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

June 7, 2024

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 Risk Management.

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 17, 2024. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
Technology Services lacks a citywide comprehensive information technology risk management program.

RECOMMENDATION 1.1 – Designate a responsible executive.

The city's Technology Services agency should designate a leader who is responsible for developing and implementing a comprehensive, citywide information technology risk assessment as part of a formal risk management program. To ensure this leader can effectively implement the program, Technology Services officials should empower this person to enhance the citywide information technology risk management policy as well as develop associated standards and procedures, as noted in Recommendation 1.2.

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	9/30/2024	Sumana Nallapati

Narrative for Recommendation 1.1
Technology Service (TS) Executive leadership and TS Project Management are actively developing a comprehensive technology risk management program in alignment with industry standards and best practices.

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

RECOMMENDATION 1.2 – Develop a citywide risk assessment process.

The city's Technology Services agency should establish and document a process for a comprehensive, citywide information technology risk assessment that includes the city's cultural facilities and independent agencies and that identifies all critical- and high-rated risks.

This risk assessment process should include:
• Working with and collecting risks from all agency and Technology Services staff who
are tasked with information technology risk management activities.
• Presenting those risks to executive leadership teams within Technology Services and individual city agencies.
• Creating a process to determine how to rank and respond to each risk.
• Defining roles and responsibilities — and any other pertinent and related policies and procedures — to identify and collect information technology risks, report them in a risk register, and escalate critical- and high-rated risks to Technology Services leaders.

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	6/30/2025	Sumana Nallapati

Narrative for Recommendation 1.2
TS intends to identify/assess/mitigate/monitor citywide technology risk holistically.

RECOMMENDATION 1.3 – Update Existing Policy

The city's Technology Services agency should update the information technology risk management policy to incorporate a comprehensive, citywide information technology risk assessment process.

At a minimum, this updated policy should address:
• Implementing a periodic, citywide information technology risk assessment.
• Documenting processes to identify, document, monitor, and resolve citywide information technology risks.
• Defining roles and responsibilities for all staff who perform information technology

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

risk management functions. • Requiring information technology risk management training for all employees.

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	12/31/2024	Sumana Nallapati

Narrative for Recommendation 1.3
All TS policies are reviewed/updated/approved by leadership on an annual basis.

RECOMMENDATION 1.4 – Create single source of record. The city's Technology Services agency should create a centralized system to serve as a single source of record in tracking and monitoring information technology risks as part of the comprehensive risk assessment called for in Recommendation 1.2. Technology Services should also continuously monitor and update this source of record — including with the status of remediation efforts — and periodically inform Technology Services executive leaders of progress throughout the year. At a minimum, this centralized system should contain all critical- and high-rated risks identified throughout the city during the comprehensive, citywide information technology risk assessment as well as any additional risks identified throughout the year.

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	6/30/2025	Sumana Nallapati

Narrative for Recommendation 1.4
TS has begun consolidating risks within a single source with the intention to mature into an enterprise solution.

RECOMMENDATION 1.5 – Develop risk management training. The city's Technology Services agency should develop a training program for employees tasked with information technology risk management. At a minimum, this training should cover defined roles and responsibilities and provide guidance on

documenting risks, communicating risks to leaders, and following up on a risk's mitigation status.		
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	6/30/2025	Sumana Nallapati

Narrative for Recommendation 1.5
TS intends to create a robust and holistic organizational risk management structure identifying roles, responsibilities, documentation, risk assumption, identification of training for necessary roles and escalation processes associated to technical risk.

RECOMMENDATION 1.6 – Create written information-exchange agreements.

In line with federal guidance, the city's Technology Services agency should take the following steps so it can realize a citywide understanding of potential threats and vulnerabilities to the city's networks and technology infrastructure:

1. Technology Services should work with the Mayor's Office and the City Attorney's Office to create information-exchange agreements between Technology Services and any independent agencies not required to comply with Executive Order No. 18. These agreements should establish a formal process to share information about critical- and high-rated technology risks, with clear roles and responsibilities for both parties. The agreements should include the information or data to be exchanged including the identified risks and a risk rating for each, any security and privacy requirements, and relevant controls.
2. If an independent agency does not agree to share risks through a signed information exchange agreement, then Technology Services should communicate this lack of cooperation to the mayor for them to determine timely next steps to gain the independent agency's cooperation.
3. If the mayor declines to act, then Technology Services should consider asking the City Council for support through a city ordinance that would bolster the city's ability to manage information technology risks. In that event, Technology Services should document its decision whether to seek support from the council.

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	6/30/2025	Sumana Nallapati

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

Narrative for Recommendation 1.6
TS agrees to pursue memorandum of understanding (MOU) with the independent agencies rather than agreements, although TS cannot require any agency to sign a MOU, nor can it require the Mayor or City Council to act. TS will reach out to independent agencies to determine their interest in pursuing a MOU by the identified target date. TS cannot commit to a completion date for any such efforts, or that a successful MOU will ever be reached.

RECOMMENDATION 1.7 – Enforce acceptable use agreements and cybersecurity awareness training.

In addition to ensuring cybersecurity awareness training is delivered to all required network users, the city's Technology Services agency should develop a communications and enforcement strategy to ensure citywide compliance in employees' signing of the acceptable use agreement and in their completing required quarterly cybersecurity training. To ensure this enforcement strategy is effective, Technology Services should:

1. Provide warning notices before each quarterly deadline to any users who have not yet
completed the assigned training.
2. Notify the users' managers of the incomplete training.
3. Escalate the names of any users who fail to complete the required trainings to their respective agency's executive leaders.
4. Include the citywide cybersecurity completion percentage as a metric in the annual performance evaluation for Technology Services leaders.

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	2/1/2025	Ashley Bolton

Narrative for Recommendation 1.7
TS is currently maturing our governance of User cybersecurity training completion and annual acknowledgement of the CCD Acceptable Use Agreement. TS recently partnered with the Berkeley Data Science Society to create better reporting and data visualization, including adding gamification elements to User cybersecurity completion. We look forward to incorporating these recommendations.

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

Please contact Tara Segura at Tara.Segura@denvergov.org with any questions.

Sincerely,

Sumana Nallapati
Chief Information Officer
Technology Services

cc: Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director
Peter Ulrich, Information System Audit Manager
Paul Kresser, Deputy Chief Information Officer
Ashley Bolton, Chief Data and Information Security Officer
Tara Segura, Data Protection Officer