May 20, 2021

The objective of our audit was to evaluate the City and County of Denver's information technology disaster recovery planning program.

We found the city's Technology Services agency made progress by creating a disaster recovery policy, but it lacks a comprehensive disaster recovery program because of an insufficient strategy. Technology Services has not prioritized disaster recovery in its strategic planning and operations — which resulted in inadequate governance, a less-than-comprehensive program that lacks documentation and maintenance, and insufficient communication and training strategies. We also identified other risks that we communicated separately because of their sensitive nature.

By implementing recommendations for stronger policies and procedures, Technology Services will be better equipped to recover data and systems during a disaster.

This audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor.” We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the personnel in the city's Technology Services agency 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
**Information Technology Disaster Recovery**

**MAY 2021**

**Objective**

To evaluate Technology Services’ information technology disaster recovery program and determine the extent to which critical systems can be restored in a timely manner.

**Background**

A disaster recovery program focuses on recovering information technology systems and data during an emergency. The program is meant to assure critical city operations continue to function during a disaster.

Technology Services is the lead agency for information technology in the City and County of Denver and provides all information technology-related infrastructure and services to city agencies. Technology Services also conducts the city’s information technology disaster recovery planning.

**Technology Services Disaster Recovery Program Needs Improvement**

- Technology Services has an insufficient disaster recovery strategy and has not prioritized disaster recovery in its strategic planning and operations. This has resulted in inadequate governance, a disaster recovery program that lacks documentation and maintenance, and insufficient communication and training strategies.

- Technology Services also has not given proper authority to its Disaster Recovery Committee, it has not updated its disaster recovery documentation for a new data center, and it has not ensured employees are aware of the disaster recovery program and can plan for their own roles and responsibilities during an emergency.

- Technology Services has not provided adequate disaster recovery awareness and training for agency personnel, contractors or contingent workers, or disaster recovery team members.

- Technology Services does not maintain disaster recovery documentation — including minimal annual tracking of changes to the information system contingency plan — and it lacks disaster recovery metrics from its system of record.

**Why This Matters**

*By Technology Services not having a comprehensive plan, an emergency could cripple city operations — causing excessive downtime, lost data, and irreparable damage to systems.*
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BACKGROUND</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>FINDING AND RECOMMENDATIONS</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Technology Services’ Disaster Recovery Program Needs Improvement</strong></td>
<td>10</td>
</tr>
<tr>
<td>The City’s Information Technology Disaster Recovery Program Lacks an</td>
<td></td>
</tr>
<tr>
<td>Adequate and Comprehensive Governance Structure and Communications</td>
<td></td>
</tr>
<tr>
<td>Strategies</td>
<td></td>
</tr>
<tr>
<td>Technology Services Has Not Maintained Its Disaster Recovery Program</td>
<td>14</td>
</tr>
<tr>
<td><strong>AGENCY RESPONSE TO AUDIT RECOMMENDATIONS</strong></td>
<td>17</td>
</tr>
</tbody>
</table>
Disaster Recovery Planning

The importance of safeguarding information technology data in an emergency is critical. Contingency planning helps ensure systems and data are up and running as soon as possible for the continuity of an organization's operations. Safeguarding data to ensure a swift and complete recovery is known as “disaster recovery planning.”

The Federal Emergency Management Agency defines a disaster as “an occurrence of a natural catastrophe, technological accident, or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries.”

Natural catastrophes include:

- Earthquakes, tsunamis, and volcanic activity.
- Avalanches and floods.
- Extreme temperatures, drought, and wildfires.
- Cyclones and storms.
- Pandemics and insect plagues.

Technological and human-caused disasters include:

- Utility disruptions.
- Dam failures.
- Sabotages.
- Chemical and biological attacks.
- Civil or political violence.
- Cyberattack threats against data or infrastructure.

The National Institute of Standards and Technology, a nonregulatory federal agency within the U.S. Department of Commerce, defines a cyberattack as an attack “that targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”

Examples of cyberattack threats include phishing, fraudulent solicitations through email or websites, and ransomware—a malicious software that holds a system owner hostage by encrypting their data for ransom.

---


Cyberattacks cost time, money, and data loss and can potentially cause more serious damage to property and lives. For example, in May 2019, a five-day human-caused nationwide blackout occurred in Venezuela.\(^3\) Inadequate hospital recovery planning and testing resulted in generators failing at some hospitals. Twenty-six people died, including babies who could not be incubated, gunshot victims who could not be operated on, and patients on dialysis who went into kidney failure when the machines stopped working.

For five days in 2018, the City of Atlanta faced what was described as “one of the most sustained and consequential cyberattacks ever mounted against a major American city.”\(^4\) The cyberattackers locked employee files with encryption, changed file names to “I’m sorry,” and demanded Atlanta officials pay a $50,000 ransom within a week to avoid losing the data forever. Either by luck or design, the attack did not freeze out 911 calls or affect control of the city's wastewater treatment plant. However, staff could not complete other operations, such as validating warrants or accepting employment applications.

The Federal Bureau of Investigation's Internet Crime Complaint Center received 2,047 reports of ransomware in 2019 — at an estimated cumulative adjusted loss of over $8.9 million. The year before, the center fielded 1,493 complaints with an estimated cumulative adjusted loss of $3.6 million.\(^5\)

These dollar amounts underestimate the full impact of these attacks. Many cases do not include a loss amount, and adjusted losses do not take into account estimates for lost business, time, wages, files, or equipment or any third-party remediation services victims may hire.\(^6\) Additionally, the number of instances represents only complaints made directly through the Internet Crime Complaint Center and does not include ransomware attack complaints made to bureau field offices.

Atlanta and Venezuela are two important examples of the costs of government not planning for disasters.

The National Institute of Standards and Technology provides a checklist of controls for organizations to incorporate into their comprehensive disaster recovery programs.\(^7\) Topics include alternate processing and storage sites, telecommunications, annual testing, and the importance of maintaining documented plans that reflect actual business processes and remedies for recovery.

---


Preventing for disasters and human-caused attacks require vigilance from local, state, and federal governments. They must comprehensively plan, develop, and maintain contingency plans and disaster recovery policy and procedures.

**Contingency Planning**

“Contingency planning” involves interim measures to recover information system services and data after a disruption. A disaster recovery program is integral to contingency planning. It focuses on recovering information technology systems and data, while a continuity of operations plan focuses on other physical assets and personnel, as well as essential functions.

Figure 1 on the following page shows the National Institute of Standards and Technology's comprehensive framework for contingency planning and disaster recovery for information technology, as part of an overall continuity of operations planning.

This framework encourages organizations to plan with three main focuses: information systems, assets and personnel, and the business and mission.

- The information systems focus encourages organizations to create both a critical infrastructure protection plan and a cyber-incident response plan. The critical infrastructure protection plan provides policies and procedures to identify and protect the organization's critical infrastructure components. The cyber-incident response plan provides procedures to mitigate and recover from cyberattacks.

  Information system contingency plans include procedures to recover each mission-critical information system and are typically developed by an information system's content owner.

- The focus on assets and personnel includes occupant emergency plans for first-response procedures. Additionally, a crisis communications plan provides standards to follow for internal and external communications during a disruptive event.

- The business and mission function plans include the continuity of operations plan, which should include plans for restoring mission-essential functions at an alternate site for up to 30 days. A business continuity plan is similar but focuses on a lower or expanded level of detail from the mission-essential functions covered in the continuity of operations plan.

The federal framework allows differently focused plans to be coordinated as part of an overall disaster recovery program.

---

FIGURE 1. Contingency and Disaster Recovery Program Framework

- Information system-focused plan
- Assets/personnel-focused plan
- Business/mission process-focused plan

Note: Multiple information system contingency plans and business continuity plans can be activated.
Source: Image designed by Auditor’s Office staff based on the National Institute of Standards and Technology’s framework diagram.

The City's Executive Order No. 18

Technology Services is the lead agency for information technology in the City and County of Denver and provides all information technology-related infrastructure and services to city agencies. Technology Services also conducts the city’s disaster recovery planning.

The mayor first established Technology Services' authority in 2005 through Executive Order No. 18. Initially, Denver International Airport, the Denver County Court, the Denver Public Library, and independently elected officials such as the clerk and recorder were exempt from Technology Services' purview and oversight of disaster recovery. Those city agencies managed their own technology assets and were responsible for creating their own disaster recovery plans for the data and systems not owned and

---

9 Exec. Order No. 18, City and County of Denver (2005).
managed by Technology Services.

After a January 2020 audit, we determined that, upon reading the 2005 version of Executive Order No. 18, it was “unclear if Technology Services has the authority to establish the citywide information technology policies needed to address today’s technology environment. Technology Services has not created or implemented citywide policies because of this vagueness.”

Recommendations were then made to the city to update the executive order to clarify Technology Services’ authority.

Subsequently, the mayor updated the executive order in January 2021. The order now says Technology Services staff have the authority to administer, manage, and sustain technology devices for all agencies, departments, divisions and other governmental instrumentalities of the City and County of Denver (“Users”) that operate on the Network. It also now specifically authorizes Technology Services to have a new and more comprehensive citywide role for information technology and disaster recovery.

Technology Services uses disaster recovery planning efforts to recover systems and data after a disruption.

As of October 2020, Technology Services had two data centers that supported nearly 500 software applications and used a mix of over 1,900 devices, including mainframes, standalone servers, and virtual servers. In 2019, Technology Services chose to migrate these data centers to a more modern alternate facility. This should be completed by the middle of 2021. Protecting these assets against a disaster is extremely important to ensure the city’s continued operations.

In September 2017, Technology Services’ staff created a disaster recovery planning policy to provide direction on elements of the city’s disaster recovery program. The agency incorporated industry guidelines from sources such as the Federal Emergency Management Agency and the National Institute of Standards and Technology.


As part of the city’s continuity planning efforts, all city agencies must develop and submit their own continuity of operations plans to the city’s Office of Emergency Management and Homeland Security. These plans are meant to ensure city operations continue to function during a disaster.

Technology Services’ continuity of operations plan includes disaster recovery procedures for mission-essential city functions it must restore after a disaster. These applications, systems, and data are prioritized by tiers of importance and also include third-party cloud systems related to body cameras, payroll operations, etc.

ServiceNow is the tool Technology Services uses to track all technology equipment and applications. For some of the tiered systems, Technology Services keeps records in ServiceNow of metrics for recovery applications and data systems during a disaster. Metrics commonly found in disaster recovery programs include:

- **RECOVERY POINT OBJECTIVE** – The “point in time, prior to a disruption or system outage, to which mission/business process data must be recovered after an outage.”\(^\text{13}\)

- **RECOVERY TIME OBJECTIVE** – The “maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the maximum tolerable downtime.”\(^\text{14}\)

- **MAXIMUM TOLERABLE DOWNTIME** – The “total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations.”\(^\text{15}\)

These metrics measure recovery time after a disaster. To protect systems and data from being lost or disrupted, Technology Services also conducts security reviews of third-party applications, systems, and data.

The agency’s information security team collects, evaluates, and records independently curated security assessment reports as well as system and organization controls reports, but the team is focused mainly on protecting regulated data.\(^\text{16}\) Each of these elements of Technology Services’ work are essential to ensuring the city’s technology is protected.

---


\(^\text{14}\) National Institute of Standards and Technology, Special Publication 800-34 (Revision 1).

\(^\text{15}\) National Institute of Standards and Technology, Special Publication 800-34 (Revision 1).

\(^\text{16}\) A system and organization controls report is an independently audited report that provides assurance over the design, implementation, and effectiveness of safeguards for applications and systems provided by a contracted service provider.
Specifically, as shown in Figure 2, this includes information related to criminal justice systems, health records, payment card charges, and personally identifiable information.

**FIGURE 2. Types of Regulated Data**

- **Criminal Justice Information System**
- **Health Information Portability and Accountability Act**
- **Payment Card Industry Standards (Credit Cards)**
- **Personally Identifiable Information**

*Source: Image designed by Auditor’s Office staff.*
FINDING AND RECOMMENDATIONS

Technology Services’ Disaster Recovery Program Needs Improvement

Technology Services has a disaster recovery policy, but the agency lacks a comprehensive plan because it has an insufficient disaster recovery strategy.

Technology Services has not prioritized disaster recovery in its strategic planning and operations. This has resulted in inadequate governance, a less-than-comprehensive disaster recovery program that lacks documentation and maintenance, and insufficient communication and training strategies.

Figure 3 lays out the National Institute of Standards and Technology’s seven fundamental steps to help organizations develop an information technology contingency plan.

FIGURE 3. Progressive Steps for Contingency and Disaster Recovery Planning

<table>
<thead>
<tr>
<th></th>
<th>DEVELOP</th>
<th>Develop the contingency planning policy statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Analyze</td>
<td>Conduct the business impact analysis</td>
</tr>
<tr>
<td>2</td>
<td>IDENTIFY</td>
<td>Identify preventive controls</td>
</tr>
<tr>
<td>3</td>
<td>CREATE</td>
<td>Create contingency strategies</td>
</tr>
<tr>
<td>4</td>
<td>DEVELOP</td>
<td>Develop an information system contingency plan</td>
</tr>
<tr>
<td>5</td>
<td>TEST</td>
<td>Ensure plan testing, training, and exercises</td>
</tr>
<tr>
<td>6</td>
<td>MAINTAIN</td>
<td>Ensure plan maintenance</td>
</tr>
</tbody>
</table>

A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

The business impact analysis helps identify and prioritize information systems and components critical to supporting the organization’s mission and business processes. A template for developing the analysis is provided to assist the user.

Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system’s security impact level and recovery requirements.

Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps. Combined, the activities improve plan effectiveness and overall organization preparedness.

The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

Source: Image designed by Auditor’s Office staff from the National Institute of Standards and Technology’s contingency planning guidance.
Contingency planning for city governments typically starts with identifying mission-essential functions deemed critical for the continuity of government (i.e., to ensure the city continues to operate and provide services to its residents). After identifying these functions, a city identifies who will be responsible for developing disaster recovery strategies, including the disaster recovery program.

Disaster recovery programs should include business impact analyses — which determine recovery metrics such as recovery time objectives, recovery point objectives, and maximum tolerable downtimes — for all critical systems.\(^{17}\)

Furthermore, disaster recovery programs should address backup restoration, alternative processing and data storage sites, telecommunications, communications and training plans, and annual program tests.

Other cities have developed more complete examples of disaster recovery strategies as a part of their strategic planning. For example, the City of Fort Collins, Colorado, developed disaster recovery strategies and included them in the city’s strategic plan. The city grouped initiatives by year and created initiatives such as conducting a business impact analysis and identifying appropriate recovery and continuity technologies. Similarly, the City and County of San Francisco’s five-year information technology strategic plan details its information technology protection and disaster recovery strategies, with associated performance metrics to achieve by 2024.

Without comprehensive strategic planning for disaster recovery — such as metrics measuring progress, success, and achievement towards goals — Technology Services is left without a strategic direction for planning disaster recovery now and in the future.

Although we found the agency lacks a comprehensive disaster recovery program, Technology Services has made progress. For example, the agency developed a disaster recovery policy in 2017, which was updated in 2019. Technology Services also built information system contingency plans for critical applications that it manages.\(^{18}\) The agency also plans to complete its move into a new tier 4 data center by mid-2021, which should reduce significant information systems and data security risks. The new data center and network configuration will provide real-time backup of the entire network for processing and storage.

Therefore, it is critically important that Technology Services staff work with city officials to revise and improve disaster recovery-related plans, policies, and strategy to enable the agency and the city to establish, enforce, measure, and maintain a formalized citywide information technology disaster recovery program.


\(^{18}\) Information system contingency plans are developed for each individual critical system as guidance on how to recover each system and related data.
The City’s Information Technology Disaster Recovery Program Lacks an Adequate and Comprehensive Governance Structure and Communications Strategies

Technology Services has not given proper authority to its Disaster Recovery Committee, it has not updated its disaster recovery program documentation for the new data center, and it has not ensured that all employees are aware of the disaster recovery program and can plan for their own roles and responsibilities during an emergency. Technology Services also has not delivered adequate disaster recovery awareness and training activities for agency personnel, contractors, or contingent workers, as well as disaster recovery team members.

Without comprehensive disaster recovery strategic planning, governance, documentation, and communication and training strategies, the city is at risk of not being fully prepared to recover data and systems from a disaster.

The Disaster Recovery Committee Lacks a Charter to Establish Its Authority

In November 2020, Technology Services created the Disaster Recovery Committee, fulfilling one of its disaster recovery policy requirements. However, we found the agency does not have a charter to establish the committee’s authority over disaster recovery. Not having a charter prevents the committee from having the authority to meet and develop policies. It also creates uncertainty for the members’ roles and responsibilities.

Technology Services has not given formal authority to the committee and has not determined membership requirements. It also has not decided where the committee should focus its attention.

According to city ordinance, several aspects of a disaster recovery committee's authority should be established through a charter. The ordinance recommends the following elements of a charter:

- Powers and duties of the advisory body.
- Requirements for appointments to committees and terms for the appointments.
- Lists of the requirements for who can be a member of the committee.
- A schedule for meetings.
- The requirements for consulting with agencies.

The cities of San Francisco, Seattle, and Los Angeles each created charters and policies for their respective information technology disaster recovery and governance committees. For example, the charter for the City and County of San Francisco’s Committee on Information Technology says its “policies should be implementable and sustainable. Impact analysis and performance evaluation metrics on both information technology systems and end-users should be included in the policy planning and review processes.” The committee developed and recommended specific disaster

---

19 Denver Revised Municipal Code § 2-126 through § 2-140.
20 City and County of San Francisco, Committee on Information Technology, Architecture Policy & Review Board Policy Development Framework.
recovery strategies, which the city adopted in its five-year information technology strategic plan.

As Denver’s Disaster Recovery Committee moves forward with disaster recovery planning and policy, strategic planning should be an integral part of the committee’s powers and duties. According to the city’s disaster recovery policy, the Disaster Recovery Committee is responsible for developing and overseeing a comprehensive disaster recovery program.

In addition, the committee does not have members from other agencies outside the Technology Services team. Technology Services is the central point of contact for disaster recovery for systems on the city’s network. But that leaves out other agencies that operate systems outside Technology Services’ purview and manage their own disaster recovery. For example, Denver International Airport does not rely on Technology Services for its systems and data. Therefore, Technology Services would not be directly involved in restoring airport systems. If the city’s systems go down in a regional information technology disaster, all agencies will need to work together to get systems back online.

The recent update to Executive Order No. 18 gave Technology Services greater authority to organize and direct information technology activities and personnel operating on the city’s network, including the ability to reassign information technology personnel. In addition, best practices say advisory committees should include members who represent the population that the committee’s decisions will impact.

The cities of San Francisco, Seattle, and Los Angeles all created information technology disaster recovery and governance committees that include members from various agencies. Not having a diverse membership on the Disaster Recovery Committee prevents Technology Services from being able to safeguard the entire city from an information technology disaster.

**Disaster Recovery Documentation Does Not Include the New Data Center**

Technology Services has not included its move to a new data center in all its disaster recovery program documentation — such as the disaster recovery policy, the agency’s continuity of operations plan, and information system contingency plans.

Federal standards recommend that organizations ensure formal written procedures reflect the current environment. This would be achieved most effectively by developing written procedures concurrently while a project

---


plan is completed for the new data center.\textsuperscript{24}

However, procedural guides will not be updated by the time the new center opens in mid-2021 and this could result in mistakes by personnel tasked with recovering systems in a disaster.

**Technology Services Does Not Have a Communications Strategy for Disaster Recovery**

Technology Services should ensure all employees are aware of disaster recovery programs so they can plan for their own roles and responsibilities in an emergency. But we learned Technology Services has not done that.

Technology Services does not comprehensively and collaboratively work with other city agencies on their disaster recovery efforts.

Under the updated Executive Order No. 18, Technology Services “has authority to organize and direct” information technology activities and personnel operating on the city’s network — including the ability to reassign information technology staff.\textsuperscript{25} Technology Services has remained focused on disaster recovery efforts for the systems it oversees, but its oversight of all city technology systems is growing because of the updated executive order.

Because Technology Services did not complete its communications and training strategy in accordance with the agency’s policy, employees do not have the guidance and tools to understand their roles and responsibilities in a disaster. We identified additional details related to the inadequate communications strategy and have provided them directly to Technology Services for remediation because they are sensitive in nature.

**Technology Services Has Not Provided Adequate Disaster Recovery Training**

In November 2019, Technology Services staff held a workshop to make decisions on the disaster recovery training needs for the agency's staff. But after that workshop, the agency held no other training and there were no further employee awareness presentations on disaster recovery. This was partially because of the COVID-19 pandemic, and no strategy was created to measure employees’ knowledge of the disaster recovery plans.

According to industry standards, training should be developed to educate employees about their roles in disaster recovery.\textsuperscript{26} Training helps prepare disaster recovery employees for how to activate and exercise plans to help identify gaps. In our research, we found that the City and County of San


Francisco has a training policy for agencies to ensure employees involved in disaster recovery are aware of their responsibilities.

As a result of Technology Services’ lack of training, the City and County of Denver cannot ensure its employees are equipped with the information they need to recover from a disaster.

Based on our review of Technology Services’ disaster recovery governance, policies, and communications and training strategies, we determined the disaster recovery program is not comprehensive enough to help ensure the city can recover fully and quickly from citywide disasters.

The current program also does not include oversight of all city agencies’ information technology assets as now required by Executive Order No. 18. As a result of these issues, we recommend the following:

### 1.1 RECOMMENDATION
Represent Other Agencies on the Disaster Recovery Committee

As Technology Services’ Disaster Recovery Committee establishes itself, it should ensure it collaborates with other agency stakeholders who are content owners of systems that connect to the city’s network. This could include making them members of the committee, inviting them to committee meetings, or sending documented committee decisions and action plans to appropriate agencies.

**AGENCY RESPONSE:** AGREE, IMPLEMENTATION DATE – DEC. 31, 2021
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

### 1.2 RECOMMENDATION
Develop Committee Charter

Technology Services should develop a charter and bylaws for the Disaster Recovery Committee to define the roles and responsibilities of the committee and its members. The charter and bylaws could include:

- Powers and duties of the advisory body.
- Requirements for appointments to committees and terms for the appointments.
- Lists of the requirements for who can be a member.
- A schedule for meetings.
- The requirements for collaborating with agencies.

**AGENCY RESPONSE:** AGREE, IMPLEMENTATION DATE – DEC. 31, 2021
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.
1.3 RECOMMENDATION Update Disaster Recovery Documentation for New Data Center

Technology Services should, as soon as possible, update all disaster recovery documentation to include the new data center before or by the time the center goes live.

AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

1.4 RECOMMENDATION Improve Strategic Plan

The Disaster Recovery Committee should develop comprehensive disaster recovery goals and objectives that are timebound, specific, measurable, and actionable and include them in the Technology Services' strategic plan.

AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

1.5 RECOMMENDATION Develop Disaster Recovery Training

Technology Services should create disaster recovery training that can be presented to all relevant personnel responsible for disaster recovery planning and consider automating the training using Workday Learning. This should include, at a minimum, members of the Disaster Recovery Committee.

AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

Technology Services Has Not Maintained Its Disaster Recovery Program

In addition to reviewing the governance of the information technology disaster recovery program, we assessed the maintenance of the program. Program maintenance includes updating program documentation on a regular basis. But we found there has been minimal annual tracking of changes to the information system contingency plan and disaster recovery metrics are missing from the system of record.
Some Information System Contingency Plans Are Not Consistently Updated

The Technology Services disaster recovery team is not efficiently and comprehensively monitoring and tracking updates and validations to information system contingency plans, nor is the team publishing them annually in the system of record, ServiceNow.

Although Technology Services staff told us the contingency plans are updated annually with Technology Services’ continuity of operations plan, our review indicates this is not always the case. For example, the agency has not prioritized reviewing, validating, and publishing its annual updates of contingency plans as part of its operational strategies.

Federal standards say managers should ensure policies and procedures, such as information system contingency plans, are reviewed periodically to ensure they are efficient and accurate. Absent these periodic reviews, the information system contingency plans may not be up to date if a disaster occurs, and the city will not be able to recover affected systems in a timely and effective manner because of errors in the procedure.

As the System of Record, ServiceNow Should Track Key Metrics

Key information metrics are not kept up to date in Technology Services’ system of record, ServiceNow. For example, recovery time objective, recovery point objective, maximum tolerable downtime, and maximum data loss are kept in separate systems or spreadsheets. We found only the following metrics in ServiceNow:

- Twenty-eight of 514, or 5.4%, of applications contain a recovery time objective.
- Twenty-nine of 514, or 5.6%, of applications contain a maximum tolerable downtime.
- Twenty-three of 514, or 4.4%, of applications contain a maximum data loss.

Because ServiceNow is the system of record, it should hold all performance metrics. However, Technology Services does not collect all recovery performance metrics for systems it does not oversee.

According to the National Institute of Standards and Technology, a business impact analysis should be done to ensure the city knows the tolerable amount of downtime for systems. In addition, the Federal Emergency Management Agency says that “priorities and recovery time objectives for information technology should be developed during the business impact analysis.” Technology Services may not have the data to

---


be able to effectively improve its recovery performance, and subsequently recover from a disaster in a timely manner, without consistently measuring its own performance before a disaster strikes.

A business impact analysis would help Technology Services prioritize the recovery of data and systems. Based on the results of each agency’s business impact analysis, recovery metrics should be developed and input into ServiceNow. We identified additional details related to the business impact analysis and have provided them directly to Technology Services for remediation because they are sensitive in nature.

### 1.6 RECOMMENDATION

**Enhance Backup Metrics**

Technology Services should ensure that backup system failures are tracked, monitored, and include trend statistics to inform management of the time it takes to complete backups, and Technology Services should update the backup system policy based on the trends identified.

**AGENCY RESPONSE:** AGREE, IMPLEMENTATION DATE – DEC. 31, 2021

SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

### 1.7 RECOMMENDATION

**Periodically Review Information System Contingency Plans**

Technology Services should develop a documented policy and procedure to update, validate, and publish information system contingency plans every year.

**AGENCY RESPONSE:** AGREE, IMPLEMENTATION DATE – DEC. 31, 2021

SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

### 1.8 RECOMMENDATION

**Update Recovery Metrics**

Technology Services should ensure ServiceNow is designated as the system of record for all technology services and other agency systems and applications and assign a designee to complete all the fields applicable for each application or system — including recovery time objective, recovery point objective, and maximum tolerable downtime.

**AGENCY RESPONSE:** AGREE, IMPLEMENTATION DATE – DEC. 31, 2022

SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.
May 10, 2021

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 Information Technology Disaster Recovery.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on May 3, 2021. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

PUBLIC REPORT AUDIT FINDING
Technology Services’ Disaster Recovery Program Needs Improvement

RECOMMENDATION 1.1
Represent Other Agencies on the Disaster Recovery Committee – As Technology Services’ Disaster Recovery Committee establishes itself, it should ensure it collaborates with other agency stakeholders who are content owners of systems that connect to the city’s network. This could include making them members of the committee, inviting them to committee meetings, or sending documented committee decisions and action plans to appropriate agencies.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2021</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>

Page 1 of 5
RECOMMENDATION 1.2

Develop Committee Charter – Technology Services should develop a charter and bylaws for the Disaster Recovery Committee to define the roles and responsibilities of the committee and its members. The charter and bylaws could include:

- Powers and duties of the advisory body.
- Requirements for appointments to committees and terms for the appointments.
- Lists of the requirements for who can be a member.
- A schedule for meetings.
- The requirements for collaborating with agencies.

### 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, 2021 | James Balogh, Director Information Technology 720.386.5836

RECOMMENDATION 1.3

Update Disaster Recovery Documentation for New Data Center – Technology Services should, as soon as possible, update all disaster recovery documentation to include the new data center before or by the time the center goes live.

### 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, 2022 | James Balogh, Director Information Technology 720.386.5836

Narrative for Recommendation 1.3
Once the base Sustainability and Resiliency Program and its systems are in place at the new City Data Center, documentation will be updated to reflect the new methodologies and procedures.
RECOMMENDATION 1.4

**Improve Strategic Plan** – The Disaster Recovery Committee should develop comprehensive disaster recovery goals and objectives that are timebound, specific, measurable, and actionable and include them in the Technology Services’ strategic plan.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2022</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.4**
The Sustainability and Resiliency Program and its systems at the new City Data Center will have methodologies and procedures that provide comprehensive, high-fidelity monitoring and operational metrics that adequately describe and report the state of the Sustainability and Resiliency Systems providing the basis for determining the program’s success and operational readiness with regard to the Strategic Plan.

RECOMMENDATION 1.5

**Develop Disaster Recovery Training** – Technology Services should create disaster recovery training that can be presented to all relevant personnel responsible for disaster recovery planning and consider automating the training using Workday Learning. This should include, at a minimum, members of the Disaster Recovery Committee.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2022</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>
RECOMMENDATION 1.6

Enhance Backup Metrics – Technology Services should ensure that backup system failures are tracked, monitored, and include trend statistics to inform management of the time it takes to complete backups, and Technology Services should update the backup system policy based on the trends identified.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2021</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.6
The Sustainability and Resiliency Program and its systems at the new City Data Center will have methodologies and procedures that have comprehensive, high-fidelity monitoring and operational metrics that adequately describe and report the state of the Sustainability and Resiliency Systems providing the basis for determining the program’s success and operational readiness with regard to Data Protection and Backups.

RECOMMENDATION 1.7

Periodically Review Information System Contingency Plans – Technology Services should develop a documented policy and procedure to update, validate, and publish information system contingency plans every year.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2021</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>
RECOMMENDATION 1.8

Update Recovery Metrics – Technology Services should ensure ServiceNow is designated as the system of record for all technology services and other agency systems and applications, and assign a designee to complete all the fields applicable for each application or system — including recovery time objective, recovery point objective, and maximum tolerable downtime.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2022</td>
<td>James Balogh, Director Information Technology 720.386.5836</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.8
The Sustainability and Resiliency Program and its systems at the new City Data Center will have methodologies and procedures that provide comprehensive, high-fidelity monitoring and operational metrics that adequately describe and report the state of the Sustainability and Resiliency Systems providing the basis for determining the program’s success and operational readiness with regard to Recovery.

The Sustainability and Resiliency Program will define classes of RTO, RPO, and MTDs based upon the methodologies and procedures within the new City Data Center. Applications will then be categorized and classified in concordance with the City and County of Denver COG Plan.

Please contact Eunice Mwebi at 720.913.4970 with any questions.

Sincerely,

David Edinger
Chief Information Officer

c: Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director
Jared Miller, CISA, CFE, CDPSE
Nicholas Jimroglou, CISA, CDPSE
James Balogh, Director Information Technology
Christine Binnicker, Deputy Chief Information Officer
Christopher Todd, Chief Technology Officer
OBJECTIVE

To evaluate Technology Services’ information technology disaster recovery program and determine the extent to which critical systems can be restored in a timely manner.

SCOPE

Our audit focused on the period from Jan. 1, 2019, through Dec. 31, 2020. Other agencies’ disaster recovery efforts that Technology Services does not support were not reviewed.

METHODOLOGY

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

- Interviewing key Technology Services personnel to obtain information about the information technology disaster recovery planning process.
- Reviewing and assessing policies and procedures for various aspects of planning for information technology disaster recovery — including data and system backups, annual disaster recovery procedures testing, vendor risk assessments, problem management, cybersecurity prevention and detection, and a move to a new data center.
- Consulting a gap analysis of best practices established by sources such as the National Institute of Standards and Technology, as well as reviewing selected other U.S. cities’ disaster recovery plans.
- Evaluating the completeness of inventories of applications, servers, and third-party service providers including cloud systems.
- Reviewing the collaboration and coordination of Technology Services with other city agencies as it relates to disaster recovery.
- Evaluating the scope of vendor security reviews conducted by Technology Services’ information security team.
- Interviewing Technology Services infrastructure architects, the new data center project manager, the data center manager, and Technology Services executive managers about accepting inherent risks at inadequate data centers and transitioning from those data centers to a new tier 4 data center.
- Evaluating the sufficiency of plans for an alternate processing site.
- Testing the completeness and timeliness of updates to disaster recovery procedures included in Technology Services’ continuity of operations plan.
Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the residents 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 residents’ confidence and avoiding any appearance of a conflict of interest.

Our Mission

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