Recommendation 4.2
Technology Services is committed to continuously enhancing the customer experience for all our customers. We will evaluate resource capacity within our existing Business Relationship Management Program with intention to improve our specific partnership, communication, and customer service with Public Works.

RECOMMENDATION 4.3 **Improve dTIMS Password Settings** – The Technology Services agency should work with the Department of Public Works to ensure dTIMS meets password security requirements as soon as possible by integrating dTIMS into the city's active directory or ensuring that a vendor-provided solution meets Technology Services' requirements.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 15, 2020	Julie Sutton Information Security Manager (720) 913-4964

Narrative for Recommendation 4.3
Technology Services agrees with the final clause of the recommendation in that the vendor-provided solution should meet Technology Services' requirements. The current vendor solution does not meet the city's information security requirements. Technology Services has provided a response and recommendations to Public Works and the vendor. Public Works should work with its vendor to find a solution that complies with the city's established security requirements.

RECOMMENDATION 4.4 **Communicate Update Process** – The Technology Services agency should, as soon as possible, communicate its process to the Department of Public Works for updating the city's geographic information system database.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	Jan 31, 2020	Kevin Anthony Director, Application Planning and Customer Engagement (720) 913-4885

Narrative for Recommendation 4.4
The process for updating the geographic information system (GIS) database is published in the city's intranet, DenverHub. We will launch a communication campaign to increase the awareness of the process.

Please contact Samantha Shih at 720-913-5485 with any questions.

Sincerely,

David Edinger
Chief Information Officer

cc: Valerie Walling, CPA, Deputy Auditor
Brenda Berlin, CPA, IT Audit Supervisor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director
Dawn Wiseman, CRMA, Audit Director
Christine Binnicker, Deputy Chief Information Officer
Christopher Todd, Chief Technology Officer
Chad Mitchell, Chief Applications Officer
Paul Kresser, Chief Data Officer
Kevin Anthony, Director, Application Planning and Customer Engagement
Julie Sutton, Information Security Manager

OBJECTIVE

The objective of the audit was to evaluate the design and the operating effectiveness of the information technology general controls, specific application controls, and infrastructure assets financial reporting for the Cartegraph and dTIMS asset management systems. The audit also assessed the shared responsibility between the Department of Public Works and the Technology Services agency to define and implement these information technology general controls.

SCOPE

The scope of the audit was limited to Public Works' Cartegraph and dTIMS asset management systems — particularly for information technology general control review and infrastructure asset financial reporting. The audit coverage for information technology general control review is between July 1, 2018, and June 30, 2019, and for asset financial reporting from Jan. 1, 2017, to July 31, 2019. For related contracts and amendments, the audit sought to review Cartegraph since implementation and to review dTIMS during the time the city switched to a cloud services provider.

METHODOLOGY

We applied various methodologies to gather and analyze information related to our audit objective. These included but were not limited to:

- Interviewing the following individuals:
  - Public Works staff (Public Works' asset application business owners and Public Works' financial accounting staff)
  - Cartegraph and Deighton (dTIMS vendor) personnel
  - Technology Services staff
- Reviewing and analyzing the following criteria, policies, contracts, and report documentation:
  - Policies, procedures, and standard operating process related to logical access in Cartegraph and dTIMS
  - Contracts and amendments between the city and the application vendors, generated from the city's Alfresco document management system
  - Project intake and project documentation
  - System and Organization Controls for Service Organizations reports and/or other vendor security assurance documents
  - City password policy
  - City executive orders
  - City Fiscal Accountability Rules and Governmental Accounting Standards Board report

- Active and inactive user populations reports and financial data from Cartegraph and dTIMS asset systems

- Testing the following areas:
  - Password setting is configured appropriately based on the city's password policy.
  - New user access is authorized and appropriately established.
  - Terminated user access is appropriately removed from each of the asset systems and city network.
  - Administrator access is restricted to authorized individuals.
  - Current user access is reviewed on an annual basis.
  - Input and output validation review is conducted.
  - Changes and vendor-supplied software patches that are applied to city asset management systems by respective vendors are validated by Public Works.
  - The backup and recovery process that is performed by the respective vendors is validated by Public Works.
  - Succession plans for system administrators are established for Cartegraph and dTIMS administrator users.
  - System and Organization Controls for Service Organizations Type 2 reports for Cartegraph and dTIMS asset systems are obtained and reviewed by Public Works and Technology Services.
  - Cloud security reoccurrences review are performed for Cartegraph and dTIMS asset management systems.
  - Vendor contract reviews are performed for Cartegraph and dTIMS asset management systems.
  - Public Works' infrastructure asset financial reporting is accurate.

Office of the 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 and contractors for the purpose of ensuring the proper and efficient use of City resources. He also provides other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver's government.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability 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.

201 West Colfax Avenue, #705

Denver CO, 80202

(720) 913-5000 ♦ Fax (720) 913-5253

www.denverauditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public's investment in the City of Denver. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.