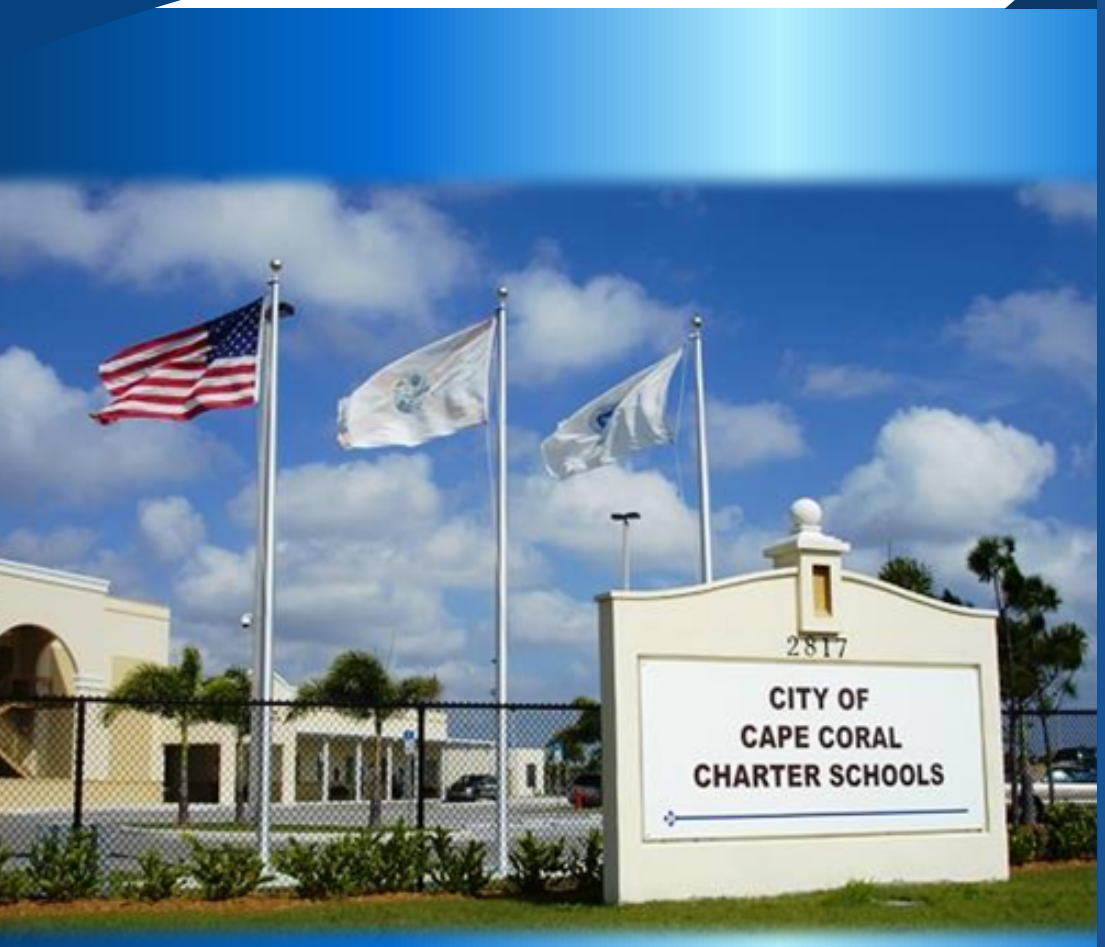


Report Issued

May 5, 2026

Audit Report No. 26-03

City of Cape Coral
City Auditor's Office

P.O. Box 150027
Cape Coral, FL 33915-0027
239-242-3383

Charter School Authority Information Technology Services Audit

Auditor In Charge: Timothy DiSano, CIA, CISA, CFE

Auditors: Joseph Devone, CIA
Jeremy Cullen, MBA

TO: Mayor Gunter and Council Members

FROM: Andrea R. Russell, City Auditor

DATE: May 5, 2026

SUBJECT: 26-03 Charter School Authority Information Technology Services Audit

The City Auditor's Office conducted a performance audit of information technology services provided to the Oasis Charter Schools by the Information Technology Services Department. This audit is included in the City Auditor's FY26 approved Audit Plan. The audit was conducted in conformance with Generally Accepted Government Auditing Standards by the authority granted through City Ordinances 28-02 and 79-10.

We would like to express our sincere appreciation to the Charter School Authority and Information Technology Services Department management and staff for the courtesy, cooperation, and proactive attitude extended to the team members during the audit. If you have any questions or comments regarding this audit, please contact Andrea Russell at 242-3380 or Timothy DiSano at 242-3308.

C: Michael Ilczyszyn, City Manager
Connie Barron, Assistant City Manager
Mark Mason, Assistant City Manger
Aleksandr Boksner, City Attorney
Kimberly Bruns, City Clerk
Ian Hyatt, ITS Director
Jacquelin Collins, Superintendent, Oasis Charter Schools
Matthew Vilord, Deputy ITS Director
Sarah Evins, Special Projects Coordinator
Kristifer Jackson, CSA Governing Board Chair
Audit Committee

REPORT HIGHLIGHTS

26-03 CHARTER SCHOOL AUTHORITY INFORMATION TECHNOLOGY SERVICES AUDIT

Issued May 5, 2026

Objectives

1. To evaluate the design and operating effectiveness of controls over the inventory management and physical safeguarding of IT assets to ensure accurate accountability and appropriate protection of technology resources.

2. To assess the adequacy and operating effectiveness of information security and user access management controls to prevent unauthorized access and protect the confidentiality, integrity, and availability of systems and data.

3. To assess the adequacy and effectiveness of IT service management processes, including incident handling, request fulfillment, and provisioning of instructional technology services.

WHY THIS MATTERS

The Information Technology Services Department (ITS) plays a critical role in supporting the Charter School Authority's (CSA) daily operations and educational programs. Because the CSA relies on the City's information technology (IT) infrastructure, the reliability and security directly affect their ability to meet instructional, operational, and administrative goals. Effective IT governance, encompassing help desk responsiveness, system upkeep, cybersecurity safeguards, disaster recovery, and staff technical proficiency, is vital to maintaining operations and protecting sensitive data. Inadequate practices in these areas could lead to system downtime, data exposure, or reduced efficiency, highlighting the need to assess the adequacy and effectiveness of ITS management and controls.

ACCOMPLISHMENTS

1. Implemented comprehensive data protection and asset tracking controls across Charter School operations.
2. Executed infrastructure upgrades across all four Charter School campuses.
3. Consolidated Charter School systems by migrating employees from legacy platforms and implementing single sign-on access across more than 50 educational applications.
4. Deployed enterprise-grade security infrastructure incorporating proactive threat detection and preventive controls through centralized monitoring and zero-trust application management.

WHAT WE FOUND

The City Auditor's Office conducted a performance audit of IT services provided to the Oasis Charter Schools by ITS. This audit is included in the City Auditor's approved FY26 Audit Plan.

We found ITS effectively manages physical safeguarding and security of assets, access controls, cybersecurity measures and service requests; however, we noted certain areas discussed in the Findings and Recommendations that need improvement.

Overall, we determined controls are in place and operating as intended. We did not identify any material control deficiencies.

City Auditor Andrea R. Russell • (239) 242-3380 • ARussell@CapeCoral.gov

Table of Contents

Background

The Charter School Authority (CSA) operates four charter schools, Oasis Elementary North, Oasis Elementary South, Oasis Middle, and Oasis High School. The Oasis Charter Schools (Charter Schools) offer a continuous kindergarten through 12th grade educational pathway aligned with Florida Department of Education curriculum standards. The school system emphasizes State of Florida educator professional development and adheres to statutory training and certification requirements.

Charter Schools Mission

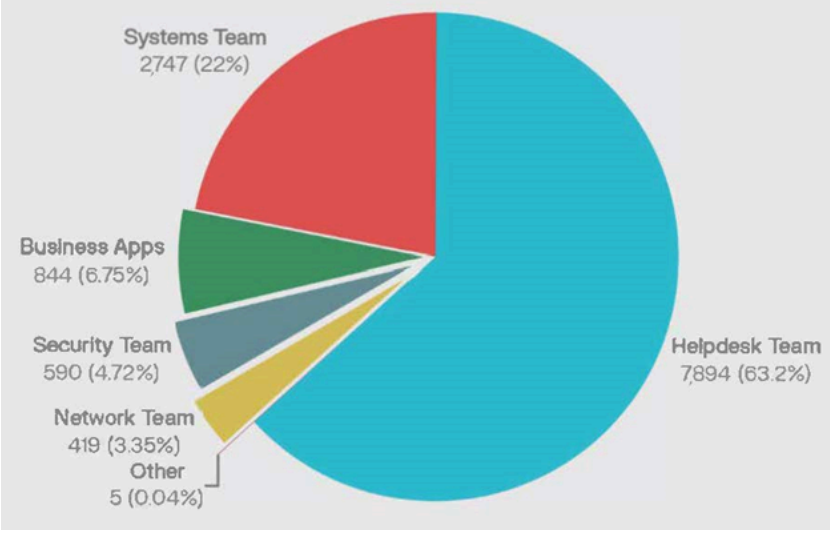
Our mission is to create a K-12 system that educates students to be responsible, critical thinkers who are prepared to successfully compete in a dynamic global workforce.

Chapter 26, Cape Coral Charter School Authority, Section 17, requires the CSA to utilize City departments and personnel for services including information technology (IT), financial, human resources, and facilities. These services provide essential operational support to the Charter Schools, enabling them to focus on their core educational mission. The City began fully supporting the Charter Schools' IT systems in July 2022. Prior to this transition, personnel employed by the Charter School did not possess the breadth of expertise available like the City's Information Technology Services Department (ITS). Given the increasing complexity of technology and the associated risks, the assignment of dedicated City ITS staff to provide oversight of the Charter Schools' IT is consistent with principles of sound governance and effective internal controls.

ITS supports the Charter Schools by providing shared municipal technology infrastructure and services used by the Charter School campuses including structured oversight of key technology processes and security that sustain reliable and secure operations across the Charter School network. ITS also maintains network connectivity and core systems for Charter School facilities and has implemented technology projects specifically for the Charter Schools, such as network upgrades and visitor management systems that support daily operations and campus safety.

We administered a survey to all teachers and administrative staff to gain an understanding of user experiences and interactions with ITS. Their perspectives help reveal strengths and weaknesses with access, usability, training, devices, software, and support tickets that may not appear in system records alone. See survey results in Appendix A and Appendix B.

Support Ticketing



ITS manages support for the Charter Schools through a centralized ticketing system that utilizes a live video dashboard to monitor ticket intake, response times, and workload. We analyzed ticket data from FY24, FY25, and FY26 through February 28, 2026. During this period, 12,499 tickets were submitted; the majority of tickets, 63.2%, were assigned to the Helpdesk Team, followed by the Systems Team, 22%, and Business Applications[1], 6.75%. ITS uses an Urgency/Impact matrix to classify ticket priority to distinguish widespread outages from isolated, lower-impact issues, such as forgotten passwords. Overall service level agreement (SLA) violation rates were low, at approximately 2% for first response and 1% for resolution across all teams.

[1] The Helpdesk Team provides support for day-to-day IT problems, the Systems Team manages the underlying servers and devices to keep services running, and Business Applications manages the setup, configuration, and workflows of organizational software systems.

Inventory Management

The Charter Schools rely on a range of IT assets, including staff desktops and laptops, student Chromebooks, and designated spare and loaner devices. A robust inventory management program helps to provide accountability for school resources, reduce the risk of loss or misuse, and ensure students and staff have access to functional devices.

Cybersecurity Training

ITS manages the Charter Schools cybersecurity training to ensure that all users understand their roles in protecting systems, data, and resources. The program aligns with ITS policies in place for the City. ITS tracks participation and compliance to reduce risk and strengthen overall security awareness.

System Security and Incident Response

ITS is responsible for coordinating and managing activities to identify, assess, and respond to cybersecurity risks across the City's systems, applications, and networks. This includes overseeing the annual penetration testing conducted by external vendors to identify and remediate security vulnerabilities. ITS ensures that identified vulnerabilities are appropriately categorized, prioritized, and tracked through remediation to closure. In addition, ITS develops, maintains, and coordinates the cybersecurity incident response plan, which provides a structured framework for preparing for, detecting, responding, and recovering from cybersecurity incidents.

Access Management

ITS administers the access management program to ensure secure and controlled access to systems, applications, and data. The program defines roles and responsibilities, establishes procedures for provisioning and deprovisioning, and enforces the principle of least privilege. It also outlines authentication requirements, periodic access reviews, and monitoring practices, while adhering to applicable policies and best practices to protect sensitive information and systems.

Findings and Recommendations

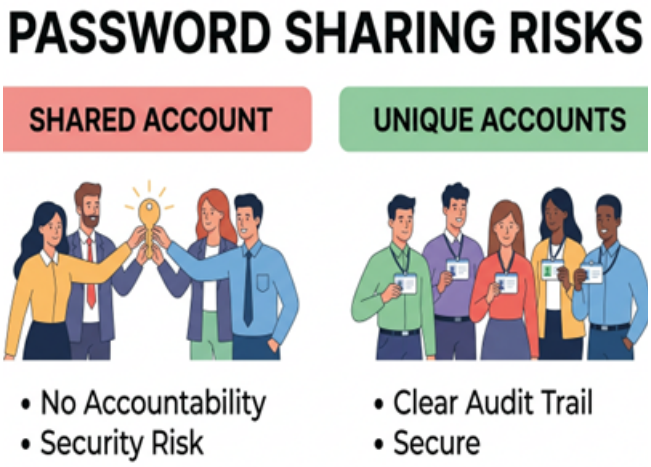
FINDING 2026-01: Improvements Needed in Monitoring Over Passwords and User Access Management

Rank: High

Condition:

Password and Credential Security

Password protection and monitoring by ITS staff is outlined in internal policies and external standards. ITS Password Policy states passwords should not be shared. Critical Security Controls (CIS) Control 5 recommends using processes and tools to assign and manage authorization to credentials for user accounts. In addition, CIS Control 8 recommends collecting, alerting, reviewing, and retaining audit logs of events that could help detect, understand, or recover from an attack.

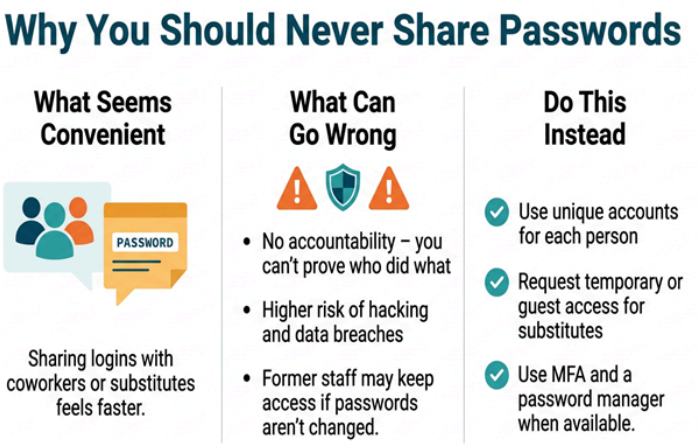


Results

The City Auditor's Office administered a survey to Charter School employees and responses indicated concerns about the use of shared login credentials, particularly when substitute teachers require access to classroom systems while the primary teacher is absent. To test the validity of survey responses, we attempted to assess the occurrence and extent of potential password sharing; however, our testing was constrained by several factors, including:

- Windows security event logs are retained for a limited period of less than 30 days due to available storage.
- Extracting authentication event data proved challenging because historical login information in a format suitable for audit review is not retained.
- ITS utilizes a Security Information and Event Management solution which collects authentication event data; however, generating login history reports requires complex queries, and the resulting output is not easily interpretable.
- The available administrative console logs lack granularity and filtering options needed to isolate and attribute logins by substitutes and teachers.

These factors also constrained ITS's ability to actively monitor credentials to detect potential password or account sharing as outlined by CIS Control 8. ITS indicated that these limitations could be mitigated by implementing an Account Management Solution (AMS), similar to the system used by the city, to centralize administration and reporting of user accounts. AMS would provide visibility into user activity and support reporting needs for future password sharing analysis.



Criteria:

- ITS Password Policy
- CIS Control 5
- CIS Control 8

Cause:

- Lack of AMS
- Potential noncompliance with ITS Password Policy
- System constraints limit monitoring and review of employee account activity

Effect:

- Increased risk of unauthorized or inappropriate access to systems and data
- Limited ability to monitor access, investigate security incidents, or identify individual system activity

Recommendations

2026-01:
Implement a centralized account management solution and configure authentication and account activity logging to capture sufficient detail to appropriately monitor and identify potential password sharing or account use anomalies.

Management Response and Corrective Action Plan:

2026-01 Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-01
IT will procure and install a centralized logging solution at the Charter Schools.

2026-01	**Management Action Plan Coordinator:** ITS *Director*
2026-01	**Anticipated Completion Date:** *07/31/2026*

FINDING 2026-02: Cybersecurity Training Administration Needs Improvement
Rank: High

Condition:
Annual Cybersecurity Training
ITS manages cybersecurity awareness training for the Charter Schools. New employees are required to complete new hire training within 30 days of hire date, and existing employees must complete an annual refresher course. Testing noted that CSA employees meet the ITS requirements for annual and new hire training with no exceptions noted. However, because the refresher course is conducted in May at the end of the academic year, this could lead to a gap in cybersecurity awareness between the start of the school year and when the refresher training is administered. At the start of the school year, large volumes of system reactivations, new staff onboarding, account creations, and student data updates occur, often alongside heavier email and technology usage. These circumstances heighten the potential for phishing attempts, credential misuse, and accidental data exposure. Also, during the timing gap between refresher training offered in May and the beginning of the school year, staff often disengage from systems and may have credentials reset or reactivated at the beginning of the academic year. This training timing gap reduces retention of cybersecurity concepts such as identifying phishing emails, managing passwords securely, and safeguarding sensitive student information. Consequently, employees may not be fully prepared to recognize or respond to cyber threats when systems are most active.

Training System Configuration and Monthly Phishing Campaign

ITS sends monthly phishing emails to educate employees about phishing cyberattacks. If an individual "fails" the attack they are required to take remediation training. As part of our review of monthly phishing email campaigns, we identified configuration and set up issues in the software utilized by ITS. Only one of the four Charter Schools received phishing training since July 2024. As a result, three of the four Charter Schools did not participate in monthly phishing campaigns or related remediation training until it was brought to the attention of ITS. Although all Charter School employees and new hires complete the required

annual and new hire cybersecurity awareness training, the absence of ongoing phishing simulations and timely remediation training increases the risk of phishing attacks.

Advanced Cybersecurity Training

Employees with access to sensitive data require a higher level of cybersecurity knowledge that goes beyond annual and new hire cybersecurity awareness training. These employees manage critical systems and confidential data that, if compromised, increases the risk of personal and protected data exposure and could disrupt Charter School operations. Control Objectives for Information and Related Technologies (COBIT) PO7.4[2] and CIS Control 14 emphasize IT personnel should receive appropriate and continuous, role-specific training to maintain the knowledge, skills, and security awareness necessary to perform their duties effectively and support organizational objectives. In addition, Administrative Regulation (AR) T-4 Information Security Awareness Training Policy requires advanced cybersecurity training to be completed by City employees who have access to protected or sensitive data. However, there is no advanced training offered to Charter School employees[3]. The absence of advanced cybersecurity training for Charter School staff limits the organization's ability to adequately prepare high risk personnel to address evolving threats. To mitigate these risks, the cybersecurity training program should align with City and industry specific

[2] Plan and Organize

[3] City employees assigned to the Charter Schools (Human Resources, Payroll, IT Systems Administrator) receive advanced cybersecurity training under the City campaign.

frameworks that incorporate regular, role specific, and ongoing development activities tailored to the sensitivity of each position.

Criteria:

- AR T-4
- COBIT PO7.4
- CIS Control 14

Cause:

- Timing of cybersecurity training
- Incomplete setup and deployment of phishing training
- Advanced cybersecurity training requirements not defined or implemented for Charter Schools

Effect:

- Potential mishandling of sensitive data
- Potential insufficient awareness of cyberattacks
- Elevated exposure to cybersecurity incidents

Recommendation

2026-02a:
Schedule Charter School cybersecurity training before the start of the school year.

Management Response and Corrective Action Plan:

2026-02a Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-02a
The annual required cybersecurity training will be scheduled for Aug 01 thru Sept 15

2026-02a **Management Action Plan Coordinator:**
ITS *Director*

2026-02a **Anticipated Completion Date:**
06/02/2026

Recommendation

2026-02b:
Complete full configuration and deployment of the cybersecurity training at the Charter Schools.

* * * * *

2026-02c:
Identify Charter school positions with access to sensitive information and enroll them into advanced cybersecurity training.

Management Response and Corrective Action Plan:

2026-02b Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-02b
The cybersecurity training program will be reviewed and updated to include all four Charter Schools.

2026-02b **Management Action Plan Coordinator:**
ITS *Director*

2026-02b **Anticipated Completion Date:**
06/02/2026

* * * * *

2026-02c Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-02c
ITS will identify appropriate staff based on position and role and assign corresponding advanced cybersecurity training.

2026-02c **Management Action Plan Coordinator:**
ITS *Director*

2026-02c **Anticipated Completion Date:**
07/31/2026

FINDING 2026-03: ITS Policies Need to be Updated to Remove Inconsistencies
Rank: Medium

Condition:
The ITS *Request for Remote Access Policy*, updated on August 12, 2025, removed prior language that specifically excluded Charter School staff from its scope. As a result, these employees are now formally subject to the policy's requirements. However, the ITS *Remote Access Policy*, dated June 25, 2025, still includes an exception under Section 5 allowing Charter School staff to access City issued devices remotely from home, with approval by the superintendent rather than the ITS. This conflicting policy information creates uncertainty regarding which remote access requirements apply to Charter School staff, and who is responsible for authorizing such access. This could result in inconsistent governance and potential security gaps in remote access management.

In addition, the ITS IT Services Recovery and Resumption Policy[4] specifically states the policy does not apply to the Charter School system. Conversely, the Cybersecurity Incident Response Plan, which outlines the City's overall approach to preparing for and responding to cybersecurity incidents, explicitly includes the Charter Schools. These contradictions between the incident response plans create ambiguity regarding responsibility for incident preparedness and response activities involving Charter Schools IT systems, which may result in confusion or delays during a cybersecurity incident.

Criteria:
- ITS Remote Access Policy
- ITS Request for Remote Access Policy
- ITS IT Services Recovery and Resumption Policy
- Cyber Security Incident Response Plan

[4] IT Services Recovery and Resumption Policy includes the Disaster Recovery Plan

Cause:

- Policies are not reviewed and updated consistently

Effect:

- Inconsistent governance and unclear accountability between ITS and Charter School security responsibilities
- Potential security gaps due to differing remote access authorization
- Possible inappropriate and insufficient response to a cybersecurity incident at Charter School

Recommendation

2026-03:
Update ITS policies and procedures to ensure they are consistent with City policies and clearly document roles and responsibilities.

Management Response and Corrective Action Plan:

2026-03 Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-03
ITS will update and remove policies to ensure they are consistent.

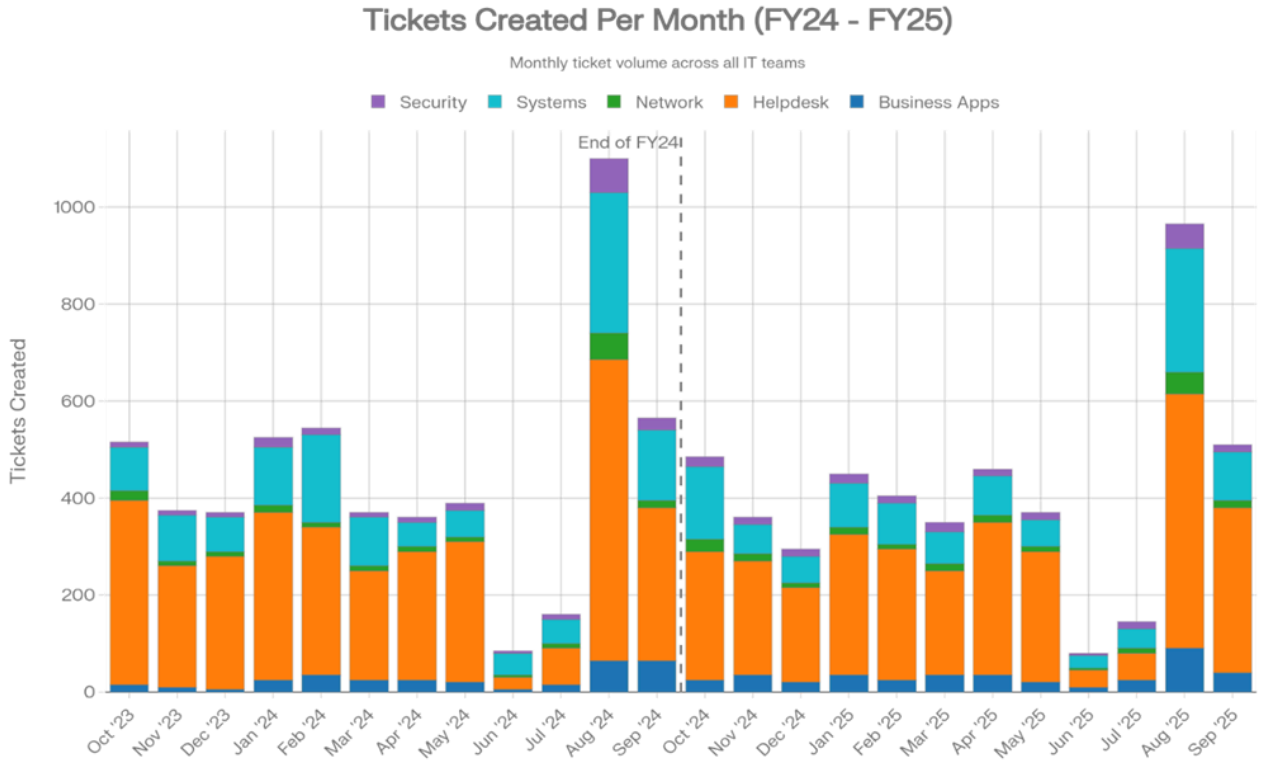
2026-03 **Management Action Plan Coordinator:**
ITS *Director*

2026-03 **Anticipated Completion Date:**
07/31/2026

FINDING 2026-04: Limited Feedback on ITS Ticket Performance and Unclear Service Expectations
Rank: Medium

Condition:
Under COBIT 2019 EDM04[5], management is responsible for ensuring that IT-related resources; including staffing, skills, processes, and supporting tools; are planned, allocated, and monitored so they are used optimally to meet needs and service expectations. This includes aligning support capacity with predictable workload peaks, providing sufficient training and guidance when systems change, and using meaningful performance information and user feedback to monitor service quality. Despite generally strong ticket timeliness, analysis of ticket trends, survey feedback, and walkthroughs identified several areas where current ITS practices do not fully align with these expectations or with Charter School needs.

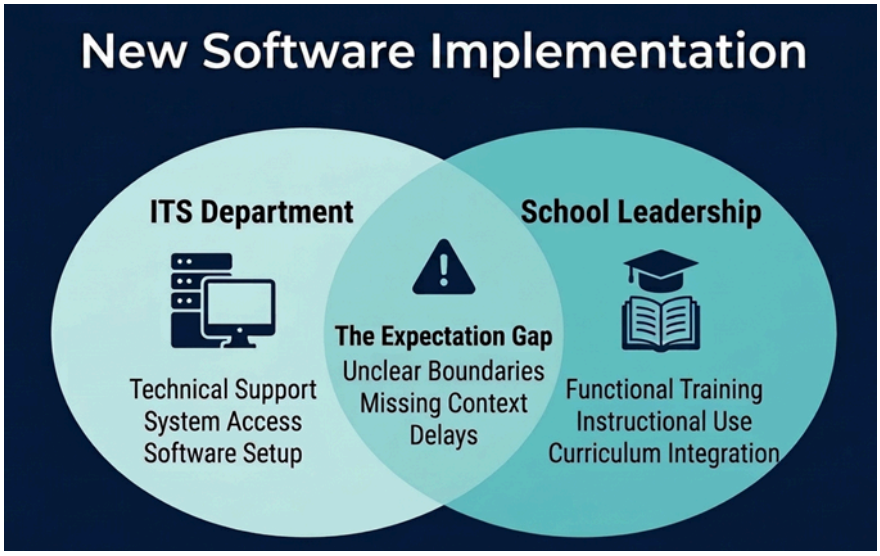
Monthly Ticket Volume
Ticket volume increases significantly at the start of the school year during the month of August. In both FY24 and FY25, tickets created during August increased by more than 135% over the average monthly volume, and more than 25% of all first response SLA violations occurred during August. Despite this recurring spike, walkthroughs and discussions indicated that staffing and on-site support patterns do not change materially at the beginning of the school year, and key IT resources, such as Business Applications Analysts, do not routinely visit schools



[5] Evaluate, Direct, and Monitor

during this period. This increases the risk that users experience delays or confusion during one of the most critical times of the year, even when formal SLA targets are being met.

Software Training



Responses from the CAO survey of Charter School staff and our walkthroughs also pointed to an expectation gap between training and support for new or changing systems. While respondents generally agreed that issues are acknowledged and resolved quickly, only 49% agreed or strongly agreed that ITS provides helpful training and guidance when new systems or tools are introduced; 14% disagreed or strongly disagreed; and the remaining responses were neutral. Through discussions with ITS, we noted that many of these requests involve school-selected instructional software, where the split between functional training and technical support has not been clearly defined or communicated to staff. In practice, ITS often needs additional student or classroom information from school staff before they can fully assist, which can lead to back-and-forth communication and longer resolution times for some requests. The communication examples provided by ITS and Charter School staff, together with staff survey results, demonstrate training and communication does not fully align with user expectations, particularly with new school software.

User Feedback

Management's awareness of user satisfaction is limited by the way customer feedback is collected. Our analysis showed that only 241 out of 12,499 tickets (2%) had completed post ticket surveys. ITS reported that one in ten service requesters are offered a post ticket survey. This low response rate, combined with infrequent outreach, reduces ITS management's ability to obtain timely and representative feedback on service quality, identify recurring issues, and prioritize improvements.

Overall, these factors can indicate a lack of understanding between the level and type of support ITS is providing and the services the Charter Schools expect, due to limited software training, lack of additional on-site presence during peak periods, and insufficient customer satisfaction feedback.

Criteria:

- COBIT 2019 EDM04
- ITS SLAs

Cause:

- Limited focus on peak period and training needs
- Unclear role definitions between ITS and the Charter Schools
- Customer service surveys infrequently administered

Effect:

- Potential lower staff confidence in IT support
- Inconsistent understanding of IT services provided
- Limited customer satisfaction data

Recommendation

2026-04a:
ITS must establish and communicate clear roles and responsibilities, along with the scope of support provided to Charter Schools.

* * * * *

2026-04b:
ITS should increase the frequency of customer satisfaction surveys to more proactively identify service gaps, training needs, and corrective actions.

Management Response and Corrective Action Plan:

2026-04a Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-04a
ITS and Charter Schools will collaborate to review and develop appropriate procedures to define IT services.

2026-04a **Management Action Plan Coordinator:**
ITS *Director*

2026-04a **Anticipated Completion Date:**
09/30/2026

* * * * *

2026-04b Select one of these boxes:

☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response.**

2026-04b
Satisfaction survey distribution will be increased from the current level.

2026-04b **Management Action Plan Coordinator:**
ITS *Director*

2026-04b **Anticipated Completion Date:**
06/02/2026

Scope

Based on the work performed during the planning phase and the assessment of risk, the audit covers processes, policies, and procedures in place over Charter School IT services for FY24, FY25, and FY26 through February 28, 2026.

Statement of Auditing Standards

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.

Methodology

In order to achieve the audit objectives and gain a better understanding of how the City delivers IT services to support the Charter Schools IT related needs, we reviewed relevant policies, procedures, and supporting documentation to understand the design of processes and controls. We held meetings and conducted field observations with ITS and Charter School personnel to gain an understanding of the processes in place. In addition, we administered a survey to Charter School staff and teachers to gather user perspectives on the effectiveness and quality of IT services provided.

Original records as well as copies were used as evidence and verified through physical examination. Sample size and selection were based on the CAO sampling methodology. Industry best practices were considered during testing to help identify potential areas for improvement and to strengthen internal controls and operational processes.

Objective 1: To evaluate the design and operating effectiveness of controls over the inventory management and physical safeguarding of Information Technology (IT) assets to ensure accurate accountability and appropriate protection of technology resources.

To determine whether device inventory records are complete and accurate we randomly selected a sample of 25 classroom devices and 40 spare and loaner Chromebooks. We also judgmentally selected two Chromebooks listed as lost or disposed.

Objective 2: To assess the adequacy and operating effectiveness of information security and user access management controls to prevent unauthorized access and protect the confidentiality, integrity, and availability of systems and data.

To verify whether Charter School personnel completed annual and new-hire cybersecurity awareness training and participated in monthly simulated phishing campaigns, we randomly selected six new hires, 40 teachers, and six administrative support staff.

Methodology (continued)

To assess whether the Charter Schools' cybersecurity incident response plan is documented, regularly tested, and implemented to support timely detection, response, and recovery, we reviewed the City-wide plan to confirm it is tested periodically and updated as needed.

We reviewed recent external penetration testing results to determine whether identified vulnerabilities were remediated in a timely manner or, if not, whether a remediation plan was in place. We selected a random sample of seven vulnerabilities identified across Charter Schools for FY24 and FY25.

To determine whether controls are in place to monitor teacher and student account access, we randomly selected a sample of six former teachers, 40 active students, and 40 former students to determine if the account had the appropriate status.

Password sharing with substitute teachers was unable to be tested due to current software limitations.

Objective 3: To assess the adequacy and effectiveness of ITS management processes, including incident handling, request fulfillment, and provisioning of instructional technology services.

To determine whether IT support tickets are managed effectively, prioritized appropriately, and responded to and resolved within defined timeframes, we reviewed 100% of all Charter School IT support tickets for the audit period and analyzed ticket SLAs.

To determine whether the level of service provided by ITS is in accordance with Charter school expectations and safeguards security, access, and functionality of IT assets for instructional use, we reviewed 100% of all Help Desk tickets for the audit period and analyzed tickets created in August of 2024 and 2025, when the school year begins.

To support the sample methodology described above to achieve the audit objectives, we discussed, obtained an understanding of the software systems used by the Charter Schools and ITS for inventorying, help desk ticketing, user access, and cybersecurity training. By doing this we deemed the data reliable for purposes of our audit objectives.

Unless specifically stated otherwise, based on our selection methods and testing of transactions and records, we believe that it is reasonable to project our results to the population and ultimately draw our conclusions for testing, findings, and recommendations on those results. Additionally, for proper context we have presented information concerning the value and/or size of the items selected for testing compared to the overall population and the value and/or size of the exceptions found in comparison to the items selected for testing.

Appendix A

The City Auditor's Office conducted a survey as part of the audit. In coordination with the Charter School Superintendent, the survey was distributed to teachers and administrative staff at the Charter Schools. Below are the results from the 12-question survey, as provided by teachers. 292 surveys were distributed to teachers, and 109 responses were received, resulting in a 37% completion rate.

1. I am a staff member at the following school:

Response	Number of Responses	Percentage of Responses
Oasis Elementary North	25	23.15%
Oasis Elementary South	33	30.56%
Oasis Middle School	21	19.44%
Oasis High School	29	26.85%
Grand Total	**108**	**100%**

2. The set up and deployment of Chromebooks for students at the beginning of the school year is completed in a timely and supportive manner by the IT department.

Response	Number of Responses	Percentage of Responses
Strongly agree	55	50.46%
Agree	36	33.03%
Neither agree nor disagree	15	13.76%
Disagree	3	2.75%
Strongly disagree	0	0.00%
Grand Total	**108**	**100%**

3. The response time by the IT help desk for acknowledging and resolving IT issues is appropriate.

Response	Number of Responses	Percentage of Responses
Strongly agree	69	63.30%
Agree	30	27.52%
Neither agree nor disagree	5	4.59%
Disagree	5	4.59%
Strongly disagree	0	0.00%
Grand Total	**109**	**100%**

4. Issues related to networking or account access (e.g. passwords, blocked accounts) are resolved quickly and effectively.

Response	Number of Responses	Percentage of Responses
Strongly agree	64	58.72%
Agree	33	30.28%
Neither agree nor disagree	6	5.50%
Disagree	6	5.50%
Strongly disagree	0	0.00%
Grand Total	**109**	**100%**

5. The IT department understands and meets the specific technology needs of my school or program.

Response	Number of Responses	Percentage of Responses
Strongly agree	55	50.46%
Agree	40	36.70%
Neither agree nor disagree	10	9.17%
Disagree	3	2.75%
Strongly disagree	1	0.92%
Grand Total	**109**	**100%**

6. The IT department collaborates effectively with school staff to address technology issues.

Response	Number of Responses	Percentage of Responses
Strongly agree	57	52.29%
Agree	34	31.19%
Neither agree nor disagree	13	11.93%
Disagree	5	4.59%
Strongly disagree	0	0.00%
Grand Total	**109**	**100%**

7. The Chromebook repair and replacement process works smoothly (loaner devices are available promptly).

Response	Number of Responses	Percentage of Responses
Strongly agree	43	39.45%
Agree	35	32.11%
Neither agree nor disagree	27	24.77%
Disagree	3	2.75%
Strongly disagree	1	0.92%
Grand Total	**109**	**100%**

8. The IT department provides clear communication about technology changesthat affect instruction or operations.

Response	Number of Responses	Percentage of Responses
Strongly agree	39	35.78%
Agree	38	34.86%
Neither agree nor disagree	20	18.35%
Disagree	11	10.09%
Strongly disagree	1	0.92%
Grand Total	**109**	**100%**

9. The IT department offers helpful training and guidance when new systems or tools are introduced.

Response	Number of Responses	Percentage of Responses
Strongly agree	22	20.18%
Agree	31	28.44%
Neither agree nor disagree	41	37.61%
Disagree	11	10.09%
Strongly disagree	4	3.67%
Grand Total	**109**	**100%**

10. Overall, I am satisfied with the support and services provided by the IT department.

Response	Number of Responses	Percentage of Responses
Strongly agree	60	55.56%
Agree	37	34.26%
Neither agree nor disagree	7	6.48%
Disagree	4	3.70%
Strongly disagree	0	0.00%
Grand Total	**108**	**100%**

11. Please describe any specific improvements or additional support you would like from the IT department.

Comments only question, responses not included.

12. What aspects of IT Support have been most helpful to you?

Comments only question, responses not included.

Appendix B

The City Auditor's Office conducted a survey as part of the audit. In coordination with the Charter School Superintendent, the survey was distributed to teachers and administrative staff at the Charter Schools. Below are the results from the 11-question survey, as provided by administrative staff. 9 surveys were distributed to administrative staff, and 6 responses were received, resulting in a 67% completion rate.

1. The set up and deployment of Chromebooks for students at the beginning of the school year is completed in a timely and supportive manner by the IT department.

Response	Number of Responses	Percentage of Responses
Strongly agree	5	83.33%
Agree	1	16.67%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

2. The response time by the IT help desk for acknowledging and resolving IT issues is appropriate.

Response	Number of Responses	Percentage of Responses
Strongly agree	4	66.67%
Agree	2	33.33%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

3. Issues related to networking or account access (e.g. passwords, blocked accounts) are resolved quickly and effectively.

Response	Number of Responses	Percentage of Responses
Strongly agree	4	66.67%
Agree	2	33.33%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

4. The IT department understands and meets the specific technology needs of my school or program.

Response	Number of Responses	Percentage of Responses
Strongly agree	4	66.67%
Agree	2	33.33%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

5. The IT department collaborates effectively with school staff to address technology issues.

Response	Number of Responses	Percentage of Responses
Strongly agree	5	83.33%
Agree	1	16.67%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

6. The Chromebook repair and replacement process works smoothly (loaner devices are available promptly).

Response	Number of Responses	Percentage of Responses
Strongly agree	5	83.33%
Agree	1	16.67%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

7. The IT department provides clear communication about technology changes that affect instruction or operations.

Response	Number of Responses	Percentage of Responses
Strongly agree	3	50.00%
Agree	3	50.00%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

8. The IT department offers helpful training and guidance when new systems or tools are introduced.

Response	Number of Responses	Percentage of Responses
Strongly agree	1	16.67%
Agree	2	33.33%
Neither agree nor disagree	2	33.33%
Disagree	1	16.67%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

9. Overall, I am satisfied with the support and services provided by the IT department.

Response	Number of Responses	Percentage of Responses
Strongly agree	5	83.33%
Agree	1	16.67%
Neither agree nor disagree	0	0.00%
Disagree	0	0.00%
Strongly disagree	0	0.00%
Grand Total	**6**	**100%**

10. Please describe any specific improvements or additional support you would like from the IT department.
Comments only question, response not included.

11. What aspects of IT Support have been most helpful to you?
Comments only question, response not included.