September 15, 2022

We audited how the city's Technology Services agency handles vendor management to assess how effectively it oversees its information technology vendors, monitors their performance, and has established policies, procedures, and other processes it follows to ensure good governance. I now present the results of this audit.

The audit revealed Technology Services has no comprehensive structure for vendor management. The agency has an incomplete strategy and lacks several key components of effective governance — including detailed and approved policies and procedures; defined roles and responsibilities; and plans for staffing, budget, and training. Because of this, the agency does not effectively monitor its vendors to ensure they have safeguards to secure city data and that they provide services as they are contractually required. Technology Services is also not holding these vendors accountable when they fail to meet contractually required objectives, and the agency does not track when vendors stop working for the city. Additionally, we found Technology Services' data for vendor management is decentralized.

By implementing recommendations for a stronger vendor management governance structure, Technology Services will be better equipped to effectively manage and monitor the city's information technology vendors and hold them accountable to providing the services they were hired for.

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

[Signature]

Timothy M. O’Brien, CPA
Auditor
REPORT HIGHLIGHTS

Technology Services Does Not Systematically Manage Its Vendors

The agency's oversight of its information technology vendors is inadequate. Agency leaders delayed finalizing a proposed vendor management policy — a crucial component of a comprehensive governance structure — until after this audit was completed.

Specifically, Technology Services is missing:

- Official policies and procedures to guide its employees, enforce requirements, and hold vendors accountable.
- Defined roles and responsibilities or designated authority for the specific employees involved with vendor management.
- Budgetary plans to fund and adequately staff the vendor management function.
- Training plans to educate employees about how to monitor vendors in line with approved policy.

Meanwhile, we also found Technology Services does not:

- Consistently monitor its vendors for existing security controls.
- Hold these vendors accountable for meeting contract requirements.
- Have a consistent process when vendors stop working for the city.
- Store vendors' data in a central system.

WHY THIS MATTERS

Technology Services' delay in establishing a comprehensive governance structure risks the city not getting what it pays for from outside vendors. If technology vendors do not adequately protect city data or if they do not deliver services as promised, city agencies and residents could be affected and the city's reputation is at risk.
## 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>7</td>
</tr>
<tr>
<td>Technology Services Does Not Systematically Manage Its Vendors</td>
<td></td>
</tr>
<tr>
<td>Technology Services Has an Incomplete Strategy and No Action Plan to</td>
<td>8</td>
</tr>
<tr>
<td>Implement Vendor Management</td>
<td></td>
</tr>
<tr>
<td>Technology Services Stores Vendor Management Data across Multiple</td>
<td>19</td>
</tr>
<tr>
<td>Systems</td>
<td></td>
</tr>
<tr>
<td><strong>AGENCY RESPONSE TO AUDIT RECOMMENDATIONS</strong></td>
<td>21</td>
</tr>
<tr>
<td><strong>OBJECTIVE, SCOPE, AND METHODOLOGY</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>APPENDIX</strong></td>
<td>26</td>
</tr>
<tr>
<td>Sampling Methodology</td>
<td>26</td>
</tr>
</tbody>
</table>
BACKGROUND

Vendor Management

With continual advances in information technology, both the public and private sectors are relying more on web applications and data that outside vendors provide via the internet. Globally, spending on such cloud-based services is forecast to grow by over 20% this year. The popularity of hybrid and remote work has helped fuel organizations' investments in third-party vendors as they seek ways for their employees to access work online.¹

What used to be a transactional relationship with a supplier is now often a close ongoing partnership spanning multiple years and millions of dollars. And because vendors now offer more than just goods — such as online services for payroll and software development — there is a greater need for organizations to monitor these ongoing partnerships through effective vendor management practices. In this way, organizations can control costs, provide better service, and reduce risks to ensure the organization gets the best value from its vendors.²

The City and County of Denver, like other organizations, can avoid problems by proactively overseeing its third-party vendors. This approach, called “vendor management,” becomes more important as vendors play increasingly more critical roles for businesses and governments.

As shown in Figure 1, vendor management guides organizations, like the city, in vetting what technology solutions they need, choosing which vendors are most qualified to provide those services, and monitoring those vendors to ensure they provide services in line with their contract terms.

---

FIGURE 1. The Vendor Management Process

![Vendor Management Process Diagram]

Source: Created by Auditor's Office staff.

---


CliftonLarsonAllen LLP, an audit and consulting firm, advises that information technology organizations should oversee their vendors through the entire vendor management process — that is, from selecting and contracting with a vendor, continuously monitoring the vendor’s performance against contracted terms, and then finally, ending the relationship.¹

- Vendor selection includes activities such as vetting ideas and technology against existing security and data protection risks and signing a contract with the best possible technology provider.
- Continuous monitoring includes activities such as reviewing for expiration dates and assessing the vendor’s performance against contract terms including service-level objectives, security, and insurance requirements.
- Ending a relationship requires activities such as notifying all stakeholders, returning or destroying data, and removing all vendor access to city systems.


⁴ Exec. Order No. 18, City and County of Denver (2021).
and cybersecurity needs of all agencies, departments, and divisions of the city.”

Four tenets make up the agency’s overall strategy:

- **RELIABILITY** – ensuring technology works as expected.
- **INNOVATION** – ensuring technology improves operational performance.
- **ACCESS** – ensuring technology connects city agencies and Denver residents to information and services.
- **PARTNERSHIP** – ensuring the agency has forward-thinking collaboration with city agencies and Denver residents.

Technology Services’ 2021 strategic plan speaks to the significance of vendor management. It says the goal is to “provide appropriate and consistent performance, reliability, confidentiality, and cost of Technology and to provide governance and deliberative process for consistent review of Technology.”

**STRUCTURE** – Technology Services’ chief information officer is responsible for “the overall strategy, policy direction, and management of the entire agency.” As shown in Figure 2, the chief information officer oversees six divisions.

---

**FIGURE 2. Technology Services Organizational Chart**

![Organizational Chart](Image)

*Source:* Created by Auditor’s Office staff based on information from the mayor’s proposed 2022 budget.

---

₅ Exec. Order No. 18, City and County of Denver (2021).
₇ City and County of Denver, “Mayor’s Proposed 2022 Budget.”
These include:

- **THE OPERATIONS TEAM** – which engineers and maintains the city’s technology infrastructure, data storage, and networks.

- **DENVER MARKETING AND MEDIA SERVICES** – which uses digital technologies for marketing and communication efforts that connect residents with city services.

- **THE APPLICATIONS TEAM** – which provides software solutions to increase efficiency, automate processes, and improve service.

- **THE PROGRAM MANAGEMENT OFFICE** – which supports other city agencies’ information technology projects by establishing policies and procedures and tracking project finances.

- **THE DATA TOOLS AND GOVERNANCE TEAM** – which connects city agencies and Denver residents with information and services.\(^8\)

---

**Proposed Vendor Management Policy**

In 2021, Technology Services drafted a policy for managing its vendors. However, officials have not yet approved this policy. Its purpose is to establish the agency’s formal governance over vendors that have access to all the data, hardware, and software used in city facilities or provided through cloud platforms.

The proposed policy also defines a handful of roles and responsibilities for certain city employees. Specifically:

- The chief information officer:
  - Approves and communicates changes and exceptions to the city’s information technology policies.
  - Blocks the acquisition of any high-risk or incompatible technology.
  - Reviews and approves all technology acquisitions, whether purchased or obtained through other means.

- Technology Services executive leadership would review and implement the city’s information technology policies.

- Business units — for example, other city agencies and their divisions — would need to understand and comply with Executive Order No. 18 and city policies. They would also need to communicate and maintain current policies and procedures, guidelines, and other documents to ensure city agencies comply and that they have clear expectations and understanding of how to buy technology for their organizations.

- Vendor managers — those city employees responsible for managing vendors’ activities and performance — would need to:
  - Understand and comply with the vendor management policy and other associated documents.

---

\(^8\) City and County of Denver, “Mayor’s Proposed 2022 Budget.”
- Ensure vendors performing work on behalf of the city also understand and comply with the vendor management policy.
- Document and communicate — in a complete, accurate, and timely fashion — any issue or violation of the policy.

**Activities for Vendor Management**

Technology Services' vendor management activities involve multiple teams, such as:

- The intake team.
- The governance risk and compliance team.
- The software asset management team.
- The contract monitoring team (in coordination with the City Attorney’s Office).
- The incident management team.

Each team performs different steps to review, approve, and monitor vendor relationships. Figure 3 illustrates the steps and the general flow of some of the activities.

**FIGURE 3. Technology Services’ Vendor Management Activities**

1. **REQUEST**
   - An agency either requests a technology purchase or Technology Services develops it.

2. **INTAKE**
   - The intake team gathers solutions for the request.
   - **Review**
     - The team reviews solutions for:
       - Initial technical architectural design.
       - Security.
       - Data protection and privacy.
   - **Bidding**
     - The team seeks proposals from qualified vendors.
   - **Vendor Selection**
     - Technology Services managers approve and select a vendor for the contract.

3. **CONTRACTING**
   - Technology Services contract administrators and the City Attorney's Office draft a contract with the chosen vendor.
   - **b**
     - Technology Services contract administrators and the City Attorney’s Office draft a contract with the chosen vendor.
   - **c**
     - Technology Services contract administrators and the City Attorney’s Office draft a contract with the chosen vendor.

4. **PROJECT MANAGEMENT**
   - Technology Services' project management team coordinates with the vendor to implement the solution.

5. **CONTINUOUS MONITORING**
   - Contract administrators; the governance risk and compliance team; the data protection and privacy team; and the incident management team share responsibility for monitoring the contract. The software asset management team manages software licensing contracts.

**Source:** Created by Auditor’s Office staff based on information from agency walk-throughs, policies, and data.
These steps begin when a city agency submits an idea to solve a technology issue or requests a specific vendor's product to help them meet business and operational objectives. Executive Order No. 18 grants Technology Services the authority to evaluate these requests.⁹

The agency's intake team evaluates each request through an initial review, which also involves the agency's security team, governance and compliance team, and data protection and privacy team. This initial review is meant to evaluate whether feasible alternative solutions exist. If the requested technology is approved to move forward, Technology Services will request bids from qualified vendors and then use a competitive selection process to choose which to hire.

Technology Services' contract administrators then work with the City Attorney's Office to draft a contract with the vendor, defining agreed-upon terms and objectives for the services being provided. Once the contract is signed, a Technology Services project management team coordinates with the vendor to implement the technology.

Then, during the life of each contract, various Technology Services teams are responsible for continuously monitoring the vendor by:

- Reviewing the vendor’s contract for expiration dates, insurance requirements, and money spent.
- Reviewing data security requirements to ensure vendors keep the city's data safe.
- Reviewing independent security assessments — such as service organization controls reports — to ensure a vendor can effectively protect its clients' data.¹⁰

Technology Services' security and data privacy teams review these specific reports to ensure vendors have appropriate safeguards covering security, availability, confidentiality, privacy, and processing integrity of systems and data. Reviewing these controls ensures vendors are compliant and can reduce risk to the city. If Technology Services' staff members identify weaknesses in the independent assessments, they can work with the vendor to resolve any issues or recommend the vendor implement other safeguards to ensure the city's data and systems are kept safe.

- Ensuring the vendor provides services as planned.

An interruption in service can impact the city's network and the city's ability to provide services to the public. Technology Services' incident management team measures an incident by how severe it is. This helps the city prioritize urgent incidents, so they can be addressed as soon as possible. Major incidents or repeated issues are escalated through a defined process, called “problem management.”

---

⁹ Exec. Order No. 18, City and County of Denver (2021).

¹⁰ We use the term “service organization controls reports” in reference to Service Organization Controls Type II reports. These are known by information technology professionals as “SOC 2” reports.
FINDING AND RECOMMENDATIONS

Technology Services Does Not Systematically Manage Its Vendors

The city’s Technology Services agency does not have an effective vendor management process to oversee and adequately monitor its information technology vendors.

Specifically, Technology Services has:

- No official policies and procedures to guide its employees, enforce requirements, and hold vendors accountable.
- No complete and approved roles and responsibilities or designated authority for the specific employees involved with vendor management.
- No plan to fund and adequately staff the vendor management function.
- No plan to train employees to monitor vendors in line with approved policy.

Technology Services lacks a defined strategy and an effective action plan for vendor management. The agency’s existing monitoring activities are insufficient, and officials have yet to approve a proposed vendor management policy the agency drafted last year.

Not having a comprehensive governance structure and adequate oversight of its information technology vendors poses many risks. For example:

- The agency does not effectively monitor outside vendors to ensure they have adequate safeguards to secure city data and that they provide services as they are contractually required.
- It does not attempt to hold vendors accountable for not complying with contract terms.
- It is not monitoring for when vendors stop working for the city nor is it letting key stakeholders know.
- It is not storing vendor data in a central location.

Leading practices for vendor management say governments should establish the organization’s level of responsibility, develop and implement strategy, and provide continuous oversight to ensure goals and objectives are achieved. But without an action plan detailing how overarching...

---

strategies would be implemented, who would implement them, how they would be funded, which take priority, and when tasks must be completed, Technology Services loses its ability to hold anyone — vendors or other city agencies — accountable.

If Technology Services cannot hold its vendors accountable, security vulnerabilities may go unnoticed, vendors may not provide services as contractually required, and city data could be lost.\textsuperscript{12}

\textbf{Technology Services Has an Incomplete Strategy and No Action Plan to Implement Vendor Management}

We interviewed Technology Services managers and staff and reviewed available strategic plans, policies, procedures, and other documents. We learned the agency has not comprehensively planned its strategy or created an action plan for a vendor management process. Instead, Technology Services has:

\begin{itemize}
  \item An incomplete strategy.
  \item An incomplete policy and procedure that remains in draft form.
  \item No defined roles and responsibilities.
  \item No staffing or budget plan.
  \item No training plan or presentation materials.
\end{itemize}

The Government Finance Officers Association says strategic planning for public organizations is based on the premise that leaders must be effective strategists for their organizations to fulfill their missions, meet their mandates, and satisfy their constituents in the years ahead.\textsuperscript{13}

\textbf{Technology Services' Strategic Plans Lack Important Elements to Act on Vendor Management}

We reviewed Technology Services' strategic plans for the last few years and found that its 2020 plan included very little information about vendor management. The plans for 2021 and 2022 spoke about maturing vendor management but without much detail.

Leading practices say government leaders should have strategies to cope with changes to the organization, and they need to develop evidence-based action plans that provide accountability to the taxpayers who fund their work.\textsuperscript{14} In addition, strategic objectives should “address the most critical issues,” and a separate action plan would describe how to address those issues.\textsuperscript{15}

\textsuperscript{14} Government Finance Officers Association, 2.
\textsuperscript{15} Government Finance Officers Association, 3.
We found Denver’s Technology Services agency has not developed certain important strategies that are critical to implementing a comprehensive vendor management process — such as specific strategies related to staffing, monitoring vendor contracts, closing out vendor contracts, training staff, and reviewing security assessments. Not only do leading practices recommend these strategies, but we learned at least one other major city has implemented them.

We compared Technology Services’ strategic plans to other similarly sized cities to identify common practices or recommendations for improvement. We learned the City and County of San Francisco’s information technology plan includes strategies for:

- Monitoring vendors’ contract compliance.
- Securing data and network infrastructure.
- Training city staff.
- Engaging proactively with vendors and partners.
- Improving how it selects and contracts with critical vendors to save taxpayer money.
- Monitoring other city agencies’ compliance with technology plans, budgets, standards, and policies and procedures.

San Francisco’s plan also included timelines for completing specified tasks.16

Meanwhile, Technology Services’ strategic plan for 2021 calls generally for a “deliberative process for consistent review of Technology.” But the agency fell short of implementing this goal.

Without key strategies specific to the vendor management process, Technology Services lacks the details of an action plan to implement them. To that end, the agency lacks approved and comprehensive policies and procedures, defined roles and responsibilities, a staffing and budget plan, and a training plan.

**NO APPROVED, COMPREHENSIVE POLICIES AND PROCEDURES**

Policies and procedures are a critical component of any governance system, because they guide employees and hold them accountable for reaching organizational goals and objectives.17 Federal standards say management of any organization should develop policies and procedures that reflect the

---


complexity and specificity of defined tasks.\footnote{18}

While Technology Services drafted a proposed vendor management policy in 2021 and the agency has some existing procedures for various activities, agency officials told us they delayed finalizing the draft policy. They also have not created all needed procedures that would be referenced in the policy.

The agency began a project in January 2021 to rewrite its existing policies by developing 16 new policies for the city’s technology infrastructure, based on a framework from the nonprofit Center for Internet Security. Of those 16 policies, the vendor management policy is one of two not yet finalized. Instead, Technology Services officials waited for this audit to finish so that they could include edits and leverage recommendations before approving the draft policy.

\textbf{LACK OF DEFINED ROLES AND RESPONSIBILITIES} – Technology Services officials outlined proposed roles and responsibilities in their draft vendor management policy. But because the policy is still in draft form, the agency has not implemented those roles or designated a leadership authority. It also has not communicated these proposed responsibilities to affected staff.

Significantly, the draft policy fails to designate a specific individual or group that would have authority to coordinate the vendor management process for information technology. Instead, the draft policy is vague and says a vendor management committee and other associated city agencies could take the lead.

Meanwhile, the city has developed some guidance on how Technology Services can manage vendor relationships. For example, its draft vendor management policy defines a “vendor manager” as the designated city representative on each contract or vendor relationship to oversee vendor activities and performance, as well as communication with the vendor. Leading practices say a service manager like this is someone who manages the development, implementation, evaluation, and ongoing maintenance of new and existing products and services.\footnote{19}

We learned other government organizations use various governance structures for their vendor management function.

In the City and County of San Francisco, officials created a seven-member team that manages the entire information technology vendor management process. This team reports to the city’s chief information officer by way of the chief finance officer.\footnote{20} Meanwhile, in Washington state, an executive steering committee makes decisions on strategy, scope, schedule, and


\footnote{20} City and County of San Francisco Department of Technology, “Procurement and Vendor Management 101 Training – Org Chart” (April 2022).
It is imperative for Technology Services to specify who will lead the agency’s vendor management process so it establishes authority and accountability over the process. Not establishing authority over the process can lead to a lack of vendor accountability or inconsistencies in how processes are performed.

**NO STAFFING OR BUDGET PLAN** – When we reviewed the existing structure of Technology Services’ teams and divisions involved in the vendor management process, we found a lack of collaboration, fragmented processes, and limited coordination and information sharing. Leading practices say that having the right organizational structure, people, skills, and competencies — along with policies and procedures — are components of effective governance.

Despite needing a centralized vendor management process, Technology Services officials told us they do not yet have a staffing plan for vendor management. Nor do they have a flowchart or other process showing how the various Technology Services teams would work together for effective vendor management. This is, in part, due to Technology Services leadership waiting to finalize and approve its proposed vendor management policy until after our audit is done.

Leading practices say organizations should have staffing plans to develop a clear understanding of the organization’s current state, the desired future state, and how to get there. When city agencies submit budget requests, staffing analyses can bolster an agency’s argument for a need.

While organizations commonly develop staffing plans when looking toward the next year’s budget, leaders can use them any time of year to make plans for the organization. However, because Technology Services officials have not created staffing and budget requests for the vendor management process, they lack this information moving forward.

**NO TRAINING AND COMMUNICATIONS PLAN** – Another important element Technology Services is lacking for its vendor management strategy is a documented training plan. Federal guidance says a successful training program would consist of details from defined policy and procedure, communicate roles and responsibilities for users, and establish expectations for monitoring and review.

---


23 Information Systems Audit and Control Association.


But Technology Services has not developed a training program specific to vendor management. The agency also has not prepared trainings in anticipation of eventually approving a vendor management policy. Officials told us a training program has not been developed and a decision will likely wait as long as the proposed vendor management policy is still a draft.

Technology Services' lack of urgency in creating an adequate governance structure and strategy for vendor management exposes the agency — and thereby, the city — to several deficiencies. These include not effectively monitoring outside vendors, not holding vendors accountable for breaking contract terms, and not monitoring for and communicating when vendors stop working for the city.

### 1.1 RECOMMENDATION

**Establish Organizational Structure**

The city's Technology Services agency should perform a staffing analysis to determine budget and staffing needs for the vendor management process. Based on this staffing analysis, the chief information officer should establish a staffing plan and designate an organizational structure, with a designated authority, for the vendor management team. The chief information officer should then document this structure in an approved vendor management policy.

**AGENCY RESPONSE** – AGREE, IMPLEMENTATION DATE – MARCH 14, 2023

SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

### 1.2 RECOMMENDATION

**Refine Strategic Plan Objectives**

The city's Technology Services agency should refine its strategic plan to include sufficient detail about how it will plan the vendor management process — including:

- Performance indicators for monitoring vendors’ contract compliance.
- Securing data and network infrastructure.
- Training city staff.
- Engaging proactively with vendors and partners.
- Improving how it selects and contracts with critical vendors to save taxpayer money.
- Monitoring other city agencies’ compliance with technology plans, budgets, standards, and policies and procedures.

Each objective should have a measurable timeline.

**AGENCY RESPONSE** – AGREE, IMPLEMENTATION DATE – MARCH 14, 2023

SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.
1.3 RECOMMENDATION  Refine, Approve, and Implement Vendor Management Policy and Procedures

The city’s Technology Services agency should refine its draft vendor management policy with more detail about the organizational structure, how it will communicate staff’s roles and responsibilities, and how it will train staff. In addition, Technology Services should create all needed procedures that will be referenced in the policy, including but not limited to procedures described in recommendations 1.5, 1.6, and 1.7. Once the agency completes these procedures, the chief information officer should approve the revised draft vendor management policy as soon as possible.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – MARCH 14, 2023
SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

1.4 RECOMMENDATION  Develop and Conduct Training

The city’s Technology Services agency should develop a training plan to ensure staff with roles and responsibilities for information technology vendor management are aware and informed of how the process is structured and how it should operate.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – MARCH 14, 2023
SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

Technology Services Does Not Consistently Review Vendors for Existing Security Controls

In assessing Technology Services’ activities for reviewing vendors’ security controls, we found Technology Services is not consistently documenting security reviews conducted either before a vendor is selected or periodically during the city’s relationship with the chosen vendor.

In 2021, Technology Services’ security team said it started a new process to review and keep documentation from third-party vendors at two stages in the vendor management process:

• When the agency’s intake team — along with the security and data protection and privacy teams — evaluates each idea or request through an initial review to evaluate whether feasible alternative solutions exist.
• Each year once a vendor is under contract with the city.
For the annual review, Technology Services' governance risk and compliance team as well as the data protection and privacy team check independent assessment reports to ensure contracted vendors have appropriate safeguards covering security, availability, confidentiality, privacy, and processing integrity.

To determine how consistently Technology Services performs these security reviews, we tested a sample of 26 information technology vendors under contract with the city. We selected this sample from several sources because Technology Services does not have a centralized and complete system of record for its vendor management data, which we discuss beginning on page 19.

Of the 26 vendors we looked at:

- Technology Services did not keep documentation or evidence of its review during the initial screening process for 17 vendors, or 65%.
- Technology Services did not document its annual reviews for 23 vendors, or 88%.
- For one review, the agency relied on an outdated service organization controls report.\(^\text{26}\)

These types of independent assessments should attest to the vendor's current security environment, which is its technical controls at a point in time. If Technology Services relies on outdated security information, it may leave city officials unaware of deficiencies in a vendor's security environment and could put the city at risk for losing data and harming its reputation.

This lack of consistency in the agency's reviews is because Technology Services has no formal policy or procedure to guide its employees in performing these security checks. Federal standards say having a formal policy with corresponding procedures allows organizations to have better operational control of their internal processes.\(^\text{27}\)

Performing security reviews consistently would ensure Technology Services is more aware of its information technology vendors' security controls, which could better shield the city against a data breach. And having a formal procedure to guide staff in this task would help make the Technology Services security team more effective and efficient. It would also help with cross-training employees and improving succession planning for when key employees leave their jobs.

---

26 We use the term “service organization controls reports” in reference to Service Organization Controls Type II reports, known by information technology professionals as “SOC 2” reports.

1.5 **RECOMMENDATION**

**Develop and Approve Security Review Procedures**

As part of implementing Recommendation 1.3, the city’s Technology Services agency should develop and implement security review procedures to ensure staff comprehensively and continuously monitor all information technology vendors for security concerns. These procedures should include at a minimum:

- Security reviews at intake and on a regular basis thereafter, at least once a year.
- Documentation for why a vendor is excluded from annual security reviews.
- Current independent security assessments.

**AGENCY RESPONSE** – AGREE, IMPLEMENTATION DATE – MARCH 14, 2023

SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

---

**Technology Services Does Not Hold Vendors Accountable for Meeting Contract Requirements**

Technology Services does not monitor all its information technology vendors to ensure they provide sufficient services as agreed upon. The agency also does not hold vendors accountable when they potentially fall short of meeting service-level objectives laid out in the contract or an accompanying agreement.

To monitor a vendor’s performance, “service-level agreements” should be included in a contract template or as a part of a contract, and specific “service-level objectives” should be defined within those agreements. These objectives are measurable criteria, such as the availability of a website to users.\(^{28}\) A vendor contract should also include clear language about what the vendor will be required to do if they break the agreement or fail to meet the agreed-upon objectives.\(^{29}\)

Technology Services has not formalized its procedures to require contractual service-level agreements that include clear service-level objectives. It also lacks procedures requiring staff to compare critical incidents with contractual service-level objectives, and it does not have procedures for seeking restitution when breaks in service levels warrant repayment from a vendor.

**MISSING OR UNCLEAR SERVICE-LEVEL OBJECTIVES** – As part of analyzing our sample of 26 vendor contracts, we found:

- Four, or 15%, had no service-level agreement included.


\(^{29}\) Information Systems Audit and Control Association.
Without clearly defined service-level objectives in vendor contracts, Technology Services cannot measure a vendor’s performance and hold them accountable for substandard service.

- Seven, or 27%, did not have clearly defined service-level objectives in either a separate agreement or the contract itself.
- Another 17 agreements, or 65%, had no service-level objectives.

Without clearly defined service-level objectives in vendor contracts, Technology Services cannot measure a vendor’s performance and hold it accountable for substandard service.

For the service-level objectives that do exist, Technology Services is not fully tracking them in its system of record, ServiceNow — such as the time a service or software application is available for use.

We found many critical incidents since January 2021 related to various vendor-provided products, and these incidents potentially broke service-level objectives. Technology Services staff told us they sometimes do not have access to a service agreement, and some contracts had missing or poorly defined objectives and penalties so agency staff could not enforce the penalties.

INCIDENT RESPONSE AND MANAGEMENT

Incident response and management is a governance structure in technology organizations that identifies, documents, and responds to deficiencies in information technology and security. Incidents can relate to any hardware, software, and data assets used in city facilities or provided through the cloud.

Technology Services defines major, or “critical,” incidents as emergencies or when the city loses critical services, security, or data affecting multiple users and agencies.

NO MONITORING FOR CONTRACT VIOLATIONS – When major incidents or repeated incidents occur — such as when a service or system goes down that affects the city’s network or the city’s ability to provide services to the public — Technology Services escalates the incident through a defined process called “problem management.” This is typically after a workaround has been developed for the critical incident.

However, Technology Services has not developed and formalized its problem management procedures to include checking the vendor’s service-level agreement and objectives to determine whether the vendor owes the city monetary penalties for failing to provide agreed-upon services. We looked at critical incidents for 26 vendors that occurred since Jan. 1, 2021, and we found eight vendors, or 31%, had critical incidents that may have impacted the service-level objectives documented in their agreements with the city. In none of those cases did the city attempt to collect restitution for the disruption in services — including one vendor with 20 separate incidents related to a single system.

We identified only one case when a vendor reimbursed the city for failing to meet its service-level objectives. However, this vendor self-reported to the city that it owed penalties. It sent two payments totaling about
A higher level of accountability would help ensure the city has the best vendors in terms of both effectiveness and efficiency.

$135,000 to the city, as of May 25, 2022.

The city needs to ensure its contracts and service-level agreements include specific, defined, and measurable objectives as well as clear language that gives the city recourse when vendors fail to meet those objectives. And then Technology Services needs to continuously monitor vendors’ performance by holding them to their contractual requirements.

Continuous monitoring will help ensure vendors do not take advantage of the city, particularly when they do not follow through on the services they were hired to perform. A higher level of accountability would help ensure the city has the best vendors in terms of both effectiveness and efficiency.

1.6 RECOMMENDATION

Develop and Approve Performance-Monitoring Procedures

As part of implementing Recommendation 1.3, the city’s Technology Services agency should:

- Populate ServiceNow with the service-level objectives.
- Develop and incorporate procedures to ensure staff are comprehensively and continuously monitoring all vendors to verify they are meeting contract terms and the requirements of their service-level agreements.
- Include steps in procedures to ensure contracts contain service-level agreements and service-level objectives and that these service-level objectives are relevant, enforceable, and measurable.
- Define and implement a process for seeking restitution when vendors break agreed-upon performance objectives.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – DEC. 14, 2022
SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

Technology Services Does Not Have a Consistent Process When Vendors Stop Working for the City

As a final step in managing its vendor relationships, Technology Services must ensure vendors separate from the city in a way that protects city data and informs key stakeholders. Vendor separation can occur when a contract ends, when the city no longer requires a service, or when the city and vendor sever their relationship after a contract violation or failure to meet service-level objectives.

But we learned Technology Services does not have documented procedures to guide this separation process. Staff within Technology Services are also not letting each other know when a vendor stops working
for the city, and the agency is not keeping data about which vendors have separated from the city so this information can be shared among agency personnel.

Technology Services’ proposed vendor management policy lacks guidance and specific procedures about what agency staff should do when a vendor separates from the city. And absent any current policy, the staff members assigned to monitor specific vendors have established their own individual processes.

For example, only some staff who monitor vendors let other Technology Services teams know when a vendor stops working for the city. Emails showed us this happened in at least one case where the city requested a security assessment from a vendor that had separated from the city. The former vendor then informed Technology Services it was no longer contracted with the city.

When other Technology Services staff are not informed, they may waste time requesting information from a vendor or even potentially receive confidential information they no longer need.

Technology Services staff told us that having a checklist for when a vendor separates from the city would be helpful in addressing inconsistencies, confusion, and poor communication. Federal standards say management of any organization should select an appropriate method to communicate the necessary information to enable staff to perform their duties and achieve their objectives.30 Areas to consider in a checklist include:

- Informing Technology Services teams, such as:
  - The contract administration team.
  - The security team.
  - The licensing team.

- Verifying that key stakeholders are told, including:
  - The purchasing division.
  - The Mayor's Office.
  - City Council liaisons.

- Removing network access for systems and individuals — including server accounts, virtual private network access, and individual accounts.

- Ensuring the system of record, ServiceNow, is updated.

---

As part of implementing Recommendation 1.3, the city’s Technology Services agency should develop and approve a process for when vendors separate from the city, and then management should communicate these procedures to relevant staff.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – NOV. 14, 2022
SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.

Technology Services
Stores Vendor Management Data across Multiple Systems

Technology Services does not centralize its vendor management data in one place. Instead, the agency has the data dispersed across at least five systems. Because of this, the agency lacks a complete, accurate inventory of its information technology vendors.

Federal guidance says all data should be in a central location as part of an effective vendor management process. Information needed for effective accountability includes the system name, software owners, and software license information. When systems are dispersed, organizations may not know which vendor owns a system. Preventing duplicate data can prevent this lack of accountability.31

We learned from the City and County of San Francisco that centralizing vendor management data could also save Denver money. San Francisco said its move to an all-in-one solution resulted in cost savings and more efficient vendor performance, but those city officials did not specify how much.

If Denver’s Technology Services agency were to centralize its vendor data, it could better maintain all vendor documentation — such as a comprehensive inventory and individual contracts, licensing, and certificates of insurance — in one system.

Technology Services staff told us that ServiceNow, the system the agency uses to track all technology equipment and software, is its system of record for tracking and monitoring vendor information. But we learned ServiceNow is not used as a centralized source.

Instead, vendor management data is dispersed across at least five systems — resulting in confusion and inaccurate records. In our testing, we found 10 of the 26 samples of vendor-supported systems listed former employees as the assigned individual responsible for managing the

vendor. Without an active employee assigned to manage vendors and perform security reviews, there is a risk that vendor incidents may go unnoticed, contracts may expire resulting in legal risk, and communication may suffer or cease altogether.

The City and County of San Francisco uses ServiceNow as its centralized system of record for information technology vendor management. This single system tracks vendor performance and includes integrated process flows for purchase approvals all in one place. Because Technology Services already uses ServiceNow for other elements of vendor management, it may be able to expand its use similar to San Francisco.

Technology Services staff told us they are aware ServiceNow is missing vendor information and that having a system of record that is 100% accurate is essential to successful vendor management.

**RECOMMENDATION**

Implement a Single System of Record for Vendor Management

The city’s Technology Services agency should establish a single system of record, such as ServiceNow, for vendor management data and monitoring activities. Once Technology Services establishes a single system of record, it should create a process for reviewing vendor management-related data to ensure accuracy.

**AGENCY RESPONSE** – AGREE, IMPLEMENTATION DATE – SEPT. 15, 2023

SEE PAGE 21 TO READ THE AGENCY’S RESPONSES.
RECOMMENDATION 1.1

AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: MARCH 14, 2023

The conclusion of this audit engagement allows Technology Services to identify any additional roles necessary for vendor management. Technology Services will conduct a staffing analysis. Once the analysis is complete roles and responsibilities will be allocated and outlined within the Technology Service’s organizational structure.

RECOMMENDATION 1.2

AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: MARCH 14, 2023

Technology Services will review the identified objectives and update its current strategic plan as appropriate.

RECOMMENDATION 1.3

AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: MARCH 14, 2023

Throughout the vendor management audit engagement Technology Services has been forthcoming in the intention to pause on the completion and implementation of the vendor management policy and procedures until the completion of the audit engagement.

The conclusion of this audit engagement allows Technology Services to evaluate the audit recommendations. Technology Services will update the policy and procedures with a holistic focus in respect to capturing the organizational structure, roles & responsibilities, processes, and procedures.
RECOMMENDATION 1.4

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: MARCH 14, 2023

Technology Services will implement a vendor management training plan for those who hold a role within vendor management.

RECOMMENDATION 1.5

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: MARCH 14, 2023

In 2020 Technology Services implemented a vendor risk assessment when evaluating potential new technology vendors. The current vendor risk assessment process includes security and data protection reviews. Currently we are refining and documenting the initial vendor risk assessment review process.

Technology Services is currently reviewing industry standards and best practices associated with ongoing security & data protection vendor management. Technology Services will create monitoring frequency and oversight criteria based on risk assessment. Technology Services will document standards and criteria for risk evaluation, monitoring, exclusion criteria, as well as risk remediation standards and processes.

RECOMMENDATION 1.6

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: DEC. 14, 2022

Technology Services will review staffing capacity, roles, responsibilities, determining where vendor performance monitoring should reside in the organization. Technology Services will also evaluate the purchase of the ServiceNow functionality necessary to populate service-level objectives.

The City Attorney’s Office in collaboration with Technology Services has created a new standardized legal agreement template to be utilized with Technology Services vendors. This agreement is not limited to, although includes relevant and enforceable service level standards, data protection and security compliance requirements, along with Technology Services right to termination without cause.

RECOMMENDATION 1.7

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: NOV. 14, 2022

Technology Services will develop and approve a communication process for vendor separation to relevant staff.
RECOMMENDATION 1.8

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: SEPT. 15, 2023

Technology Services is currently evaluating the expansion of ServiceNow. Stakeholders outside of Technology Services utilize various systems for management of legal and financial documentation associated with technology services vendors. To ensure all vendor management information is accessible for all stakeholders without duplication of efforts technology services will determine the feasibility of the implementation of this recommendation.
OBJECTIVE

To assess the effectiveness of Technology Services’ processes for vendor management governance, continuous monitoring, and compliance with agency policies and procedures.

SCOPE

We focused our audit on software and services managed by third-party vendors that Technology Services is contracted with. Our audit did not include other vendors such as concessionaires or those that provide hardware such as networking equipment, internet-connected devices, and software asset management (e.g., licensing).

We reviewed Technology Services’ data, processes, and future planning efforts from Jan. 1, 2021, through May 31, 2022.

METHODOLOGY

We used several methodologies to gather and analyze information related to the audit objectives. The methodologies included but were not limited to:

• Interviewing key Technology Services personnel about the city’s information technology vendor management process — including the process for when a vendor separates from the city.
• Reviewing and assessing Technology Services’ proposed policies and procedures for vendor management.
• Reviewing and assessing contracts related to vendor management.
• Reviewing and researching leading practices, including the city’s annual budgets, the city’s Executive Order No. 18, and information from CliftonLarsonAllen, the Government Finance Officers Association, the Information Systems Audit and Control Association, the National Institute for Standards and Technology, the Society for Human Resource Management, and the U.S. Government Accountability Office.
• Evaluating the scope of vendor security reviews conducted by Technology Services’ information security team.
• Testing the completeness and accuracy of the agency’s vendor inventory list.
• Comparing Technology Services’ systems that track vendor information.
• Interviewing and researching other comparable cities’ vendor management practices against Technology Services’.

• As described in the appendix, sampling a selection of vendors to determine whether each sample:
  ▪ Had an assigned vendor manager who is an active employee.
  ▪ Had evidence that an initial vendor risk assessment was conducted and approved.
  ▪ Used a standard city contract template.
  ▪ Included service-level agreements and service-level objectives in the contract.
  ▪ Had evidence of restitution to the city if a contract violation occurred.
APPENDIX

**Sampling Methodology**

We used both judgmental and random sampling to select a sample of 26 software applications and vendors.

We identified these from several sources because Technology Services does not maintain one complete system of record for vendor management, as we discuss on page 19. Our sample did not include vendors providing hardware and software assets, as those were beyond the scope of this audit.

We compared three different datasets to link a software application with the vendor providing the technology. These datasets included a list of contracts provided by the Technology Services’ contract administration team, a list of critical incidents provided by the Technology Services incident manager, and a list of business applications that we were able to export from the agency’s ServiceNow system.

To ensure this data was reliable and accurate, we:

• Directly observed Technology Services staff export the data from each respective system it was originally stored in.
• Directly exported some data from the same systems to perform data comparisons.
• Checked the data for missing or blank values, duplicate entries, etc.

We used both judgmental and random sampling techniques for some selections based on our review of the data, our interviews, and known risks. We identified random samples using an online random number generator and then applied those random selections to each random sample.

Because of the disparate data, we could not easily find the vendors matched to specific software applications, which limited our overall subpopulation.

Therefore, we used three approaches to select our sample of 26 vendors:

• We identified the first 10 items in our sample after comparing risk assessments by Technology Services’ security team with a contract list from the agency’s contract administration team. We chose five and then randomly selected the other five.
• Next, we identified six more vendors using the incident management team's list of critical incidents since Jan. 1, 2021. We chose three vendors based on conversations with the critical incident manager where the incident manager highlighted repeated incidents. We selected the other three randomly.
• Lastly, we identified our final 10 vendors after comparing the applications in ServiceNow with the contract administration team’s list of contracts. We identified 56 applications that had a contract with Technology Services. We removed from the list the 16 applications and vendors that we had already identified for sampling. Of the remaining 40 vendors, we chose five to sample and selected another five at random.
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.