Audit Team

Peter Ulrich, CISA, CSX-A, Information Systems Audit Manager
Nicholas Jimroglou, CISA, CDPSE, Information Systems Audit Lead
Rob Farol, CISA, CIA, CGAP, Information Systems Audit Senior
Dave Hancock, CISA, CISM, MURP, Information Systems Audit Senior

Other Contributors

Kristen M. Clark, Senior Communication and Reporting Specialist
Stelios Pavlou, Reporting Specialist
Jeff Neumann, Graphics and Visual Information Specialist

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 Blumenthal, 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 Ave. #705
Denver, CO 80202
(720) 913-5000

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

Response narratives are reprinted verbatim from the agency’s letter, which is available in full on our website.

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

June 20, 2024

We audited how the city's Technology Services agency handles information technology risks and how effectively it oversees a comprehensive risk assessment process to track and address information technology risks citywide. I now present the results of this audit.

The audit found Technology Services lacks several key components to effectively assess citywide information technology risks. Specifically, the policy and procedures for information technology risk management are incomplete, roles and responsibilities are not clearly defined, and no central system of record exists to track how city staff address information technology risks. Additionally, Technology Services is not fully using its authority to oversee all technology on the city's network, and it is not ensuring all city employees consistently complete mandatory cybersecurity awareness training to do their part in protecting city systems.

By implementing recommendations to strengthen policies, create procedures, provide training, and establish partnerships with independent agencies through information-exchange agreements, Technology Services will be better able to monitor and mitigate all information technology risks citywide.

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.” 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 appreciate the leaders and team members in Technology Services who shared their time and knowledge with us during the audit. Please contact me at 720-913-5000 with any questions.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
Objective

- To assess how well the city's information technology risk management program identifies, assesses, and addresses risk citywide.
- To determine whether the city's Technology Services agency has created necessary guidance for staff to understand their roles and responsibilities and sufficiently manage information technology risk.

Background

Managing information technology risk involves the City and County of Denver and its Technology Services agency identifying, assessing, and responding to potential threats and vulnerabilities.

A risk management program documents potential cyber threats, data breaches, system failures, and other hazards that threaten the confidentiality, integrity, and availability of systems and city services. With this information, leaders are empowered to address risk based on available resources.

Technology Services lacks a citywide comprehensive information technology risk management program

The city's Technology Services agency has no citywide comprehensive information technology risk management framework, and it lacks full cooperation from some agencies and city staff. This prevents Technology Services from having a complete understanding of potential risks and vulnerabilities across the city.

Although Technology Services assesses risks for most systems it directly manages, the agency does not have defined ways to work with agencies outside its control to ensure risks are identified, assessed, and responded to. Specifically, we found:

- No periodic, comprehensive, and citywide information technology risk assessment and no authorization for a citywide risk management executive to take the lead.
- No comprehensive, citywide information technology risk management policy or specific procedures.
- No documented roles and responsibilities — or training program — for Technology Services' agency relationship managers and other staff responsible for information technology risk management.
- No source of record to assess and monitor information technology risks.
- No partnerships with independent agencies to share data about potential risks.
- Inconsistent completion of mandatory cybersecurity awareness training across city agencies.

WHY THIS MATTERS

In 2021, Denver's mayor authorized Technology Services to manage all technology that operates on or connects to the city's network. But disputes with some agencies about Technology Services' authority over their connected subnetworks limits Technology Services' ability to identify all potential risks.

Without a comprehensive, citywide information technology risk management framework, Technology Services officials cannot have the full knowledge they need to deploy available resources in the most effective manner and respond appropriately to technology threats citywide.
Technology Services lacks a citywide comprehensive information technology risk management program

Technology Services does not have a comprehensive, citywide information technology risk management program.

Because of questions on how effectively Technology Services can exercise its authority over the city's technology infrastructure, it cannot comprehensively assess risks citywide.

City employees are not consistently completing mandatory cybersecurity awareness training.
The importance of managing information technology risks

The City and County of Denver relies on information technology systems to carry out its mission and operations — including the various services it provides residents, local business owners, and other community members. Some of these systems are accessed directly by the public, while other systems are used internally to enable effective and efficient city operations.

Protecting the confidentiality, integrity, and availability of information in these systems, as well as respecting the public's privacy, is paramount to managing risk. Risk comes in various forms including from human error, mismanagement, and cyberattacks. Most external cyberattacks are committed by malicious individuals or criminal organizations, who can be sophisticated and well-organized.

When successful, attacks can cause serious or catastrophic damage to city operations and assets — as well as individuals who rely on city services, city agencies and employees, or third-party vendors that contract with the city. Consequences can include equipment failures, operational disruptions, unauthorized access to city systems and data, and potentially millions of dollars in costs and other damages.

Because of the gravity of these potential outcomes, the City and County of Denver must stay vigilant and staff at all levels of city government must:

- Understand their responsibilities in using city information technology resources.
- Be accountable for helping to manage risk.
- Do their part to protect the city’s information technology.

Risk management is vital to having a resilient information technology infrastructure, ensuring regulatory compliance, and safeguarding sensitive information. When an organization systematically evaluates and manages information technology risks, it can enhance its ability to adapt to a rapidly evolving technological landscape while safeguarding digital systems and assets and ensuring continuity in operations.

Information technology risk management, specifically, is a comprehensive approach all organizations — including city governments — use to identify, assess, and appropriately address potential threats and vulnerabilities associated with information technology systems. As shown in Figure 1 on the next page, this formal process involves analyzing and choosing how to respond to potential risks including cyber threats, data breaches, system failures, and other hazards that threaten the confidentiality, integrity, and availability of critical information assets and services.
Effective information technology risk management requires developed strategies, policies, and procedures to proactively address identified risks using robust controls and safeguards.

Technology Services and its role in the city

Technology Services is the city agency responsible for the city's information technology infrastructure, systems, and services. It provides these resources to most city agencies and is responsible for protecting technology and data while maintaining continuous technology operations.

The mayor’s Executive Order No. 18 grants Technology Services the authority to oversee these various systems and services. An update to the executive order in 2021 specifically increased Technology Services' ability to manage, monitor, and protect technology across the city.

As with all executive orders, Executive Order No. 18 applies to city agencies under the mayor — but not independent agencies, like the City Council — and it remains in effect until a mayor withdraws it. Because of this limited reach, maintaining collaborative partnerships with other city agencies is critical to ensuring Technology Services knows about all information technology risks that may pose a threat to the city.

Although the updated executive order has been in place for more than three years, some city agencies still foster a culture that excludes Technology Services' involvement.

EXECUTIVE ORDER NO. 18

Executive Order No. 18 was revised in January 2021 to further clarify the mission, role, and authority of Technology Services. The order granted the city agency the power to manage all physical and virtual technology that connects to the city's network — which are the hardware and software that support the city's digital infrastructure and services.

---


2. 
This has created persistent challenges for Technology Services, which we have noted in prior audits. For example, in the “City Council Operations” audit published in December 2023, we reported how some council operations were exposing the city to risks because of council members’ reluctance to partner with Technology Services.²

### A risk management framework

The National Institute of Standards and Technology — a laboratory and nonregulatory federal agency within the U.S. Department of Commerce that publishes best practices for information technology — developed a risk management framework that provides organizations with the fundamentals to manage information technology risks.

By using this framework, organizations can proactively and regularly identify information technology risks and manage them before they become a problem. This tool also helps executive leaders consciously make informed decisions about how best to resolve information technology risks using available resources. The risk management framework consists of seven elements that are critical in the risk management process, as shown in Figure 2.

#### FIGURE 2. The risk management framework

- **Prepare**: Essential activities to prepare the organization to manage security and privacy risks.
- **Categorize**: The system and information processed, stored, and transmitted based on an impact analysis.
- **Select**: The set of controls to protect the system based on risk assessments.
- **Implement**: The controls and document how controls are deployed.
- **Authorize**: Senior official makes a risk-based decision to authorize the system to operate.
- **Monitor**: Continuously monitor control implementation and risks to the system.
- **Assess**: To determine whether the controls are in place, operating as intended, and producing the desired results.

*Source: Created by Auditor’s Office staff using information from the National Institute of Standards and Technology.*

Managing information technology risks

Once executive leaders of an organization are informed of a risk, they must decide how to respond. They can mitigate, transfer, avoid, or accept the risk. Each choice comes with its own implications.

- **Mitigating** the risk is typically the best choice as it reduces the likelihood and impact of a potential threat. This can involve implementing security controls such as risk assessments, asset management controls, system configurations, and patches to fortify vulnerable systems.

- **Transferring** the risk shifts the responsibility to someone else, usually a third party. This does not eliminate the risk, but it is still a viable choice depending on the situation. For example, because all organizations are vulnerable to a cyberattack, an organization can purchase cybersecurity insurance that would compensate the organization if an attack were to occur — essentially transferring the financial risk to an insurance provider.

- **Avoiding** the risk eliminates the problem by stopping the risky operation from functioning. For example, if a software application or server is outdated and no longer supported, it might be vulnerable to cyberattacks. Executive leaders can choose to avoid this risk by no longer using the application or server, which removes the risk entirely.

- **Accepting** the risk could leave an organization susceptible to the greatest consequences. This involves executive leaders acknowledging the threat exists but choosing not to take any action — leaving the organization vulnerable. This choice is the least effective option, but it may also be the only viable one when budget or time constraints are a factor.

**WHAT ‘MITIGATION’ MEANS**

Within information technology, “mitigation” has a specific, technical meaning. When an organization mitigates a risk, it means the organization has either reduced the risk significantly or completely removed it by implementing control activities.
FINDING AND RECOMMENDATIONS

Technology Services lacks a citywide comprehensive information technology risk management program

The city’s Technology Services agency does not have a comprehensive, citywide information technology risk management program that captures and manages all information technology risks throughout the city.

Technology Services officials said they approach risk at both the organization and system levels. But we found instances where agencies outside Technology Services’ purview do not communicate their information technology risks to Technology Services leaders.

Several agencies also said they do not have a formal risk management process between their agency and Technology Services, and some agency relationship managers within Technology Services were unaware of their responsibility to inform Technology Services leaders of potential risks. Instead, knowledge of other agencies’ information technology risks is kept within those agencies — excluding Technology Services’ involvement.

A RECURRING RISK – One contributing factor underlying this finding is Technology Services’ ability and willingness to enforce information technology policy across all agencies on the city’s network.

Although Technology Services’ authority expanded in 2021 after the mayor updated Executive Order No. 18, several of our office’s audits since then have reported on the same significant risk. Some agencies resist Technology Services’ authority and partnership, and Technology Services leaders face challenges in exercising the agency’s authority over the entire city on matters related to information technology. Specifically, we reported these issues in the following audits:

- “Information Technology Disaster Recovery” in May 2021.
- “Citywide Information Technology Purchases” in April 2023.

THE CITY’S RISK MANAGEMENT PROCESS

Technology Services has a proactive approach to identify and manage information technology risks within its own agency and some other city agencies.

This process is informal, ranging from executive leader presentations to discussions between staff and their supervisors. But we found this does not ensure information technology risks are fully communicated to leadership.
According to Technology Services executive leaders, Executive Order No. 18 is intended to promote a collaborative partnership between Technology Services and other city agencies. Instead, some agencies continue to work in silos and do not recognize the importance of Technology Services’ duty to protect technology and data citywide. Technology Services continues to make concerted efforts to build these partnerships with agencies citywide, but obstacles remain a recurring theme — and this audit is no different.

As a result, Technology Services has not established a formal, comprehensive information technology risk management program that captures all of city government. Because of this, Technology Services executive leaders are not fully informed of all information technology risks — and therefore, they lack the context needed to make informed decisions and allocate available resources to respond to identified risks.

We also found Technology Services’ existing risk management policy does not reflect a comprehensive, citywide program. The policy does not address the roles and responsibilities of Technology Services’ agency relationship managers or other employees tasked with risk management activities, nor does it ensure sufficient training and guidance for those employees to do their work.

Meanwhile, staff citywide are not consistently completing mandatory cybersecurity awareness trainings each quarter. Until this issue in particular is addressed, the city is at greater risk of a cyberattack that could cost the city millions of dollars, expose the city’s and residents’ private or sensitive data, and waste time and resources to repair the damage from such an event. For example, using data from 2018, Technology Services estimates that a cyberattack resulting in a citywide shutdown could cost the city up to $5.3 million a day.

Technology Services does not have a comprehensive, citywide information technology risk management program

We found Technology Services’ processes focus exclusively on assessing system-level risks rather than addressing information technology risk management in a formal and comprehensive way citywide. The following elements are missing:

- A periodic, citywide information technology risk assessment and documented procedures for it.
- A comprehensive policy to guide a citywide information technology risk management program.
- Documented roles and responsibilities for Technology Services’ agency relationship managers and other employees tasked with risk management activities.
- A single source of record for documenting citywide information technology risks.
- Formal and comprehensive training for agency relationship managers and other employees involved with citywide information technology risk management.
Without a complete citywide information technology risk management program, the Technology Services staff who are responsible for risk management will not be sufficiently prepared to identify and mitigate information technology risks in a timely manner.

Technology Services leaders have not prioritized establishing a robust information technology risk management program, which exposes the city to several vulnerabilities. For instance:

- They have an incomplete view of potential risks across the city.
- They may not properly allocate available resources to mitigate known risks.
- They may not sufficiently monitor whether risks are adequately resolved.
- They will not have assurance that other city agencies are prioritizing or sharing information about risks with Technology Services to reduce or remove potential threats and vulnerabilities to the city.

**Technology Services does not conduct a periodic, citywide information technology risk assessment and has no authorized role to lead assessments**

Managing information technology risks requires participation from every agency and employee — from senior leaders who provide the strategic vision and top-level goals and objectives for the organization; to mid-level leaders who plan, execute, and manage projects; to individual staff who develop, operate, and maintain the systems that support various city services and functions.³

We identified two reasons why Technology Services leaders have not developed a citywide information technology risk assessment:

1. Technology Services has not designated an executive responsible for developing, implementing, and supervising a citywide assessment. Leading practices say organizations should delegate responsibility for a comprehensive information technology risk assessment to a senior-level official to ensure the information technology risk assessment is effective and complete.⁴

We looked at three cities comparable to Denver — Seattle; San Francisco; and Portland, Oregon — to understand their practices for information technology risk management. We found all three cities had designated executives responsible for periodic risk assessments.

---


2. Technology Services cannot assess risk from a citywide perspective because it does not have visibility into some systems and subnetworks. For example, Denver County Court and the city’s cultural facilities — like the art museum and the zoo — do not formally share information technology risks with Technology Services because their systems, called “subnetworks,” operate separately from most of the city even though they are, in fact, connected to the city’s network.

Federal guidelines say organizations should collect risks from across the organization, determine the likelihood and impact of risks, document the risks into a single source of record, and communicate the results of a risk assessment with the organization to allow leaders to deploy resources based on the most critical risks. Further, the guidelines recommend that organizations implement a ranking system based on organizational culture — categories such as very low, low, moderate, high, and very high are an example — which supports the communication of risks to all employees and leaders alike.

All three other cities we looked at had developed a comprehensive, citywide information technology risk assessment program. For example, the City and County of San Francisco conducts annual maturity assessments of its agencies. First, the agencies complete a risk and vulnerability self-assessment, then the city follows up with the agencies to verify their self-assessments are accurate.

By Denver not having a designated leader to ensure risk assessments are done regularly and not having access to all agencies connected to the city’s network, Technology Services may not have a complete view of potential citywide risks to its information technology infrastructure. Because of that, Technology Services leaders and agency managers across the city lack the full knowledge and insight they need to properly deploy available resources to protect the city from vulnerabilities.

### 1.1 RECOMMENDATION

**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

---

5 National Institute of Standards and Technology, Special Publication 800-53, Section RA-3.

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.

**AGENCY RESPONSE – AGREE**

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

**IMPLEMENTATION EXPECTED BY SEPT. 30, 2024**

<table>
<thead>
<tr>
<th>1.2</th>
<th>RECOMMENDATION</th>
<th>Develop a citywide risk assessment process</th>
</tr>
</thead>
</table>

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.

This process should complement the updated information technology risk management policy called for in Recommendation 1.3.

**AGENCY RESPONSE – AGREE**

TS intends to identify/assess/mitigate/monitor citywide technology risk holistically.

— Technology Services

**IMPLEMENTATION EXPECTED BY JUNE 30, 2025**
The city’s information technology risk management policy is incomplete, and no associated procedures exist to guide a regular citywide risk assessment

In 2021, Technology Services leaders developed the city’s information technology risk management policy to manage risk; assess all city data, hardware, and software assets; and protect those from misuse, threat, and loss of data. But the policy focuses exclusively on assessing system-level risks — not on assessing risks across all city agencies. In addition, there are no procedures to guide employees in performing either the system-level risk assessments or a comprehensive, citywide assessment.

For example, Technology Services developed policies specifically to identify system-level risks for the agency’s vulnerability management and asset life cycle management processes. While these policies are meant to identify risks within systems across the city, they are limited. Technology Services leaders said they cannot identify risks outside what they can see within the network. Vulnerabilities and asset life cycle risks for agencies like Denver County Court, the Denver District Attorney’s Office, and the city’s cultural facilities are beyond the scope of these processes because Technology Services has no visibility into those agencies’ subnetworks.

The city’s risk assessment policy lacks key elements of the National Institute for Standards and Technology’s risk management framework — which provides guidance to ensure a robust information technology risk management program. Specifically, Denver’s policy is missing requirements and guidance for:

- A periodic, comprehensive, and citywide information technology risk assessment.
- Authorization for a citywide risk executive to lead risk management activities.
- A single source of record to track information technology risks.
- Training and procedures on information technology risk management.

Federal guidelines recommend organizations develop a policy and detailed procedures to communicate the purpose, scope, roles, and responsibilities of an information technology risk management program. These documents should express management’s commitment and describe the coordination and collaboration expected among agencies. The policy and procedures should also enable leaders to implement the risk assessment policy and any associated controls developed to respond to identified risks.

---


Technology Services lacks a well-defined policy and set of procedures that define the formal roles and responsibilities for employees responsible for risk management. While Technology Services has not formally defined the employees who are responsible for identifying citywide information technology risks, agency leaders have designated agency relationship managers and executive leaders as points of contact to funnel and communicate risks to Technology Services for review.⁹

Absent formalized or documented roles and responsibilities, employees tasked with risk management activities have no consistent instruction on when and how to communicate agency risks to a centralized system. By not having a comprehensive policy and associated procedures, as well as lacking documented roles and responsibilities for staff to perform, Technology Services has not prioritized a comprehensive, citywide information technology risk assessment. In addition, these gaps leave the city vulnerable because staff are not equipped with the tools to identify and manage risk — which weakens their ability to protect the city and potentially prevent attacks of critical operations, essential services, and city data.¹⁰

<table>
<thead>
<tr>
<th>1.3</th>
<th>RECOMMENDATION</th>
<th>Update existing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implementing a periodic, citywide information technology risk assessment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Documenting processes to identify, document, monitor, and resolve citywide information technology risks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Defining roles and responsibilities for all staff who perform information technology risk management functions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Requiring information technology risk management training for all employees involved in managing information technology risks.</td>
<td></td>
</tr>
</tbody>
</table>

⁹ “Agency relationship managers” are tasked with understanding the demands and risks at each of the agencies.

Technology Services has no single source of record to document citywide information technology risks

In addition to Technology Services lacking a comprehensive, citywide information technology risk management program, the agency has no centralized system to track and monitor whether identified citywide risks have been sufficiently addressed.

Instead, agencies’ directors and managers track their information technology risks using various processes. For example, absent any comprehensive agencywide tool, divisions within Technology Services focused on software management, hardware management, and life cycle management have created their own risk registers to track potential threats and vulnerabilities.

Not having a single source of record for all citywide information technology risks creates its own set of problems. For example, information on identified risks and how well they have been addressed is fragmented across the city — leaving Technology Services leaders without a clear understanding of the full risks and whether they have been dealt with appropriately. Technology Services also cannot ensure available resources are effectively disbursed to the highest risk areas citywide, nor can leaders effectively monitor risks to protect the city and maintain technology operations.

Federal guidelines emphasize the need for organizations to have a centralized way to track and monitor all information technology risks as part of a comprehensive risk management program.\textsuperscript{11} An ideal record-keeping system would include information about how risks were identified, what activities or action plans are planned to address the risk, and associated timelines. Also documented should be the names of the staff responsible for the source of record to ensure executive leaders are kept informed of efforts to protect the organization.

1.4 RECOMMENDATION Create a 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.

AGENCY RESPONSE – AGREE

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

— Technology Services

IMPLEMENTATION EXPECTED BY JUNE 30, 2025

Technology Services offers no specific training for staff responsible for citywide information technology risk management

We learned through interviews and a staff survey that, in addition to Technology Services’ lack of a comprehensive and citywide risk management program, no information technology risk management training exists for agency relationship managers and other employees with related responsibilities. This lack of training leaves these employees without a clear, consistent understanding of their roles and responsibilities in managing citywide risks.

An established training program would include lessons on:

- The roles and responsibilities involved with identifying and collecting data about information technology risks.
- How to document risks in a centralized system.
- How to escalate critical- and high-rated risks to agency and Technology Services leaders.

Although we were told no comprehensive training like this exists, we sought to learn how well agency relationship managers and other Technology Services employees understand their roles and responsibilities in information technology risk management.
We surveyed 36 agency relationship managers and Technology Services directors and received responses from 18, for a response rate of 50%. Among those who responded, 13 — or 72% — reported they did not receive formal training on their roles and responsibilities related to information technology risk management.

Additionally, through interviews, we learned Technology Services' agency relationship managers for Denver County Court and the city's cultural facilities were not aware that they should be compiling data about information technology risks from their assigned agencies. Through our survey, we concluded these staff could collect this detail if they had had proper direction and guidance.

Federal guidance on risk management training says the organization is responsible for providing role-specific training to staff involved with the risk management program. This training should provide the knowledge necessary for individuals to fulfill their responsibilities in performing periodic risk assessments within the organization. Comprehensive, role-specific training should always address roles and responsibilities for managers as well as operational and technical staff.\(^\text{12}\)

As of April 2024, Technology Services had not prioritized — and therefore, not developed — an information technology risk management training program that includes clear roles and responsibilities for agency relationship managers and other employees tasked with managing information technology risks.

Without sufficient training, employees may not be fully aware of their duties to identify risks and protect city systems and sensitive data and they may not know how to escalate information technology risks to appropriate leaders. Risks may go unidentified, or known risks may not be resolved.

### 1.5 Recommendation

**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.

**Agency Response – Agree**

---

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.

— Technology Services

IMPLEMENTATION EXPECTED BY JUNE 30, 2025

Because of questions on how effectively Technology Services can exercise its authority over the city's technology infrastructure, it cannot comprehensively assess risks citywide

Even if Technology Services takes the necessary steps to establish a comprehensive information technology risk management program for the city technology under its control, the agency does not have a full citywide understanding of information technology risks because some independent agencies are reluctant to cooperate.

In 2021, Mayor Michael B. Hancock signed an update to Executive Order No. 18 that empowered Technology Services with the authority to manage technology for “all agencies, departments, divisions and other governmental instrumentalities ... that operate on the city's Network.”

As discussed, while most city agencies operate on the city’s network, some agencies use their own subnetworks that still connect to the city’s network. A “subnetwork” is a smaller network inside a larger one and it works to segment these smaller networks from one another. Within the City and County of Denver, publicly owned entities like Denver International Airport and several independent agencies — such as Denver County Court, the Denver Public Library, and the city’s cultural facilities — use subnetworks.

Therefore, this remains a gray area open to conflicting interpretations because — as we noted in our 2023 audit of citywide information technology purchases — no documented definition exists to clarify what city entities are considered “on the Network.” As part of that audit, Technology Services agreed with our recommendation that it change its policies and procedures to define what “on the Network” means. We have not yet formally followed up on that audit to assess implementation of that recommendation, but during our work on this audit, we saw no evidence that the meaning of “on the Network” had been clarified.

Technology Services staff told us some independent agencies argue that Executive Order No. 18 does not apply to their agencies. These agencies assert they:


• **MANAGE THEIR OWN SUBNETWORKS WITHIN THE CITY’S NETWORK** – For example, the Denver Public Library operates its technology independently of Technology Services. Because of this, the library asserts that Technology Services has no decision-making authority over the library's technology decisions.

• **DO NOT REPORT TO THE MAYOR** – For example, the City Council is independently elected and, therefore, reports to the residents of Denver, not the mayor. As the legislative branch of city government, council members say the Mayor’s Office — the executive branch of government — does not have the authority to enforce executive orders on the council as it does with other agencies under the mayor's purview.¹⁵

• **HAVE LEGAL AUTHORITY TO OPERATE SEPARATELY** – For example, Denver County Court officials assert they have legal authority to operate independently as the separate, judicial branch of city and county government. Court officials cite Article III of the Colorado Constitution, which says the powers of the executive, legislative, and executive branches are to remain separate.¹⁶

Denver County Court and some other agencies claim they are not required to communicate in any formal way with Technology Services about information technology risks, nor do officials in those agencies believe they must share information about ongoing risks.

But this assertion of independence with limited collaboration undermines the greater good of protecting the city from costly and damaging cyberattacks and other information technology risks that could tarnish the city's reputation, risk sensitive and confidential data being stolen or exposed, and cost the city millions in time and resources to repair damage that might have been prevented with a functioning comprehensive citywide risk assessment program. As we mentioned, Technology Services — using data from 2018 — estimates that a cyberattack resulting in a citywide shutdown could cost the city up to $5.3 million a day.

The Center for Information Security — an independent, nonprofit dedicated to safeguarding governments and businesses through best practices against pervasive cyber threats — says establishing, maintaining, and communicating a regularly updated information technology risk assessment is critical to the security of organizations and their networks.¹⁷

When agencies do not regularly identify and communicate risks, leaders cannot determine the best ways to manage risks that threaten the network.

---


¹⁶ Colorado Constitution, Article III (1876).

Meanwhile, the National Institute of Standards and Technology says, “Managing information technology risks requires every member of the organization, from the senior leader developing strategies and business goals to the individual analyst who keeps systems running.”

As Figure 3 demonstrates, without each level of the organization communicating about risks, the organization as a whole cannot fully comprehend how risks affect the organization nor how each level can help the other manage risks across the organization.

**FIGURE 3.** Citywide comprehensive risk management approach

In comparison to Denver, the peer cities we researched — Seattle; San Francisco; and Portland, Oregon — were quick to note how important communication and information sharing are to managing their information technology risks. In the City and County of San Francisco, the city's 50 department information security officers communicate information technology risks regularly to the city's audit team. The officers collect the risks throughout the year and communicate those to audit leaders in a timely manner.

In Portland, the city's chief information security officer discusses all items on the city's risk register with city divisions each month. Further, the City of Portland’s risk management leaders use the risk register to track risks and monitor the risk mitigation process until the responsible division appropriately addresses the identified risk.

---

While the answers to Denver’s questions about what systems are “on the Network” remain contentious, the city’s main network and any subnetworks must still operate safely to serve residents and safeguard city services, operations, and sensitive data. Leading practices from the federal government offer a viable solution to ensure Denver’s city agencies can work together effectively for the good of the city, regardless of an agency’s status as an independent authority.

Guidance from the National Institute of Standards and Technology acknowledges that not all agencies within an organization have the same reporting structure. This federal guidance says that when two agencies operate independently within the same organization, both have the responsibility to agree to information-exchange agreements that ensure the agencies share information on known risks and data. These kinds of agreements are intended to:

- Enable exchanges of data, information, and understanding about technology risks.
- Provide a platform for separate agencies to agree on the extent of risks shared; security and privacy requirements, controls, and responsibilities for each system; and the impact level of the data or information shared.

Until defined agreements exist to share risks across all “governmental instrumentalities” within the City and County of Denver as specified in Executive Order No. 18, Technology Services may not completely fulfill its responsibility to protect the city’s technology infrastructure. More specifically, this means the agency cannot effectively deploy available resources to manage risks that exist across all city systems and any associated subnetworks connected to the city’s network.

Furthermore, Technology Services cannot safeguard the city’s technology infrastructure on its own. Having a complete, citywide view requires support and partnership from independent agencies and other entities with access to the city’s network. If all agencies do not work together to identify and manage potential risks and deploy resources based on the most critical- or high-rated risks, the city may be more vulnerable to a major cybersecurity incident.

### 1.6 RECOMMENDATION

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.

AGENCY RESPONSE – AGREE

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.

— Technology Services

IMPLEMENTATION EXPECTED BY JUNE 30, 2025
Figure 4 shows the 10,167 individuals who were given cybersecurity training in the fourth quarter of 2023. While 8,716 individuals, or 86%, completed the training, 1,451 individuals, or 14%, did not. In addition, 730 of the individuals who did not complete the quarterly cybersecurity training also did not sign an acceptable use agreement, which is about 7.2%.

![Figure 4. Citywide completion rate for cybersecurity training in fourth quarter 2023](image)

**Source:** Created by Auditor's Office staff based on Technology Services data.

By not completing ongoing training and by not signing the acceptable use agreement, these individual users of city technology are not held accountable for their actions if they were to misuse taxpayer-funded technology resources. They also will not have been properly educated on cybersecurity risks and how their action — or inaction — in defending against those risks may harm the city.

This is not the first time we have identified this lack of consistent cybersecurity training among city employees. Our “Phishing” audit report from April 2021 noted that training was not being delivered to key employees.20

Among Technology Services’ recent data, we looked at the 10 agencies that had the greatest failure in completing the cybersecurity awareness trainings and the 10 agencies with the most unsigned acceptable use agreements.

---

As shown in Figure 5, we found overlap across four agencies, which collectively have about 3,200 employees. Because of the information security sensitivities involved, we have separately communicated the names of these four agencies to Technology Services.

**FIGURE 5.** Agencies with highest rates of noncompliance

<table>
<thead>
<tr>
<th>AGENCY</th>
<th>DID NOT COMPLETE CYBERSECURITY TRAINING</th>
<th>DID NOT SIGN ACCEPTABLE USE AGREEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency 1</td>
<td>59%</td>
<td>50%</td>
</tr>
<tr>
<td>Agency 2</td>
<td>42%</td>
<td>50%</td>
</tr>
<tr>
<td>Agency 3</td>
<td>29%</td>
<td>44%</td>
</tr>
<tr>
<td>Agency 4</td>
<td>24%</td>
<td>29%</td>
</tr>
</tbody>
</table>

*Source: Created by Auditor’s Office staff using Technology Services data.*

Cybersecurity training is integral to the city’s defense against cyberattacks and its ability to manage information technology risk. The Center for Internet Security says proper training can reduce the risk of cybersecurity attacks on an organization.  

As mentioned, Technology Services estimates that — based on data from 2018 — a cyberattack resulting in a citywide shutdown could cost the city up to $5.3 million a day. While Technology Services has defenses to prevent cyberattacks and fortify vulnerabilities to the city’s network, no defense is foolproof and multiple layers help lower the risk of a successful attack. Staff training is critical to preventing a successful cyberattack.

### 1.7 RECOMMENDATION

**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.

AGENCY RESPONSE – AGREE

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

IMPLEMENTATION EXPECTED BY FEB. 1, 2025
OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

• To assess how well the city’s information technology risk management program identifies, assesses, and addresses risk citywide.
• To determine whether the city’s Technology Services agency has created necessary guidance for staff to understand their roles and responsibilities and sufficiently manage information technology risk.

Scope

We assessed how well the city’s Technology Services agency maintains a risk management life cycle. This included assessing the city’s compliance with its own risk management policy and comparing Technology Services’ efforts with industry frameworks, leading practices, and peer cities. We reviewed Technology Services’ and the city’s data, processes, and future planning efforts from Jan. 1, 2022, through Dec. 31, 2023.

Methodology

We used several methods to gather and analyze information related to the audit objectives. These included:

• Researching leading practices and reviewing city regulations including the city’s annual budgets, the mayor’s Executive Order No. 18 and No. 143, and Technology Services’ risk management policy.
• Interviewing key Technology Services staff and obtaining documentation about the information technology risk management life cycle and the existence of any comprehensive information technology risk assessments.
• Reviewing and assessing Technology Services’ policies and procedures for information technology risk management life cycle activities and for gaps when compared to the National Institute of Standards and Technology’s risk management framework.
• Determining whether managers have documented, approved, and communicated sufficient policies, procedures, and standards to relevant employees.
• Comparing Denver with other comparable cities — namely, Seattle; San Francisco; and Portland, Oregon — and identifying best practices within each city’s comprehensive information technology risk assessment process.
• Developing a survey of Technology Services’ directors and agency relationship managers to:
  ▪ Determine the various processes being used to monitor and track agencies’ risks.
  ▪ Assess these employees’ understanding of their roles and responsibilities in collecting, managing, and reporting information technology risks to executive leaders.
  ▪ Assess the training developed for employees to understand their roles within the information technology risk management process.
• Reviewing data on cybersecurity awareness trainings from 2022 through 2023 to determine the
completion rate for the city and to identify which agencies did not complete the trainings.

- Obtaining a list of which employees signed the city’s acceptable use agreement and comparing that list to those who completed cybersecurity training in 2023.
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.