Audit Team
Nicholas Jimroglou, CISA, CDPSE, Information Systems Audit Lead
Rob Farol, CISA, CIA, CGAP, Information Systems Audit Senior
Dave Hancock, CISA, MURP, Information Systems Audit Senior

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director

Audit Committee
Timothy M. O’Brien, CPA, Chairman
Jack 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 Avenue, #705
Denver, CO 80202
(720) 913-5000

Or download and view an electronic copy by visiting our website at:

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

September 21, 2023

We audited how well Denver International Airport's Business Technologies division manages the airport's information technology vendors — specifically how effectively it oversees these vendors and monitors performance and whether it has established policies, procedures, and other processes it follows to ensure good governance. I now present the results of this audit.

The audit revealed the airport inadequately monitors its information technology vendors. It has no documented policies, procedures, or training plans for monitoring vendors, and the airport lacks a centralized system to track technology vendors. We also found the airport does not require service-level agreements in each technology contract, does not consistently document lessons learned after major incidents, and does not evaluate compliance with service-level objectives within its system of record.

By implementing recommendations for stronger policies, procedures, training, data management, contract administration, and incident management, the airport will be better able to hold its technology vendors accountable to specific standards while also having the means to enforce those standards through contract- and airport-specific requirements.

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 at Denver International Airport 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
Denver International Airport’s Business Technologies division lacks a robust information technology vendor management program

The airport does not adequately monitor its information technology vendors to ensure third-party systems are monitored and maintained. We found Business Technologies is missing:

- A formal strategic plan to guide its vendor management governance.
- Documented and approved policies and procedures to guide its employees, enforce requirements, and hold technology vendors accountable.
- Training plans to educate staff about how best to monitor technology vendors in line with approved policy.
- A centralized list of technology vendors.
- Procedures to periodically assess risks around technology vendors’ security and architectural controls.

Meanwhile, Business Technologies also does not:

- Hold information technology vendors accountable by requiring service-level agreements and objectives in each technology contract.
- Consistently document lessons learned after major incidents or evaluate compliance with service-level objectives.

WHY THIS MATTERS

Business Technologies’ delay in establishing a comprehensive governance structure for vendor management puts Denver International Airport at risk of not getting what it pays for from its technology vendors and potentially exposes the airport to vulnerabilities.

If technology vendors do not adequately protect the airport’s data or if they do not deliver services as promised, the airport could lose revenue, passenger services could be affected, and the airport’s reputation could be damaged.
## 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>5</td>
</tr>
<tr>
<td>Denver International Airport’s Business Technologies division lacks a robust information technology vendor management program</td>
<td></td>
</tr>
<tr>
<td>Business Technologies has no strategic plan to guide information technology vendor management</td>
<td>6</td>
</tr>
<tr>
<td>Business Technologies has not formalized its information technology vendor management process</td>
<td>8</td>
</tr>
<tr>
<td>Business Technologies lacks a consistent way to monitor the airport’s information technology vendors</td>
<td>14</td>
</tr>
<tr>
<td><strong>AGENCY RESPONSE TO AUDIT RECOMMENDATIONS</strong></td>
<td>19</td>
</tr>
<tr>
<td><strong>OBJECTIVE, SCOPE, AND METHODOLOGY</strong></td>
<td>22</td>
</tr>
</tbody>
</table>
BACKGROUND

Denver International Airport

Denver International Airport is owned by the City and County of Denver and is under the purview of Denver’s mayor. In 2022, it was the third-busiest airport in the world and served 69 million passengers.¹

The airport is a government-owned enterprise — meaning it operates like a business and must raise its own revenue and cover all its own costs. The airport uses its money to operate, maintain, plan, and develop airport property.

BUSINESS TECHNOLOGIES – Business Technologies is the technology division of the airport and provides information technology-related infrastructure and services for airport operations. It manages the airport’s information security and cybersecurity activities. Business Technologies has significant power in setting strategy and determining funding for airport technology within the airport’s overall budget, as well as vetting potential technology vendors and working with and managing those vendors it ultimately contracts with.

Business Technologies also manages the airport’s data centers and provides services for technical infrastructure, maintenance, voice and data networks, wireless networks, and cybersecurity at the airport.

As of December 2022, Business Technologies had about 140 full-time staff positions across five teams. These teams specialize in:

- Information security and information technology compliance.
- Infrastructure and operations.
- Information technology business operations.
- Information technology business solutions.
- Information technology communication services.

Business Technologies manages 248 vendors — which are used both within Business Technologies and among overall airport operations staff. These vendors include those involved with security, baggage handling, badging, Microsoft 365, timekeeping, payroll, financial systems, and a host of other systems and information technology-related professional services. Business Technologies also maintains relationships with specialized airport operations software providers such as PROPworks — the airport’s revenue management system — and other systems specifically designed for airport operations.

Several of these systems are managed and administered by Business Technologies itself, but other systems are managed by various outside

Information technology vendor management

Sufficiently managing information technology vendors is crucial to supporting efficient and effective operations at a major international airport. Airport technology vendors provide essential services, software solutions, and technical support to ensure smooth operations, security, and passenger safety and satisfaction.

CliftonLarsonAllen LLP, an audit and consulting firm, advises that information technology organizations should oversee specific activities during their vendor management life cycle. As shown in Figure 1, this life cycle starts with intake and vetting what technology solutions and vendors are the most appropriate for the organization’s operational, architectural, security, and data protection needs.

FIGURE 1. Information technology vendor management life cycle stages and recommended activities

VENDOR SELECTION
• Perform intake and vet solutions and vendors.
• Request and evaluate proposals.
• Perform due diligence and assess risks (e.g., security, architectural, data protection and privacy).
• Select a vendor.
• Negotiate and sign vendor contract.

CONTINUOUS MONITORING
• Relationship management.
• Key contract terms including certificates of insurance.
• Service-level agreements and objectives including performance metrics.
• Annual and ongoing risk assessments.
• Continuous security and data protection reviews.
• Renewal monitoring.

END OF RELATIONSHIP
• Give notice of termination.
• Remove access (physical and electronic).
• As appropriate, ensure vendor either returns data or destroys it.

Source: CliftonLarsonAllen LLP.

Once a contract with a vendor is signed, the organization should then continuously monitor performance metrics and perform periodic security reviews and data privacy risk assessments. This continuous monitoring helps ensure the vendor provides services in line with contracted terms and protects the organization’s data.

When it is time for the organization to end its relationship with a vendor, the organization should remove the vendor’s access and get back any proprietary data or otherwise verify that such data has been destroyed.

Vendor management governance at the airport

In 2022, we audited how well the city’s Technology Services agency oversees information technology vendor management across city government.\(^3\) Technology Services released its official vendor management policy in September 2022, around the time we published that audit.\(^4\)

After we began this audit at the airport in February 2023, Business Technologies managers said that because of the airport’s autonomy as a government enterprise and because of specific federal aviation requirements, they would not adopt the city’s vendor management policy as the airport’s own. But they planned to mirror some of the policy for the airport’s needs.

Like the city, the airport uses ServiceNow as its system of record for information technology. As shown in Figure 2: In February 2023, Business Technologies asked the airport for funding to buy a vendor risk management module for ServiceNow. This add-on feature would provide a single system of record for the airport to manage its vendors and document its continuous monitoring of risks and security controls, among other tasks.

FIGURE 2. Business Technologies’ implementation timeline

- **February**
  - Audit begins.
  - Business Technologies asks the airport for funding to buy a vendor risk management module for ServiceNow.

- **April**
  - After receiving approval for the project using airport capital funds, Business Technologies begins implementation.

- **Late May**
  - Business Technologies managers finish a staffing analysis for the airport’s annual budget process and ask for two administrators dedicated to vendor management.

- **June**
  - Business Technologies hires a third-party contractor to implement the ServiceNow vendor risk management module.

**Within 11 weeks**

The airport expected to have the new feature fully implemented.

**Source:** Auditor’s Office analysis.


\(^4\) We will not officially evaluate the quality of Technology Services’ new policy until we follow up on that original audit at a later date.
Business Technologies received approval for the project using airport capital funds, and the division began implementing it in April 2023. Acquiring the vendor risk management module for ServiceNow is estimated to cost the airport $480,000 for design, implementation, project management, and contingency — as well as another $100,000 for additional licenses.

In late May 2023, Business Technologies managers finished a staffing analysis for the airport’s annual budget process and asked for two administrators dedicated to vendor management, one starting in 2024 and the other starting in 2025. The two positions would focus on finalizing and implementing a vendor management policy for the airport and managing its vendors using the new ServiceNow module.

Meanwhile, in June 2023, Business Technologies hired a third-party contractor to implement the ServiceNow vendor risk management module, at an estimated cost of $182,000.

As of then, the airport expected to have the new feature fully implemented within 11 weeks. During the same time, officials planned to implement new requirements from the federal Transportation Security Administration and also finalize and distribute a vendor management policy and supporting procedures.
FINDING AND RECOMMENDATIONS

Denver International Airport’s Business Technologies division lacks a robust information technology vendor management program

The airport’s Business Technologies division does not adequately oversee the airport’s nearly 250 information technology vendors to ensure third-party systems are monitored and maintained.

We found the airport has an informal process for its information technology vendor management program. While this system works for employees who have been at the airport and know the process well, it has not been formalized nor has it been disseminated to other employees who are unfamiliar with the process.

Because of escalating demands for information technology services, airport officials have put constant pressure on Business Technologies and diverted its focus toward more urgent tasks — such as implementing new requirements from the Transportation Security Administration. This has left division managers and staff with limited time to dedicate toward developing an effective way to manage the airport’s technology vendors.

Business Technologies is aware it needs to make improvements in this area and has already taken some steps to do so.

Since April 2023, the division has been acquiring a new feature for its system of record to improve how it manages information technology vendors. Managers have also prepared a project charter, requested the needed funding, prepared a draft vendor management policy, and completed a staffing analysis. This work, as well as implementing the new feature for its system of record, will help address several of the risks we identified during this audit.

While we determined Business Technologies’ efforts to implement a new vendor risk management module are a good start, we also noted several key areas of improvement that division managers will need to address before they fully implement the new feature. In the absence of a well-defined governance structure, formal guidance, and adequate oversight...
of information technology vendors’ activities, the airport has already encountered challenges in:

- Establishing documented policies and procedures.
- Ensuring staff are sufficiently trained on vendor management.
- Maintaining a complete and accurate inventory of vendors.
- Coordinating efforts between Business Technologies and the city’s Technology Services agency to ensure all vendors are assessed for potential risks.

Additionally, the airport faces increased vulnerabilities in other ways. Business Technologies is not consistently performing initial and periodic risk assessments of its vendors, and not all contracts have specific agreements and objectives laying out the levels of service vendors are supposed to provide — including what the consequences are when a vendor does not follow through. Furthermore, we found airport staff are not consistently documenting lessons learned after major vendor incidents or ensuring the airport seeks restitution for service interruptions.

In recent years, the aviation industry’s reliance on information technology systems and services has significantly increased. As airports adopt advanced technologies to enhance their security, improve passengers’ experiences, and streamline operations, the complexity and scale of information technology vendor management have grown proportionally.

Consequently, it is imperative for airports to maintain robust governance and oversight that ensures vendor compliance, reduces and addresses risks, and achieves desired outcomes. This is especially crucial for Denver International Airport, given it is the third-busiest airport in the world.

The issues we detail in this audit stem not only from the constant pressure Business Technologies faces but also the airport’s lack of a documented strategic plan to guide information technology vendor management using concrete and measurable goals.

The airport crafted a “Vision 100” strategic plan as its guiding framework to accomplish defined objectives and aspirations. It is the responsibility of all divisions — including Business Technologies — to facilitate and execute the airport’s strategic vision and plans.

While the Vision 100 plan provides a high-level overview, it does not delve into the specifics of vendor management goals. Instead, Business Technologies adopts project-specific plans, like the one staff prepared for the new vendor risk management module they are acquiring for ServiceNow, the airport’s system of record.

---

Business Technologies has no strategic plan to guide information technology vendor management

---

These project-specific plans play a crucial role in supporting the airport’s overall strategic vision; however, Business Technologies has no strategic plan to document its own vision.

Leading practices for information technology vendor management say governments should establish an organization’s level of responsibility, develop and implement a strategy, and provide continuous oversight to ensure the organization achieves its goals and objectives. The organization should also have an action plan detailing how overarching strategies are to be implemented, who would implement them, how they would be funded, which take priority, and when tasks must be completed.

In addition, other leading practices recommend that organizations follow specific steps in their strategic planning processes. This includes defining the problem to be solved, developing a vision to solve each problem, and documenting strategies to achieve the vision.

Without a strategic plan or a detailed action plan for its information technology vendor management, Business Technologies loses its ability to hold airport vendors accountable and ensure they provide the services they are hired for.

1.1 RECOMMENDATION

Document an information technology vendor management strategic plan

Denver International Airport’s Business Technologies division should create and document a strategic plan for information technology vendor management that supports the overall strategic vision at the airport. In developing its vendor management program, Business Technologies should include sufficient detail — and measurable time frames — in its strategic plan for each of the following objectives:

- Having performance indicators to monitor vendors’ contract compliance.
- Securing data and network infrastructure.
- Training airport staff.
- Engaging proactively with vendors and partners.
- Improving how it selects and contracts with critical vendors to save money.
- Monitoring other airport divisions’ compliance with technology plans, budgets, standards, and policies and procedures.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JAN. 2, 2024

SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

---


Business Technologies has not formalized its information technology vendor management process. Business Technologies’ process for managing technology vendors has so far been informal and undocumented, but managers are taking steps to formalize this. For instance, Business Technologies drafted a proposed policy and procedures for information technology vendor management, which were still in draft form as of June 2023.

We found the division lacked other key pieces for its vendor management process, too. For example, in addition to the lack of approved policy and procedures, we found:

- An absence of staff training for vendor management.
- No comprehensive list of the airport’s technology vendors, as well as missing vendor names in the system of record.
- No process to coordinate periodic risk assessments and security reviews of vendors shared with the city.

Without a documented and approved policy and without formalizing these key pieces of the vendor management process, Business Technologies staff responsible for vendor management may not be aware of their responsibilities — which could lead to inconsistent vendor management and oversight. This also risks affecting airport revenues and the services provided to passengers and other third-party vendors.

This lack of urgency in establishing a robust governance structure and strategy for information technology vendor management exposes the airport to several vulnerabilities. These include ineffectively monitoring third-party vendors, failing to hold vendors accountable when they violate contract terms, and not ensuring sufficient oversight and communication when vendors stop providing services to the airport.

**NO FORMAL POLICY 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. Federal standards say managers of any organization should develop policies and procedures that reflect the complexity and specificity of defined tasks. Such policies should explain compliance with regulatory requirements, roles and responsibilities, training activities, and provide further guidance on how to assess compliance.

When we began this audit in February 2023, Business Technologies staff told us they were developing a comprehensive vendor management policy that covered all three phases of the vendor management life cycle, a process we illustrated in Figure 1 on page 2. Throughout most of our audit, we found no other evidence of documented policies or procedures the airport might have had related to vendor management. This included no documented and approved policies for the entire vendor management life cycle from vendor selection to vendor separation.

---


Business Technologies staff told us they are not consistently involved early enough in the vendor selection process for all technology solutions at the airport. Finalizing and approving a vendor management policy that dictates Business Technologies' consistent involvement during the vendor selection process can ensure airport divisions appropriately involve Business Technologies.

By the end of our fieldwork in June 2023, Business Technologies staff had written an initial draft of a proposed vendor management policy. The draft discussed elements such as vendor regulatory requirements, roles and responsibilities, continuous monitoring requirements, vendor termination activities, and more.

While this draft policy appeared to be comprehensive and it outlined several important vendor management activities, it was still only a draft — and as such, airport officials had not yet approved it or put it into use. Formal approval and implementation of a policy is necessary for it to be optimally useful.

For example, in its draft vendor management policy, Business Technologies had outlined proposed roles and responsibilities, but because the policy was still in draft form, the division had not put those roles into effect or designated an official authority over vendor management activities. It also had not communicated these proposed responsibilities to affected staff.

**NO TRAINING OF STAFF RESPONSIBLE FOR VENDOR MANAGEMENT** – Business Technologies is also lacking a documented training plan for its vendor management strategy. Federal guidance says a comprehensive training program should include specific details derived from established policies and procedures. A training program should clearly communicate the roles and responsibilities of users and establish expectations for monitoring and review.10

As of June 2023, Business Technologies had not created a training program specifically tailored to vendor management. Even if it had, such a training program could not have been sufficiently tied to established policies and procedures as leading practices recommend, because Business Technologies' proposed policy was still in draft form.

Staff said they intend to develop a training plan, but they had not yet begun this process during our audit. They said their plans are on hold until they can refine the breadth of the vendor management life cycle.

**NO CENTRALIZED LIST OF INFORMATION TECHNOLOGY VENDORS** – Business Technologies does not have a systematic way of centralizing its vendor management data in one place. The division uses ServiceNow — the city's and the airport's system of record for information technology — to keep information on all technology vendors at the airport.

Until the vendor risk management module is implemented, Business Technologies will be missing out on important record-keeping abilities.

But this functionality is limited because Business Technologies has not yet fully implemented ServiceNow’s vendor risk management module, an add-on feature that offers detailed vendor inventory-tracking capabilities, continuous monitoring features, and vendor risk assessments, among other tools. Until the vendor risk management module is implemented, Business Technologies will be missing out on important record-keeping abilities.

A team within Business Technologies was working to update the vendor list in ServiceNow during our audit. Our analysis found 16 unique vendor names missing from the airport’s list of 248 vendors in ServiceNow. Instead, vendor names and management information were scattered throughout various reports — including incident reports, performance metric analyses, and initial and periodic security reviews and operational risk assessments.

In addition to the incomplete inventory of vendors, the airport’s current record-keeping capabilities in ServiceNow do not easily allow Business Technologies to keep track of which employees are assigned to manage a vendor. For example, we sought to determine whether each vendor in our sample was assigned to an active employee. Three of the 20 vendors we chose to look at, or 15%, had a service manager associated with an airport employee who had either transferred from that position or who no longer worked at the city.

Federal guidance says all data for an organization should be in a central location as part of an effective vendor management process. Information needed for such effective accountability includes the system name, the vendor name, and software license information. When systems are fragmented, organizations may not know which vendor is responsible for a given system. Duplicative data can also hinder accountability.¹¹

This lack of a complete and centralized system to manage vendor records can make it more difficult for Business Technologies to track and monitor its vendors. This could hinder the airport’s efforts for continuous monitoring and overseeing vendor relationships.


---

**SAMPLING METHODOLOGY**

To analyze a sample of the airport’s 248 technology vendors for this audit, we used our professional judgment to select a pool of 20 vendors that are managed by third parties and considered among the airport’s most critical vendors.

We selected this sample from several sources because Business Technologies does not have a centralized and complete system of record for its vendor management data, which we discuss beginning on page 9.
NO FORMAL PROCESS TO COORDINATE RISK ASSESSMENTS WITH THE CITY – We found no clear distinction between vendors that are tracked and monitored by Business Technologies versus those that are tracked and monitored by other agencies at the city that perform the same work.

For example, across the City and County of Denver, all city agencies use some vendor-supported systems such as Workday, the city’s human resources, payroll, and timekeeping system. Technology Services — being the overarching information technology agency for most of the city — is responsible for tracking and monitoring these citywide vendors.

When we analyzed our sample of 20 airport information technology vendors, we learned some of those from Business Technologies’ vendor list had little or no information listed. Initially, it appeared as if Business Technologies had done neither an initial review nor periodic reviews of these vendors to ensure they posed no risk to the airport.

After we investigated further, we learned some of these airport vendors also provide services citywide so they are shared with the city’s Technology Services agency. Therefore, these shared citywide vendors are tracked and monitored by Technology Services — not Business Technologies.

Airport officials told us that because Technology Services tracks and monitors these shared vendors, it would be duplicative for Business Technologies to track them, too. But Business Technologies’ vendor list does not distinguish between which vendors are Technology Services’ responsibility to track and monitor and which are Business Technologies’.

Additionally, of the vendors Business Technologies does track and monitor, we found 12 of the 20 vendors in our sample — or 60% — did not have evidence of an initial risk assessment being done and 11 — or 55% — did not have evidence of periodic risk assessments being done. An initial risk assessment is important for organizations to determine what security issues might be present in a system they plan on connecting to their network. Periodic assessments are necessary to determine whether new risks have been introduced to the system that may have otherwise been undetected.

For example, the airport did not complete an initial risk assessment of NanoLumens Inc., a critical vendor responsible for displaying airline gate information for traveling passengers. Business Technologies also had no evidence on file of having done periodic risk assessments for NanoLumens.

As another example, the airport did complete an initial risk assessment in 2019 of PROPworks, its critical financial system of record — but there was no evidence it has performed any periodic assessments since.

Airport officials told us they are working on a consistent risk assessment process to review all technology vendors. They said the process will include initial and periodic risk assessments.
Federal guidance says governments should have a formal policy with corresponding procedures that allow the organization to have better operational control of its internal processes. The absence of a formal process to conduct initial and periodic risk assessments for vendors managed by or used by Business Technologies can leave the airport vulnerable to unidentified risks and inadequate risk mitigation strategies.

1.2 RECOMMENDATION Finalize a vendor management policy

As part of implementing the ServiceNow vendor risk management module, Denver International Airport’s Business Technologies division should finalize and approve its draft vendor management policy and ensure it includes details about the organizational structure supporting the airport’s vendor management life cycle, staff resources and roles and responsibilities, and all related activities needed to ensure sufficient governance of information technology vendor management at the airport.

Additionally, Business Technologies should develop and finalize supporting procedures for all vendor management life cycle activities, including but not limited to procedures described in recommendations 1.3, 1.4, 1.5, 1.7, and 1.8 — such as procedures for continuous security and performance monitoring as well as consistent steps to end a relationship with a vendor.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – APRIL 1, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

1.3 RECOMMENDATION Require Business Technologies’ early involvement in technology procurement

As part of implementing Recommendation 1.2, Denver International Airport’s Business Technologies division should work with airport officials to require the division’s involvement during procurement to ensure initial technical, architectural, security, data protection, and privacy risks are addressed upfront for any technology introduced at the airport.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JULY 1, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

1.4 RECOMMENDATION  Develop a vendor termination process

As part of implementing Recommendation 1.2, Denver International Airport’s Business Technologies division should develop, approve, and document a consistent process for staff to follow when information technology vendors stop working for the airport. This process should include considerations like updating the airport’s vendor inventory list, ensuring vendors return or destroy city data in their possession, and removing vendor accounts from airport systems. Once these procedures are approved, division managers should communicate them to relevant staff.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – APRIL 1, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

1.5 RECOMMENDATION  Develop security review procedures

As part of implementing Recommendation 1.2, Denver International Airport’s Business Technologies division should develop, implement, and document procedures to ensure staff continuously monitor all airport information technology vendors for risks and security concerns. These procedures should include, at a minimum:

- Ensuring security reviews and risk assessments are done at intake and at regular times thereafter, depending on the criticality to the airport and the risks posed by a vendor’s system.
- Detailing requirements for security reviews and risk assessment reports from independent assessors.
- Obtaining a copy of vendors’ risk assessments for vendors managed by the city’s Technology Services agency, so Business Technologies has it for its own records and can document these exceptions.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JUNE 3, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

1.6 RECOMMENDATION  Develop an information technology vendor management training plan

Denver International Airport’s Business Technologies division should develop a training plan to ensure staff with roles and responsibilities related to information technology vendor management life cycle activities are aware and informed of how the governance process is structured and how it should operate.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JAN. 2, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.
1.7 RECOMMENDATION

Ensure complete and accurate information in ServiceNow

Denver International Airport’s Business Technologies division should continue to implement an automated single system of record for vendor management — such as the ServiceNow vendor risk management module — to monitor all vendor management life cycle activities and ensure the airport’s information technology vendor inventory list is complete and accurate.

Furthermore, as part of implementing Recommendation 1.2, Business Technologies should develop a process, policy, and procedures to ensure data stored in this system of record remains complete and accurate.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – APRIL 1, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

Business Technologies lacks a consistent way to monitor the airport’s information technology vendors

Leading practices for information technology say organizations should establish and maintain criteria to measure how their technology vendors perform in accordance with their contracts. But the airport’s Business Technologies division has not established and documented such a process to ensure it consistently and sufficiently monitors the airport’s information technology vendors and holds them accountable for contracted services.

An ideal monitoring process should be documented and include:

- Monitoring service-level agreements and objectives that are included in contracts.
- Documenting in a system of record lessons learned from major vendor incidents.
- Seeking restitution from technology vendors that did not fulfill their contractually required service-level objectives.

As we discussed, Business Technologies managers have drafted an information technology vendor management policy, but as of June 2023, this policy had not been finalized or approved. This draft policy includes requirements to monitor and track vendors’ performance based on their service-level objectives.

SERVICE-LEVEL AGREEMENTS AND OBJECTIVES

In information technology, a “service-level agreement” supplements a vendor contract by laying out the exact levels of service the vendor agrees to provide. Such agreements should ideally include “service-level objectives” that are specific and measurable, so that the organization can monitor the vendor’s performance.

Because the airport lacks a defined monitoring process, it inconsistently holds vendors accountable for the levels of service they have agreed to provide. This lack of oversight also hinders the airport's ability to identify and address recurring issues, which could result in repeated incidents and service disruptions affecting passenger travel and airport operations.

Several airport technology contracts do not include service-level agreements and objectives

We learned Denver International Airport does not consistently require or ensure service-level agreements are in its technology vendors’ contracts. Where service-level agreements are added to a contract, they are generally provided by the vendor and included only as an exhibit. In fact, none of the airport procedures we reviewed contained a requirement for service-level agreements to be included in technology contracts.

Because airport officials are not actively requiring or ensuring service-level agreements are included in vendor contracts, they lose the ability to control what they can measure.

Service-level agreements and objectives define the criteria for monitoring and measuring a vendor’s performance. For example, a typical objective vendors use is how often a service ought to be available, also called “uptime.”

Among our chosen sample of 20 information technology vendor contracts at the airport, we looked at how consistently Business Technologies includes service-level agreements and objectives in these types of contracts.

Of the 20 vendors we analyzed:

- Five, or 25%, had no evidence of a service-level agreement attached to the contract.
- Six, or 30%, had no evidence of service-level objectives attached to the contract.

We learned that when the airport develops a contract with a technology vendor, staff use a boilerplate contract template that includes general terms required in all contracts — such as pricing, invoicing, and terms regarding when the vendor gets paid. Once the airport and the vendor specify the work to be done, more details can be added to the contract.

When a vendor adds a service-level agreement to a contract, these
agreements are negotiated with the airport to ensure they do not conflict with the city’s general contract terms or other requirements. The airport itself has no boilerplate list of specific objectives that should be included in a service-level agreement for technology vendor contracts.

Business Technologies managers said how and to what extent they review vendor performance can vary. The process is decentralized, because each technology vendor contract is managed by different teams at the airport, which results in varying methods of measuring vendor performance. Therefore, how airport staff review service-level objectives depends on the team overseeing the contract.

Leading information technology practices say that, to hold vendors accountable, organizations should set guidelines for how they will measure vendor performance against relevant service-level agreements and metrics.\(^{37}\)

Not consistently having service-level agreements and measurable objectives in technology contracts prevents the airport’s Business Technologies division from holding its vendors accountable when service interruptions prevent a vendor from fulfilling its contracted scope of work. This lack of accountability risks damaging the airport’s reputation and risks the airport losing revenue if repeat incidents or recurring issues affect passenger travel or airport services.

The airport does not consistently document lessons learned after vendor incidents

Business Technologies is not consistently documenting what lessons it learns after a major incident occurs with a vendor-provided technology system or service. Additionally, staff are not documenting whether or how they review service-level objectives related to major incidents to ensure the airport recoups potential restitution it may be owed for a technology vendor’s failure to provide reliable service.

When the airport’s technology systems experience a service disruption, a formal incident has happened. Incidents are reported to the airport’s ServiceDesk team and documented in ServiceNow, the information technology system of record. The ServiceDesk team investigates the incident and coordinates the response. Smaller incidents are typically resolved by service owners, but the response to a “major” incident — one that has a high impact or potentially high impact on the airport — is coordinated by a major incident manager within Business Technologies itself.

When staff document an incident and describe any actions taken in response, they are supposed to use ServiceNow’s major incident workbench. This tool is also where post-incident actions should be documented to ensure an incident is fully resolved.

To determine how well airport Business Technologies is documenting its incident reviews in ServiceNow, we reviewed reports for each of the 17 major technology incidents that occurred at Denver International Airport from Jan. 1, 2022, through March 21, 2023. Of these 17 major incidents:

- None of the follow-up incident reports discussed any monitoring of service-level objectives.
- Only seven reports, or 41%, included documented lessons learned, but some of those were incomplete. Among those, only four — or 24% of the 17 — had complete incident lessons learned documented in ServiceNow.

The sample of 20 vendor contracts we chose to analyze for this audit included five vendors that had had a major incident sometime from Jan. 1, 2022, through March 21, 2023. Two of these vendors did not fulfill their service-level agreements for an incident, but we found no evidence that the airport collected either a remedy or restitution to the city, as was required in these vendors’ service-level agreements.

Instead, for one of the vendors, the airport decided to implement a service improvement plan rather than seek restitution from the vendor, even though the contract does not explicitly require them to do so. This demonstrates that the airport is not consistently following its contract requirements.

In our review of major airport incidents, we found that instead of consistently adding “specific actionable recommendations” to ServiceNow’s major incident workbench, airport employees often do not fill out such details.

Furthermore, the National Institute of Standards and Technology recommends that incident managers hold and document a lessons-learned meeting to find ways to prevent major incidents from occurring in the future.\(^{18}\) We found the airport’s major incident management policy does not require staff to hold such lessons-learned meetings.

Leading information technology practices recommend that organizations review major incidents to identify and document lessons learned, particularly in comparison to what service-level agreements and objectives required the vendor to do.\(^{19}\)

Without consistently documenting lessons learned and ensuring vendors comply with service-level objectives, the airport hampers its ability to identify and address recurring issues, prevent repeated incidents and service disruptions, and ensure the airport gets what it pays for from contracted technology vendors. Additionally, by not documenting these items in the system of record, staff may be unable to efficiently identify all relevant details in a centralized location.


\(^{19}\) National Institute of Standards and Technology, Special Publication 800-61 (Revision 2), 48.
1.8 RECOMMENDATION  Define and monitor service-level objectives

As part of implementing Recommendation 1.2, Denver International Airport’s Business Technologies division should:

- Ensure all technology contracts contain service-level agreements and specific service-level objectives for vendors to meet and that these service-level objectives are relevant, enforceable, and measurable.
- Refine and supplement procedures to ensure airport staff comprehensively and continuously monitor all technology vendors and verify that these vendors are meeting contract terms — including the requirements of their service-level agreements and objectives.
- Define and implement a process to seek restitution when vendors do not fulfill their agreed-upon service-level objectives, in accordance with their contracts.
- Include detailed information about service-level objectives in ServiceNow to support staff’s comprehensive and continuous monitoring.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JULY 1, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.

1.9 RECOMMENDATION  Update policy and procedures for vendor incidents

Denver International Airport’s Business Technologies division should revise its major incident management policy and any associated procedures to require staff to document lessons learned after each major incident to help prevent future events and to hold vendors accountable to service-level objectives agreed to in their service-level agreements. These lessons learned should be documented in ServiceNow, given it is the airport’s system of record for information technology.

AGENCY RESPONSE – AGREE, IMPLEMENTATION DATE – JAN. 2, 2024
SEE PAGE 19 TO READ THE AGENCY’S RESPONSES.
AGENCY RESPONSE TO AUDIT RECOMMENDATIONS

The following agency narratives are reprinted verbatim from the agency’s response letter.

RECOMMENDATION 1.1
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: JAN. 2, 2024

DEN Business Technologies agrees with the recommendation and will document an information technology vendor management strategic plan. The plan will address the objectives identified with this recommendation.

RECOMMENDATION 1.2
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: APRIL 1, 2024

DEN Business Technologies agrees with the recommendation and will finalize the draft vendor management policy, and upon approval, publish and communicate the policy for all DEN departments to utilize by the date indicated with this recommendation. In addition, procedures will be developed, published, and communicated for vendor management life cycle activities by 07/01/24.

RECOMMENDATION 1.3
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: JULY 1, 2024

DEN Business Technologies agrees with the recommendation and will refine policies and procedures to clarify to airport personnel that all technology procurement requires timely engagement, review, and approval from Business Technologies.
RECOMMENDATION 1.4
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: APRIL 1, 2024
DEN Business Technologies agrees with the recommendation and will develop, approve, and document a vendor termination process to provide consistent standards to address the objectives identified with this recommendation.

RECOMMENDATION 1.5
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: JUNE 3, 2024
DEN Business Technologies agrees with the recommendation and will redesign, implement, and document our vendor security review processes. Successful implementation of this plan is dependent on the completion of the vendor risk management module implementation to appropriately categorize the criticality of the vendor.

RECOMMENDATION 1.6
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: JAN. 2, 2024
DEN Business Technologies agrees with the recommendation and will develop an information technology vendor management training plan. Development of the training plan will be conducted during the remediation of Recommendation 1.1 and will ensure appropriate staff receive and understand their roles and responsibilities with information technology vendor management life cycle activities.

RECOMMENDATION 1.7
AGENCY RESPONSE: AGREE
AGENCY’S TARGET DATE FOR IMPLEMENTATION: APRIL 1, 2024
DEN Business Technologies agrees with the recommendation and will continue efforts to complete the implementation of vendor risk management in ServiceNow. The technology implementation is estimated to be completed by 01/02/23.

Business Technologies is adopting a phased plan to implementing risk management for vendors. During this process Business Technologies will prioritize the completeness, and accuracy of vendor data for the vendors providing services to DEN that are categorized as “Critical”, followed by vendors managed by Business Technologies that provide services categorized as “High” by 04/01/24.

The priority for ensuring completeness and accuracy for vendor services provided to other DEN divisions and Business Technologies vendors providing services categorized as “Medium” and “Low” will be determined after those efforts conclude.

In addition, the phased plan will develop policy, procedure, and process as necessary to ensure that vendor information is updated to ensure completeness and accuracy of data.
RECOMMENDATION 1.8

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: JULY 1, 2024

DEN Business Technologies agrees with the recommendation and will create and publish service-level agreement and objective standards. Further, we will work with DEN Legal to incorporate these standard service-level agreements and service-level objectives into technology contracts.

Procedures will also be developed, and appropriate staff will be trained on monitoring vendors to address the objectives identified with this recommendation.

In addition, we will consider options for a tool, like ServiceNow, to assist staff with monitoring service-level objectives.

RECOMMENDATION 1.9

AGENCY RESPONSE: AGREE

AGENCY’S TARGET DATE FOR IMPLEMENTATION: JAN. 2, 2024

DEN Business Technologies agrees with the recommendation and will update the policy and procedures for vendor incidents. These updates will include the Business Technologies Major Incident Management process documents, which will include additional requirements when documenting lessons learned in the post incident report in ServiceNow.
OBJECTIVE

To assess how effective Business Technologies processes are for information technology vendor management governance and for ensuring continuous monitoring of information technology vendors.

SCOPE

We focused our audit on vendors managed by the Business Technologies division at Denver International Airport. The information technology vendors within our scope included those for applications, software as a service, and professional services such as software reselling.

Our audit did not include other third-party vendors or contractors at the airport — such as concessions vendors or vendors that provide hardware like laptops, networking equipment, internet-connected devices, or off-the-shelf small software solutions.

We reviewed Business Technologies’ data, processes, and future planning efforts from Jan. 1, 2021, through June 30, 2023.

METHODOLOGY

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

- Reviewing city regulations and researching leading practices, including the city’s annual budgets, the city's Executive Order No. 18, and Technology Services' vendor management policy.
- Evaluating the scope of vendor risk assessments conducted by Business Technologies and airport operations.
- Interviewing key Business Technologies and airport operations officials, managers, and staff about the airport's information technology vendor management life cycle processes.
- Reviewing and assessing Business Technologies’ policies and procedures for vendor management life cycle activities.
- Reviewing and assessing contracts and service-level agreements for sufficient language regarding service-level objectives and monitoring a vendor’s performance.
• Evaluating the scope of initial and periodic risk assessments for vendors as well as vendor security reviews conducted by Business Technologies.

• Testing the completeness and accuracy of Business Technologies’ vendor and service inventory lists and collected vendor information.

• Interviewing both Business Technologies and Technology Services staff about the city’s Executive Order No. 18 and Technology Services’ information technology vendor management policy.

• Using our professional judgment to sample and analyze 20 top-tier information technology vendors to assess whether evidence exists to show:
  • An initial risk assessment and periodic risk assessments were done.
  • A vendor manager was assigned and was an active Business Technologies employee.
  • Contracts included service-level agreements and service-level objectives.
  • Staff reviewed critical incidents that occurred for a vendor and whether these incidents were measured against service-level agreements and objectives.
Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the residents of Denver. He is responsible for examining and evaluating the operations of city agencies and contractors for the purpose of ensuring the proper and efficient use of city resources. He also provides other audit services and information to City Council, the mayor, and the public to improve all aspects of Denver's government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the city's finances and operations, including the reliability of the city's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of city operations, thereby enhancing residents' confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue, #705
Denver, CO 80202
(720) 913-5000
www.DenverAuditor.org

Our Mission

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