Audit Team
Nick Jimroglou, CISA, CDPSE, Acting Information Systems Audit Manager
Dave Hancock, CISA, MURP, Information Systems Audit Senior

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
Jack Blumentha, Vice Chairman
Frank Rowe
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

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

Cover photo illustration by Denver Auditor’s Office staff.
AUDITOR’S LETTER

October 5, 2023

In keeping with generally accepted government auditing standards and Auditor’s Office policy, as authorized by city ordinance, we have a responsibility to monitor and follow up on audit recommendations to ensure city agencies address audit findings through appropriate corrective action and to aid us in planning future audits.

After following up on the “Information Technology Disaster Recovery” audit report issued in May 2021, we determined the Technology Services agency fully implemented seven of the recommendations it agreed to and partially implemented one.

During the original audit, we found Technology Services had an insufficient disaster recovery strategy which resulted in inadequate governance, a disaster recovery program that lacked documentation and maintenance, and insufficient communication and training strategies.

Based on our follow-up work, we determined the Technology Services agency did not fully address all the risks associated with our initial findings. Consequently, we may revisit these risk areas in future audits to ensure the city takes appropriate corrective action.

We appreciate the leaders and team members at Technology Services who shared their time and knowledge with us throughout the audit and the follow-up process. Please contact me at 720-913-5000 with any questions.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
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.
Action Since Audit Report
Information Technology Disaster Recovery

8 recommendations proposed in May 2021

Technology Services fully implemented seven of eight recommendations made in the original audit report and partially implemented one.

Because of this, Technology Services will be better equipped to recover data during a disaster and has reduced the risk of losing critical systems. Improvements include adding other agencies to the Disaster Recovery Committee, developing a charter, and updating and reviewing disaster recovery documentation, incorporating the new data center into disaster recovery plans, and providing training.

REMAINING RISKS
The recommendation Technology Services partially implemented will address some of the risk related to backup metrics. However, because backup metrics have not been documented in a backup policy the risk remains that staff responsible for performing these duties may not be aware of their responsibilities.
FINDING | Technology Services’ disaster recovery program needs improvement

FULLY IMPLEMENTED

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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 21, 2021

The Disaster Recovery Committee has had discussions with various agencies throughout the city to further collaborate and encompass a wide range of agency stakeholders. These discussions occur six times a year and address different aspects of disaster recovery. The invitees for these meetings are specifically selected based on the agency need to be on the committee and their expressed interest in participating.

We reviewed agendas and meeting minutes from October 2022 through September 2023 from disaster recovery meetings to verify involvement with other agencies. These meetings covered updates and accomplishments from and included a wide range of agencies including the Office of Emergency Management, Denver International Airport, the District Attorney’s office, and General Services.

Based on this evidence, we consider this recommendation fully implemented.

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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 31, 2021

We reviewed the Disaster Recovery Committee Charter, which was last updated in October 2021, and found that all items outlined in the requirements of the recommendation have now been included.

Therefore, we consider this recommendation fully implemented.

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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 31, 2022

In 2022, Technology Services created new disaster recovery procedures for all major components at the new data center and published them in the third quarter of 2022. The procedures now include system architecture and integrations with hardware components at the data center. All procedures are reviewed and updated for completeness any time a material change is made to the system, or at least once annually.

We reviewed the updated procedures and found they reflect the current environment which includes the new data center and its accompanying systems. Additionally, as noted in Recommendation 1.7, Technology Services has established an annual schedule to review all relevant procedures for material changes and update them as needed.

Therefore, we consider this recommendation fully implemented.
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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 31, 2022

Technology Services staff said disaster recovery specific goals and key performance indicators were added to their 2022 strategic plan in the fourth quarter of 2021. To verify, we reviewed the 2022 disaster recovery goals and objectives. We found 15 measurable goals. These goals include a focus on disaster recovery procedure development, documentation, training, and testing.

We also found the plan establishes a process for quick recovery from a breach, in alignment with the Continuing Operations and Continuity of Government plans coordinated by the Office of Emergency Management. These include metrics to track the percentage of completion of and gauge effectiveness of the disaster recovery program.

Based on this, we consider this recommendation fully implemented.

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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 31, 2022

Technology Services added a training course focusing on disaster recovery awareness to Workday. Mandatory training is scheduled for those on the Technology Services’ Disaster Recovery Committee, and other select personnel who have a role in disaster recovery. The scope of who needs to take the course has been expanded to include all Technology Services staff who must take the training once every two years. In the future, Technology Services staff said they will decide how to include those outside the agency whose roles touch on disaster recovery to take the awareness training.

Additionally, Technology Services reviews training compliance once a month. We reviewed a Workday spreadsheet that showed staff compliance with completing the disaster recovery awareness training over 95% of staff have completed the course and have done so within the last two years.
**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.

**AGENCY ACTION**  
*Agency's original target date for completion: Dec. 31, 2021*

Information system contingency plans are procedures to recover each mission-critical information system and are typically developed by an information system's content owner. Information system contingency plan updates are conducted annually, and when major changes occur to the respective process. When major changes occur to processes, then a discussion is held on whether the information system contingency plans should be updated.

We found Technology Services documented the frequency of updating information system contingency plans in an official standard. We reviewed the information system contingency plan standard, which is the governing document for developing and updating city information system contingency plans. Technology Services has established an annual schedule to review all information system contingency plans and if processes materially change, to make updates to the plans as needed.

Based on these results, we consider this recommendation fully implemented.

**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.

**AGENCY ACTION**  
*Agency's original target date for completion: Dec. 31, 2022*

Technology Services has designated ServiceNow as the system of record, as we recommended, and is building out the business application service within ServiceNow to enter recovery metrics.

We reviewed screenshots of ServiceNow and found recovery metric fields have been entered in ServiceNow and are being tracked. For example, the
ServiceNow screenshots show that an information system contingency plan has been developed for each service’s disaster recovery planning efforts. Annually, the information system contingency plans are reviewed and updated, which includes reviewing and updating recovery processes and procedures. Because information system contingency plans are reviewed, tracked, and updated, recovery is also tracked to ensure plans are accurate and the processes will result in full recovery.

Because of this, we consider this recommendation fully implemented.

PARTIALLY IMPLEMENTED

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.

AGENCY ACTION

Agency’s original target date for completion: Dec. 31, 2021

Technology Services is collecting backup and restore standard metrics, which are considered critical for the agency’s technology operations. These backup and restore metrics are important to track because they demonstrate the failures and successes of the data that gets backed up. These results are then communicated monthly to the agency’s leadership so they can analyze performance trends and make informed decisions. Generally, these metrics are provided to the Disaster Recovery Committee’s reliability team. That team includes the highest levels of the executive team.

We reviewed the Disaster Recovery Committee reliability team’s presentation slide decks for the team’s first and second quarter 2023 meetings. The documentation shows that the metrics are shared with Technology Services’ leadership. The slide deck evidence indicates that backups are completing successfully 99-100% of the time.

However, while the backup statistics are being tracked and monitored, there is no documented and approved backup policy for directing the process to track and monitor results.

Because of this, we consider this recommendation partially implemented.
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.

201 West Colfax Avenue, #705

Denver, CO 80202

(720) 913-5000

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 and County of Denver. Our work is performed on behalf of everyone who cares about the city, including its residents, workers, and decision-makers.