

# AUDIT REPORT

## Denver Zoo Conservation Alliance ***Outdated Infrastructure***

JULY 2025



**TIMOTHY M. O'BRIEN, CPA**  
DENVER AUDITOR

**OFFICE OF THE AUDITOR**  
AUDIT SERVICES DIVISION,  
CITY AND COUNTY  
OF DENVER

## Audit Team

Peter Ulrich, CISA, CSX-A, Information Systems Audit Manager

Nicholas Jimroglou, CISA, CDPSA, Information Systems Audit Lead

Dave Hancock, CISA, CISM, MURP, Information System Audit Senior

## Other Contributors

Stelios Pavlou, Senior Communication and Reporting Specialist

Manda Troutman, Communication and Reporting Specialist

Jeff Neumann, Graphics and Visual Information Specialist

## Audit Managers

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

Reed Hatch

Frank Rowe

Leslie Mitchell

Florine Nath

Edward Scholz

**You can obtain  
copies of this  
report by  
contacting us.**



### **Office of the Auditor**

201 West Colfax Ave. #705  
Denver, CO 80202  
(720) 913-5000

Or download and view  
an electronic copy by  
visiting our website at:  
[www.DenverAuditor.org](http://www.DenverAuditor.org).

*Agency responses are unedited and taken directly from the agency's letter, which is available on our website.*

*Cover photo illustration by Denver Auditor's Office staff.*

# City and County of Denver



**TIMOTHY M. O'BRIEN, CPA**  
AUDITOR

201 West Colfax Ave. #705, Denver, CO 80202  
(720) 913-5000 | [www.DenverAuditor.org](http://www.DenverAuditor.org)

## AUDITOR'S LETTER

July 17, 2025

We audited the outdated infrastructure processes performed by the Denver Zoo Conservation Alliance to assess whether it is effectively managing the risks of outdated infrastructure. I now present the results of this audit. In addition, we audited three other city agencies. Due to their sensitive nature, our findings are confidential and were communicated to the relevant agencies separately.

The audit found the Denver Zoo Conservation Alliance is effectively managing the risk of outdated infrastructure in its technology environment and had minor process and policy enhancements to make to improve its processes and reduce the risk to a low level.

By implementing recommendations for stronger processes and policies, the Denver Zoo Conservation Alliance will be better able to identify and manage the risks of outdated infrastructure.

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 the Denver Zoo Conservation Alliance who shared its time and knowledge with us during the audit. Please contact me at 720-913-5000 with any questions.

Denver Auditor's Office

A handwritten signature in black ink, appearing to read "Timothy M. O'Brien".

Timothy M. O'Brien, CPA  
Auditor



# HIGHLIGHTS

## Outdated Infrastructure

JULY 2025

### Key facts

- The Denver Zoo Conservation Alliance’s Information Technology team provides IT support and services to an 80-acre campus with over 2,500 animals, almost 400 staff, 600 volunteers, the board of governors, the leadership council, and nearly two million visitors a year.
- In October 2024, US News and World Report ranked the Denver Zoo in the top 27 zoos in the United States.
- The Denver Zoo received accreditation from the Association of Zoos and Aquariums — setting it apart as one of only 238 institutions in the world to achieve the certification.
- The 22,000-sq.-ft. Helen and Arthur E. Johnson Animal Hospital was honored by the Association of Zoos and Aquariums with a 2023 significant achievement in facilities award.

**The Denver Zoo Conservation Alliance agreed with all recommendations**

### What we found

- **THE DENVER ZOO CONSERVATION ALLIANCE’S IT TEAM TRACKED AND MONITORED ITS IT EQUIPMENT INVENTORY.** Additionally the zoo identified IT equipment needing replacement before it reached its end of life.
- **THE ZOO REPLACED OLDER EQUIPMENT AS NEEDED OR APPROPRIATELY MANAGED THE LIMITED USE OF OUTDATED TECHNOLOGY EQUIPMENT.**
- **REFINEMENTS IN PROCESSES ARE NEEDED TO IMPROVE THE DOCUMENTATION OF TRACKED IT EQUIPMENT.** The risk associated with the use of outdated infrastructure needs to be documented and the IT database inventory should be reconciled with the IT management software inventory.
- **THE ZOO’S IT TEAM SHOULD UPDATE ITS RISK ACCEPTANCE PROCEDURES.** A documented process to ensure risk acceptance is appropriately approved is needed. Documented processes will ensure the decisions are aligned with policy and risk tolerance.

### Why we did this audit

We completed a risk assessment of technology in several city agencies, resulting in this planned audit. This audit assessed the zoo’s management of technology approaching or having reached the end of its life — including examining the zoo’s strategies for outdated technology management and evaluating the timing and extent to which systems were maintained to reduce the risk of outdated technology.

### Why it matters

IT hardware and software needs updating to help organizations innovate and use technology to better serve its stakeholders.

When vendors stop supporting the product, the product is not provided with security updates or spare parts, which may allow bad actors to perform cyberattacks.

# CONTENTS

<b>BACKGROUND</b>	<b>1</b>
<b>FINDING AND RECOMMENDATIONS</b>	<b>6</b>
<b>The Denver Zoo Conservation Alliance is managing the risk of outdated infrastructure, but processes can be improved</b>	
The Denver Zoo Conservation Alliance is tracking and monitoring its IT equipment, but inventory processes can be improved .....	<b>10</b>
The Denver Zoo Conservation Alliance should update the process for how the risk of outdated infrastructure is accepted .....	<b>11</b>
<b>OBJECTIVE, SCOPE, AND METHODOLOGY</b>	<b>14</b>

---

# BACKGROUND

According to Kyndryl, a leading IT consulting and infrastructure services provider, in “Navigating the readiness paradox: The Kyndryl Readiness Report 2024,” 90% of business leaders are confident their Information Technology infrastructure is best in class. However, the report highlights only 39% of those leaders believe their IT infrastructure is ready for the future and 64% believe they have outdated or near end-of-life IT equipment. In addition, 44% of business leaders’ hardware and operating systems are near or at end of life. This demonstrates many leaders have significant concerns about the way their organizations are managing the IT equipment life cycle and specifically the end of life of these assets. Leaders have significant control over effectively managing end-of-life assets as they can either fund or not fund the replacement and modernization of end-of-life assets and demand effective reporting of their IT equipment.

The terms “end of life” and “outdated” when describing infrastructure mean the same thing and will be used interchangeably throughout the report.

## END OF LIFE

**Cisco, a leader in IT equipment and software, defines “end of life” as, “A process that guides the final business operations associated with the product life cycle. The end-of-life process consists of a series of technical and business milestones and activities that, once completed, make a product obsolete. Once obsolete, the product is not sold, manufactured, improved, repaired, maintained, or supported.”**

## Outdated infrastructure risks

Outdated infrastructure in IT equipment and software poses several risks such as weak security, loss of innovation, and wasted productivity. These risks can be reduced by replacing outdated infrastructure or implementing complimentary controls to reduce the risk to an acceptable level for the organization.

**SECURITY** – According to the “2024 Verizon Data Breach Investigations Report,” exploiting vulnerabilities from outdated infrastructure was the third most used attack method used in 2024, which represented a 180% increase from 2023. When the vendor determines its products will be deemed “end of life,” it also stops looking for security vulnerabilities in its products and providing solutions for these security vulnerabilities to its clients. The products may have vulnerabilities that could be used by a bad actor to take over a product and gain access to systems and to potentially perform a ransomware attack, compromise systems, or steal data. As the average cost of a breach is \$4.88 million, according to IBM’s “Cost of a Data

*Investments and continual processes to assess and replace outdated technology should be used to prevent the buildup of old technology that limit innovation.*

Breach Report 2024,” many organizations may find it cheaper and better for the people it serves to replace end-of-life products than to live with the risk of outdated infrastructure.

**INNOVATION** – Many leaders, including the mayor, are looking to technology to help solve problems facing agencies. But older technology may not be optimized for using new technology such as artificial intelligence. According to a survey performed by NTT DATA, a global technology infrastructure and services provider, 86% of organizations agree that inadequate or outdated technology hinders organizational progress and innovation efforts. The same survey noted 94% of C-suite executives believe outdated infrastructure limits their business agility. Investments and continual processes to assess and replace outdated technology should be used to prevent the buildup of old technology that limit innovation. Technology costs increase over time and the longer organizations do not fund replacements, less innovation occurs and the more expensive the replacements become.

**INCREASED MAINTENANCE AND LOSS OF PRODUCTIVITY** – Postponing unavoidable outdated infrastructure replacements can result in unstable systems that require emergency actions to restore services. A study by Gartner, a research and advisory firm, shows when IT systems are not working it may cost organizations anywhere from \$5,600 to \$9,000 per minute depending on the industry. Frequent disruptions can reduce city residents satisfaction and damage its reputation.

A survey from Forrester, a leading global research and advisory firm, found about 60% of chief technology officers believe outdated infrastructure is too costly to maintain. Additionally, research performed by Atera, an AI IT software provider and consulting firm, also found that about 80% of companies’ IT budgets is spent keeping old IT systems afloat and 40% of IT leaders regret their legacy technology purchases.

Maintaining outdated infrastructure leads to wasted effort and lower efficiency. For example, a study by Moldstud, a research firm specializing in IT consulting and development, found outdated infrastructure maintenance leads to more than three hours per day of wasted effort by employees. Gartner, also, found a 25% lower efficiency rate in organizations that employ outdated technology and infrastructure.

The cost of not replacing outdated infrastructure likely outweighs the cost of modernizing the hardware. Productivity, innovation, and security are all improved when outdated infrastructure is replaced — providing the return on investment leaders are searching for in their organizations. Outdated infrastructure is another form of debt organizations need to address to remain healthy and viable.

## **Relevant frameworks and standards to outdated infrastructure**

There are established standards and frameworks for managing outdated infrastructure in technology, such as those provided by the National Institute of Standards and Technology, the Payment Card Industry Security Standards Council’s “Payment Card Industry Data Security Standards 4.0,” and the Center for Internet Security’s “CIS Critical Security Controls Version

8.1.” These standards and frameworks help organizations mitigate risks, increase IT security, and optimize IT infrastructure performance.

### **NIST Special Publication 800-53A Revision 5**

The National Institute of Standards and Technology’s “NIST Special Publication 800-53A Revision 5 — Assessing Security and Privacy Controls in Information Systems and Organizations” provides guidance for organizations to manage end-of-life infrastructure in SA-22. SA-22 defines two controls:

1. “Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or”
2. “Provide the following options for alternative sources for continued support for unsupported components using in-house support, or support from an external party.”

The discussion of the two controls provides examples of support such as updates, patches, maintenance contracts, and replacement parts. This support would be developed without the assistance of the original vendor, making the process more difficult. The standard discusses other mitigating controls such as isolation, microsegmentation, or dedicated networks as actions for organizations to take to reduce risk to an acceptable level. The standard provides exceptions for replacing mission critical systems when there is a lack of new technology, or replacement is technically infeasible. While these exceptions exist, the need for complimentary controls is not reduced and regular risk reviews are necessary to ensure new technology is not available to replace end-of-life equipment.

### **Payment Card Industry Data Security Standards 4.0**

As of March 31, 2025, “Payment Card Industry Data Security Standards 4.0” requires organizations to review in-scope hardware and software every 12 months. The requirements list four items for organizations to perform during the 12-month review,

“including at least the following:

1. Analysis that the technologies continue to receive security fixes from vendors promptly.
2. Analysis that the technologies continue to support and do not prevent the entity’s PCI DSS compliance.
3. Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced end-of-life plans for a technology.
4. Documentation of a plan, approved by senior managers, to remediate outdated technologies, including those for which vendors have announced end-of-life plans.”

The “Payment Card Industry Data Security Standards 4.0” also contains a customizable control approach objective and says: “The entity’s hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.”

These controls enhance the controls described by “NIST Special Publication 800-53A Revision 5” by requiring the organization to document vendor announcements for end of life, which creates a requirement to monitor the vendors. In addition, it creates a requirement for a plan to be documented and approved by senior managers for managing end-of-life infrastructure. When reviewing these criteria, we recognize that these controls are only required for “Payment Card Industry Data Security Standards 4.0” in-scope systems. However, we believe it may be easier to develop an organizationwide process at the organizational level versus a compliance-specific process.

### **The Center for Internet Security**

The Center for Internet Security created the “CIS Critical Security Controls Version 8.1,” which was published in August 2024. This provides further descriptions of controls needed for outdated infrastructure processes, enhancing the controls listed in “NIST Special Publication 800-53A Revision 5” and “Payment Card Industry Data Security Standards 4.0.” Control 1 highlights the need for inventory and control of organizationwide assets processes and controls for an organization and describes the controls and safeguards to implement. Safeguard 1.1, a part of Control 1, describes the controls and rationale for establishing and maintaining a complete and accurate organization equipment inventory.

Control 2 highlights the need for software inventory processes and controls for an organization and describes the safeguards to implement. Safeguard 2.2 requires an organization to ensure supported software is in the software inventory as authorized and describes steps the organization should take to restrict the software or ensure mitigating controls are in place and the risk is accepted. Safeguard 2.3 requires an organization to either remove the software or have a documented exception that is reviewed, at a minimum, monthly.

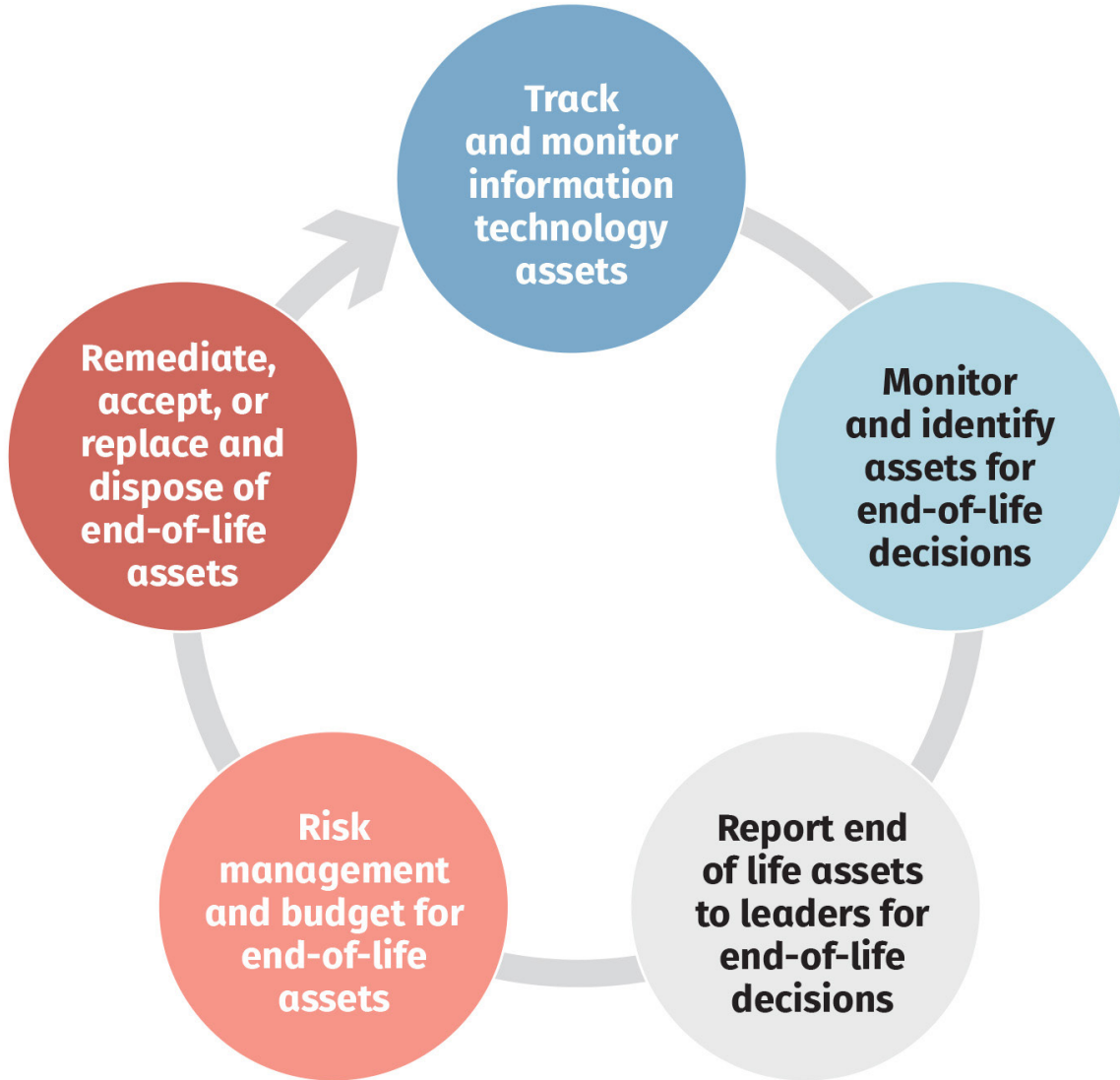
Controls 1 and Control 2 are similar, but Control 1 pertains to hardware and Control 2 pertains to software. These standards help create more clarity on the necessary processes and controls needed to effectively manage end-of-life or outdated infrastructure.

These multiple standards support the case that organizations should have well-developed plans and risk strategies for reducing its risk exposure to outdated infrastructure and technology.

## End-of-life process design

Based on the analysis of the standards, we developed Figure 1 to show the circular nature of the end-of-life process and the high-level process flow for managing outdated infrastructure.

**FIGURE 1.** End-of-life IT asset risk management process



**Source:** Developed by the Auditor’s Office staff based on “NIST Special Publication 800-53A Revision 5,” “Payment Card Industry Data Security Standards 4.0,” and “CIS Critical Security Controls Version 8.1.”

---

## FINDING AND RECOMMENDATIONS

### ***The Denver Zoo Conservation Alliance is managing the risk of outdated infrastructure, but processes can be improved***

The Denver Zoo Conservation Alliance’s Information Technology team is proactively identifying, reporting, budgeting, and replacing its outdated infrastructure and is committed to providing IT users a secure and modern IT environment to allow the zoo to innovate. To do so, it is tracking and monitoring its inventory, identifying IT equipment before it has reached end of life, reporting end-of-life equipment to leaders through its budgeting process, replacing older equipment as needed, and properly disposing of the equipment.

The zoo’s effective management of outdated infrastructure can be attributed to a professional culture where the IT team communicates its needs through the zoo’s leaders and to the board of governors. The board of governors approves the budget and provides sufficient funding to replace outdated infrastructure based on requests from leaders. The bottom-up flow of information as well as the tone at the top sets an example for other city agencies.

Replacing IT equipment before it has reached end of life increases the security and operational efficiency of IT operations, while providing the opportunity for the zoo to innovate on technology that is supported by the vendor. To ensure the risks posed by outdated infrastructure are reduced to an acceptable level, the Denver Zoo Conservation Alliance’s IT team works closely with its leaders to report outdated infrastructure so it can budget appropriately for end-of-life equipment before outdated infrastructure becomes too expensive.

Although we found that the Denver Zoo Conservation Alliance proactively monitors and identifies IT equipment that is approaching end of life, we also found some areas of improvement. We found:

- It is tracking and monitoring its IT equipment; however, the completeness and accuracy of the IT equipment inventory can be improved.
- Its IT asset policy needs updating to define outdated infrastructure and its risk acceptance procedures.

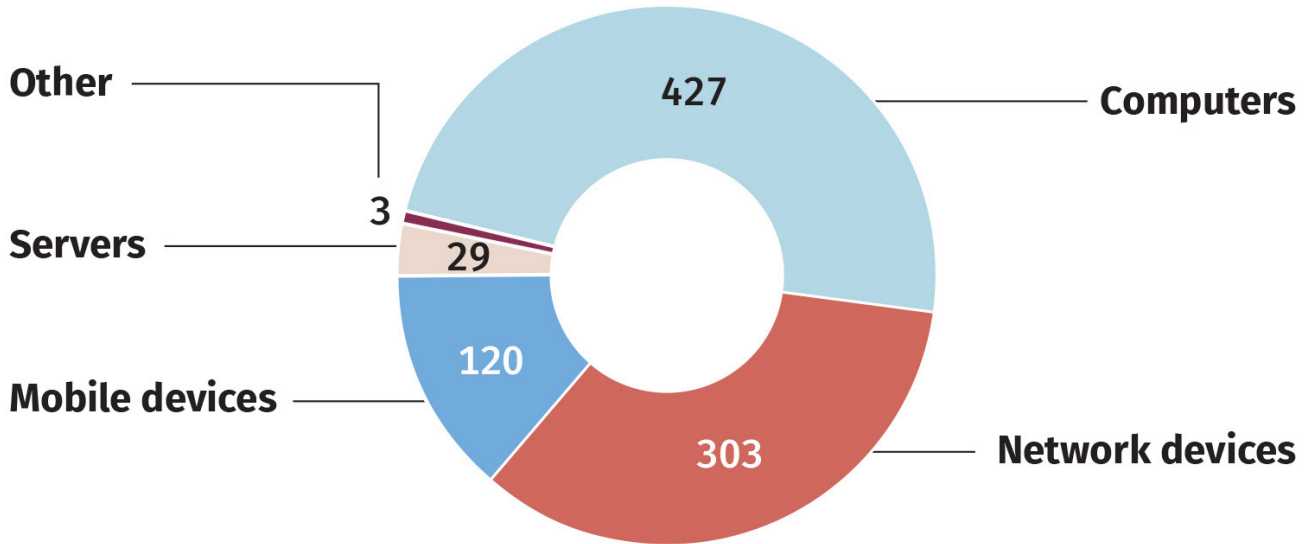
#### **Analysis of IT equipment**

We found the zoo has 882 pieces of IT equipment comprising computers, mobile devices, network equipment, servers, and other IT devices. The 427 “Computers,” laptops and desktop computers, are used by employees for the day-to-day operations at the Denver Zoo Conservation Alliance. The 120 “Mobile devices” are used for multiple purposes, such as scanning

*Replacing IT equipment before it has reached end of life increases the security and operational efficiency of IT operations, while providing the opportunity for the zoo to innovate on technology that is supported by the vendor.*

tickets to enter the zoo and to record animal behavior as part of animal studies. There are 303 “Network devices” and 29 “Servers” that make up the infrastructure and backend of the Denver Zoo Conservation Alliance’s operations. There are three “Other” pieces of IT equipment that do not fall into any of these categories. See Figure 2 for a breakdown of the IT equipment as described.

**FIGURE 2. Population of IT equipment at the Denver Zoo Conservation Alliance**



*Source: Created by Auditor’s Office staff.*

*The zoo has reduced the risk exposure to security vulnerabilities and wasted productivity while increasing the potential for innovation.*

We examined the Denver Zoo Conservation Alliance’s IT equipment for end-of-life IT equipment and found 13 instances of outdated infrastructure or 1.3% of the total IT equipment. The 13 items were being appropriately risk managed and the uses were low risk or were appropriately controlled. For example, the IT team has a set of outdated switches that are powered off and not used unless the zoo’s primary and secondary systems fail. The risk of these switches needing to be used is low and if it were needed, it would only operate until the primary or secondary systems are brought back online.

Because the Denver Zoo Conservation Alliance is identifying IT equipment that is reaching end of life and replacing the equipment before it reaches end of life, it has reduced the risk exposure to security vulnerabilities and wasted productivity while increasing the potential for innovation.

Figure 3 on the next page, shows the breakdown of outdated infrastructure by type of IT equipment.

**FIGURE 3. Population of IT supported and unsupported equipment at the Denver Zoo Conservation Alliance**

	CURRENTLY SUPPORTED	AT END OF LIFE
Operating systems	531	2
Mobile devices	117	3
Network equipment	300	3
Servers	24	5
Other	3	

Source: Created by Auditor's Office staff.

**OPERATING SYSTEMS** – The Denver Zoo Conservation Alliance maintains operating systems on hardware where it is needed to make the equipment usable. For example, a computer or mobile device needs an associated operating system like Windows, Android, or Apple iOS to provide security and allow the applications to be used.

Because the operating system is one component that safeguards a computer, mobile device, or server from vulnerabilities, the IT team focuses on maintaining operating systems by ensuring they are up to date and supported by the vendor. To ensure all computers, mobile devices, and servers are receiving the latest operating system, software is installed on the equipment that communicates with computer management programs the IT team uses to monitor the operating system version.

We found 531 of the 533 operating systems being used are still supported by the vendor and receiving security updates. The two operating systems that are not supported by the vendor are installed on computer equipment that are powered off and ready to be disposed of. This greatly reduces risk as the computers would need to be powered on for the computers to be compromised.

**COMPUTERS** – The IT team replaces a computer every five years – when the computer can no longer operate a supported operating system or as needed to support operational needs. This helps ensure the computer can support the latest operating systems and receive the critical security updates to the operating system from the vendor.

As computers approach end of life, the Denver Zoo Conservation Alliance is assessing the risk for its IT equipment and is making proactive business decisions to reduce risk by replacing the equipment. For example, at the time of testing, the Denver Zoo Conservation Alliance had about 100 Windows 10 operating systems running in its environment. Microsoft has

announced that Windows 10 will reach end of support on Oct. 14, 2025. The zoo's IT team is taking a proactive approach to upgrading these computers before this date. It has already upgraded an additional 293 computer operating systems to Windows 11 as of March 2025.

**MOBILE DEVICES** – Mobile devices are also replaced every five years to ensure devices support the latest operating systems and receive the critical security updates from the vendor. We found that 117 of 120 mobile devices are still within the five-year period and have a supported operating system that is receiving security updates.

Because the zoo's IT team replaces mobile devices every five years, it has plans to replace the remaining three of its 120 mobile devices to ensure they are supporting the latest operating systems and receiving critical security updates from the vendor. In addition, the zoo's IT team said these outdated mobile devices were used in animal studies and are not used for any critical operations. The animal studies consist of a volunteer using a web-based application to observe and document animal behavior using the mobile device. The risk is further reduced as these mobile devices are usually powered off when not being actively used in an animal study.

**NETWORK EQUIPMENT** – We found 300 of 303 pieces of network equipment are still supported by the vendor and receive security updates. As these approach end of life, the zoo's IT team is managing the risk by replacing the equipment as needed. The remaining three of the 303 pieces of network equipment are not connected to the network, remote access is disabled, and the equipment is powered off reducing the risk of the equipment becoming compromised. The equipment is used for testing and are backups in case of a failure to a piece of network equipment actively in use.

**SERVERS** – We found that 24 of the 29 servers at the zoo are virtual servers running on supported hardware and have the latest operating systems installed to ensure it is receiving critical security updates from the vendor. The remaining five of the 29 servers have reached end of life, but are powered off and only used as a tertiary – or third in line – disaster recovery backup solution to continue operations in the event of a disruption to the primary and secondary systems. If the primary server has a problem and is not available, a secondary backup server takes over to ensure the IT service provided by the primary server is available to help keep operations running.

In the unlikely event both the primary and secondary servers have problems and are not available, the zoo's IT team can use these outdated servers to keep IT operations running. The need for this tertiary backup server is low as it is unlikely that both the primary servers and secondary backup servers would go offline at the same time. Additionally, the zoo's IT team has plans to replace these tertiary servers in 2026.

**OTHER IT EQUIPMENT** – We found that all three miscellaneous equipment that falls under the "Other" category are still supported by the vendor and are receiving critical security updates as needed.

**The Denver Zoo Conservation Alliance is tracking and monitoring its IT equipment, but inventory processes can be improved**

The “Center for Internet Security Control 1, Inventory and Control of Enterprise Assets,” describes actions an organization can take to manage its IT equipment. The control requires an organization to inventory, track, and correct all hardware equipment connected to a network to accurately know all equipment that needs to be monitored and protected.

**POSITIVE EFFORTS**



While it is difficult to have a 100% complete and accurate inventory, the Denver Zoo Conservation Alliance’s process for managing its inventory is appropriately designed and effective.

To determine whether the Denver Zoo Conservation Alliance’s inventory is accurate, we tested a sample of 25 pieces of equipment to determine whether the items listed in its inventory are physically present at the location listed in the inventory. We visited the Denver Zoo Conservation Alliance and were able to locate all 25 samples we selected from its inventory records at various locations around the zoo.

In addition, we tested the IT equipment inventory completeness by judgmentally selecting 25 pieces of IT equipment during our site visit and verified the 25 pieces of IT equipment existed in the IT inventory. We found one of the 25 samples we selected did not have a corresponding record in its inventory. This was a mobile device that did not have the required software to communicate with the management software.

To assist the zoo’s IT team in inventorying and tracking, it implemented computer management software and installed the software on most of the zoo’s computers and mobile devices. The software allows the IT team to communicate with computers and mobile devices through the management software, which allows it to track and monitor the devices for items such as outdated operating systems. This process is about three years old and appears to have contributed to the success of the zoo’s inventory management.

During discussions with the IT team, we determined the device was purchased before the management software implementation and never had the management software installed. Before the management software implementation, the IT team relied on a manual database. The zoo continues to update the manual database when IT equipment is purchased. This assists in the financial recording of IT equipment.

We reviewed the database and determined there are 25 pieces of IT equipment recorded that do not have the required software to communicate with the management software. When the Denver Zoo purchased its management software, it did not perform a reconciliation between the purchased equipment database and the management software listing to ensure all devices that were purchased had the required management software installed. This prevented the zoo from monitoring and tracking the equipment using the management software. The IT team

*Maintaining a complete and accurate inventory is essential to ensure outdated infrastructure is updated.*

is working to locate these pieces of IT equipment to either install the management software or retire the device, but it is a difficult process given the 80-acre campus with a small IT team of three individuals and with the mobile device being powered off.

Maintaining a complete and accurate inventory is essential to ensure outdated infrastructure is updated. Without a complete and accurate inventory, it is difficult to manage what exists in the environment and can result in IT equipment at end of life that may contain security vulnerabilities, decrease productivity, and limit innovation.

## 1.1

### RECOMMENDATION

### Reconcile information technology equipment with inventory

**The Denver Zoo Conservation Alliance should perform a reconciliation of its IT equipment database with its IT equipment management software records. Then decide whether any equipment not currently being managed should be retired or have the software installed – allowing it to be tracked by the management software.**

#### AGENCY RESPONSE – AGREE

*We agree with the recommendation and are conducting a comprehensive audit of all legacy hardware to ensure enrollment in our endpoint management system. Devices found to be incompatible with our endpoint management system will be replaced. This process will be completed by September 30, 2025*

— Denver Zoo Conservation Alliance

IMPLEMENTATION EXPECTED BY SEPT. 30, 2025

### **The Denver Zoo Conservation Alliance should update the process for how the risk of outdated infrastructure is accepted**

According to the “NIST Special Publication 800-53 revision 5,” organizations should replace system components when support is no longer available from the vendor. In addition, it says organizations should reduce the unsupported system components risk by implementing complementary controls. This should be documented and shared with the relevant stakeholders involved with the process.

The Denver Zoo Conservation Alliance has an IT asset policy that provides guidance on identifying, tracking, maintaining, and disposing of IT equipment. When we reviewed the policy, we found it does not define what would constitute support no longer being available from a vendor. This definition would initiate a replacement. For example, some of the laptop computers used by the zoo are no longer supported by the vendor, specifically the firmware and drivers that are not being updated.

The zoo's IT team said that if a computer can use a supported operating system and the needed applications run on the computer, then it does not consider this device end of life unless it is older than five years. We agreed with this stance. But this practice is not documented in any zoo policy and relies on the staff's institutional knowledge. By not defining outdated equipment, there is the potential for employees to act — or not act — when their understanding of what is outdated infrastructure differs from what managers understand.

#### FIRMWARE

**IBM defines firmware as, "software for hardware." It is program code embedded in a hardware device that enables it and its features to properly function.**

#### DRIVERS

**Microsoft defines drivers as, "a software component that lets the operating system and a device communicate."**

*The zoo's policy does not include guidance on how the risk is accepted for outdated infrastructure that remains in use.*

Additionally, the zoo's policy does not include guidance on how the risk is accepted for outdated infrastructure that remains in use. For example, the mobile devices that are used in animal studies are older than five years. The zoo's IT leader has accepted the risk of continuing to use these devices for this particular use case and knew about these devices without needing to do any research. However, there was no supporting documentation or any documented process to ensure the risk accepted was appropriately approved and documented to ensure the decision aligned with policy and risk tolerance.

Because the zoo's IT team is small, it may not require the same level of documented policies as a larger more complex organization. Direct manager oversight may provide a suitable substitution. However, we believe these definitions will help improve consistency in the process and prevent knowledge loss in the event of staff turnover. Should any of the staff abruptly leave without a documented policy to provide guidance on what outdated infrastructure is, and how the risk is accepted for continued use, there is a risk that knowledge will be lost because it is not documented. This may result in a lack of consistency in the process.

**1.2**

**RECOMMENDATION**

**Update policies and procedures**

**The Denver Zoo Conservation Alliance should update its policy by documenting the definition of what outdated infrastructure is and how the risk is accepted and documented for outdated infrastructure to reduce the risk of knowledge loss from staff turnover.**

**AGENCY RESPONSE – AGREE**

*We agree with the recommendation and will revise our policies to accurately reflect current operational processes. This includes updates to policies governing our hardware refresh cycle and the management of devices that have reached end-of-manufacturer support, including the acceptable level of associated risk. These updates will ensure policies align with our processes moving forward*

**— Denver Zoo Conservation Alliance**

**IMPLEMENTATION EXPECTED BY SEPT. 1, 2025**

---

---

# OBJECTIVE, SCOPE, AND METHODOLOGY

## **Objective**

To assess technology that is approaching or has reached the end of its useful life at the zoo and at other agencies. This includes assessing the city's proactive strategies and planning and evaluating to what extent city systems are patched and updated in a timely manner.

## **Scope**

We assessed the effectiveness of the Denver Zoo Conservation Alliance's processes for managing outdated infrastructure from Jan. 1, 2023, through March 31, 2025.

## **Methodology**

To accomplish our audit objectives, we:

- Interviewed staff at the Denver Zoo Conservation Alliance.
- Conducted on-site walkthroughs of the Denver Zoo's campus and observed IT equipment, such as laptops, servers, network switches, routers, and wireless access points.
- Reviewed applicable laws, ordinances, and executive orders; rules and regulations; fiscal rules; and policies and procedures.
- Analyzed agencies' mission statements, strategic plans, organizational charts, annual budgets, expenses, annual reports, and management plans.
- Reviewed policies and procedures and system generated reports.
- Reviewed leading practices from the National Institute of Standards and Technology, Payment Card Industry Data Security Standards Council, and the Center for Internet Security.
- Analyzed and observed statistical and judgmental samples of IT equipment for completeness and existence.
- Performed data analysis to determine whether the IT equipment inventory contained the required fields for outdated infrastructure processes.
- Analyzed IT equipment to determine whether the equipment was supported by the vendor and not consider outdated or end of life.
- Examined risk treatments for existing outdated infrastructure for appropriate risk treatments.
- Examined the outdated infrastructure reporting process to determine whether it was sufficient based on the current risk to the organization.
- Examined and observed the IT equipment disposal process to ensure the process properly disposed of IT equipment.

---

## 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](http://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.

---