KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

Evaluating Access Controls of School District Accounting Systems

September 2025

Report Number: R-25-017

Introduction

The Legislative Post Audit Committee requested and authorized this audit at its April 10, 2025 meeting.

Objectives, Scope, & Methodology

Our audit objective was to answer the following question:

1. Do selected school districts' accounting systems have adequate access security controls?

The scope of our work included 20 school districts' current accounting systems policies and practices in place as of June 2025. The judgmental selection of school districts was based on location and size. Because this selection is judgmental, the results of this audit cannot be projected to all 286 school districts.

Our method included reviewing IT Security and accounting controls and best practices related to information system access. From that list, we focused on basic controls we would expect to be in place for school district accounting systems. We requested and reviewed documentation and observed each school district's accounting software to look for evidence that the chosen access controls were in place in both written policy and in practice.

More specific details about the scope of our work and the methods we used are included throughout the report as appropriate.

Important Disclosures

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. Overall, we believe the evidence obtained provides a reasonable basis for our findings and conclusions based on those audit objectives.

Audit standards require us to report confidential or sensitive information we have omitted when circumstances call for that. Kansas Open Records Act (KORA) exemption criteria allow our work to remain confidential. K.S.A. 45-221(a)(12) states that records regarding security information or procedures of a public agency can remain closed if disclosure would jeopardize the agency's security. This includes, among other things, records of cybersecurity plans, assessments, vulnerabilities or procedures. However, K.S.A. 45-221(d) states that agency records, if anonymized, can be used to create a summary level report. For these reasons, we've anonymized the school districts included in our selection.

Audit standards require us to report our work on internal controls relevant to our

audit objectives. They also require us to report deficiencies we identified through this work. In this audit, we evaluated internal controls related to accounting system access at a selection of school districts in Kansas. We noted that weak access control policies and practices for accounting systems increase the risk of both internal and external threats, such as ransomware, phishing attacks, and fraud.

Our audit reports and podcasts are available on our website www.kslpa.gov.

Of the 20 districts we reviewed, only some had adequate access controls for their accounting systems, and very few had adequate written policies.

Background

School districts use accounting systems to manage their expenses and report on their financial information.

- The Kansas State Department of Education (KSDE) requires school districts to report on their finances regularly, but they do not require school districts to use a particular accounting system. School districts generally contract with a vendor to obtain their individually chosen accounting system.

- Accounting systems record and track school districts' financial transactions. They hold and provide access to important K-12 funding used for staff salaries and benefits, operational expenses, and costs for students and staff such as curriculum, staff development, transportation, and special education.

- As of June 2025, Kansas had 286 school districts. The most recent finance report available through KSDE shows that the state's school districts managed about $8.5 billion in the 2023-2024 school year.

- School districts are regularly audited by Certified Public Accountants and KSDE. These audits verify whether school districts were legally compliant with accounting standards. This includes whether districts made purchases from the correct accounts and whether numbers on invoices and receipts match the district's records. These audits do not focus on the type of IT security controls we reviewed in this audit.

It's critical that school districts protect their accounting systems against unauthorized access.

- School districts house more data and processes in computerized systems than ever before. This means that school districts must be proactive with implementing computer-based controls to keep their data and processes safe and secure.

- District staff have varying levels of access to school district accounting systems for different reasons. Staff in charge of payroll and purchasing generally need access to create and modify data in multiple accounts. Superintendents may only need to be able to view certain data or summary reports. Principals and department directors may need access to request or approve purchases within their respective schools or areas. Teachers or other classified staff may only need access to submit their timesheet and view their

own personnel information like their W2. Contractors may also need access in some situations, such as for providing technical support.

- Each school district is responsible for ensuring their accounting systems have proper controls to safeguard their financial information. These include preventing unauthorized access (through various security controls such as passwords) and limiting access to a "need to know" basis.

- Inadequate accounting system access controls leave districts' systems more susceptible to unauthorized access through things like phishing scams. These types of schemes typically use e-mail to trick a recipient into revealing sensitive information or providing access to the system. Districts' systems may also be more vulnerable to ransomware attacks which use software to prevent entry to the system or hold data hostage until the user makes a payment. Inadequate controls also leave districts susceptible to fraud, such as a user making unauthorized changes in systems to siphon off funds disguised as legitimate district expenses.

- A recent audit found that a Missouri school district's accounting system did not have adequate controls in place to reasonably ensure the security of their accounting information. For instance, multiple staff had more access to create or modify accounting system data than they should have had given their job duties. Confidential IT audits conducted by the Kansas Legislative Division of Post Audit have audited other general IT security controls, including data encryption, backups, and physical controls. Those audits found several IT security problems in reviews of several Kansas school districts. These general IT security controls are also important but were not part of our audit work.

School districts are not required to follow the state's IT security policies.

- The Legislature created the Information Technology Executive Council (ITEC) in 1998. State law (K.S.A. 75-7203) requires ITEC to adopt information technology resource policies for executive-branch state agencies. In turn, ITEC established security, data, and applications and software policies. However, school districts are not subject to the state's ITEC policies.

- Districts are subject to other state and federal laws to protect sensitive data. For example, the federal Family Educational Rights and Privacy Act and the Kansas Student Data Privacy Act restrict who districts can release certain student data to. But neither requires school districts to implement specific IT security controls.

- KSDE (the state's oversight agency for Kansas' 286 school districts) also does not require school districts to implement specific IT security controls for accounting systems. Our 2021 audit on school districts' self-reported IT security practices found many districts did not follow basic security standards. In response to that audit, the department took several actions to help improve districts' IT security processes. These actions included the following:

- creating a K-12 technology council (tasked with developing best practices and a how-to toolkit);

- creating an IT technology webpage (including resources, training materials, and a link to the department's IT policy handbook);

- making security awareness training available to all districts at no cost; and

- providing districts with templates they should consider when developing security policies.

- However, KSDE stopped short of requiring districts to follow a minimum set of security standards.

- There are no requirements for Kansas school districts' accounting system controls in Kansas law. Similarly, KSDE does not formally provide criteria or guidance to school districts regarding accounting system controls.

We compiled a set of IT security and accounting best practices to evaluate school districts' access controls for accounting systems.

- We reviewed best practices in IT Security from ITEC and the National Institute of Standards in Technology (NIST). We also reviewed accounting control best practices available on the Kansas Department of Administration website.

- Given the scope, we focused on best practices relevant to access controls for accounting systems. Most of the controls we identified are required for Kansas' state agencies. While these controls are not required of school districts, we think the state's IT security requirements and accounting best practices also provide a reasonable standard for school districts. We identified a few additional controls to evaluate based on best practices available through NIST that the LPA IT security audit staff recommended as basic security practices for computerized systems. We think these controls represent a reasonable baseline for access controls for school district accounting systems.

- The 3 sources of best practices we reviewed included over 200 controls. We identified 12 controls as relevant to basic accounting system access controls. Those controls fell into 3 main categories: account management, identity management, and user limits.

    - Account management controls protect against unauthorized account creation and modification. This ensures that only authorized users have access to the system. We evaluated 3 controls in this category. These controls covered things like having an assigned account manager to oversee district accounting systems, and having a formal process to create, modify, or terminate access to the systems.

- Identity management controls protect against unauthorized users. This ensures only authorized users have access to the accounting system. We evaluated 4 controls in this category. These controls cover things like requiring multi-factor authentication, having processes that prohibit sharing passwords, and locking accounts after a designated number of failed log-in attempts.

- User limits controls reduce the risk that users have more access than necessary. We evaluated 5 controls in this category. This included things like maintaining a list of authorized system users, having defined access levels (i.e., read-only), and segregating accounting duties so no single user has access to all critical components of a system.

We reviewed accounting system access control policies and practices for 20 judgmentally selected school districts across Kansas.

- We judgmentally selected 20 districts based on district location, size, population density, as well as by how recently the Kansas Legislative Division of Post Audit has audited the district. **Figure 1** gives details of the districts we selected. As the figure shows, our selection includes districts across all regions of Kansas. Our selection is also similar to the overall state in terms of district size: Large districts make up 13% of the overall number of districts, and 20% in our selection. However, we cannot generalize our results because the districts were not chosen randomly.

Figure 1. We chose a selection of 20 school districts of varying size and location to evaluate accounting system access controls.

Region	Number of Students	Number of Districts
Southwest	1,500	3
Northwest and North-Central (a)	1000	2
Northeast	21,000	5
South-Central	9,000	3
Southeast	2,500	3
Central	2,500	4

(a) Northwest and North-Central categories were combined to maintain anonymity.

Source: LPA judgmental selection.

- We evaluated whether districts had adequate written policies to address the controls we selected. Policies help codify expectations across all staff, ensure consistent understanding, and contribute to institutional memory (important for staff transitions). We requested formal policy from districts. We gave districts credit if they could produce a documented policy that adequately addressed the control we evaluated.

- We also checked to see whether districts implemented the controls in practice. To do this, we spoke with district officials, reviewed relevant documentation (e.g., checklists, forms, etc.), and reviewed automated system processes. We asked district officials to demonstrate that these practices were in place. We gave districts credit for having a practice if the practice adequately addressed the control we evaluated and we could see evidence that the practice was in place.

There are some important caveats about the work we did.

- We expected the districts to have the selected access controls regardless of their accounting systems' age or functionality. This is because the controls we were looking for were the most basic controls a system could have in place. The districts we audited used 5 different accounting systems from 4 different vendors. Some districts have had their accounting systems for many years, while others had recently changed systems. Some systems were entirely web-based while others were desktop applications. Further, some districts had systems with more extensive built-in controls while others had limited control features. Despite the age or functionality differences, we still expected the selected districts to have the same basic access controls (e.g., having multi-factor authentication, requiring segregation of duties, etc.) in place. That's because we selected basic controls that provide a baseline of security for accounting systems.

- We were specifically looking for evidence that districts independently determined the security needs for their accounting system within the context of their district. For instance, some districts may be small enough that it's reasonable to have purchasing procedures that include the superintendent's approval for every purchase. In larger districts, this would be unreasonable, so they may include the superintendent's approval only on higher-level purchases.

- Finally, we evaluated whether access controls were in written policies and in practice. We did not evaluate whether districts effectively used these controls. This means that we checked that there were clear processes in place that, if used correctly, would provide a basic level of control. The scope of this audit did not include testing that these controls were effective.

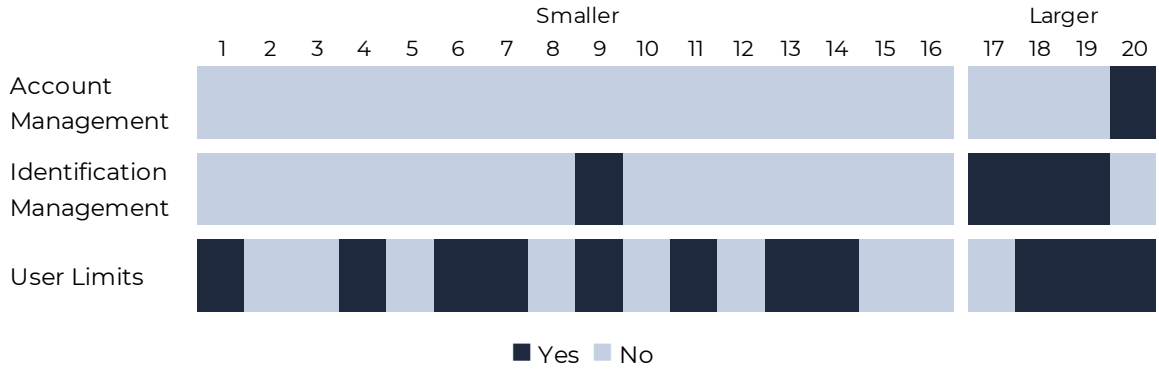
Overall Outcomes

None of the 20 districts we reviewed had adequate IT security access control practices in all 3 categories we evaluated.

- Best practices in IT security and accounting outline numerous access controls for sensitive information systems such as school district accounting systems. We reviewed 12 basic access controls that fell into 3 categories including account management, identity management, and user limits. For reporting purposes, districts with less than 2,500 students are categorized as smaller, and districts with more than 2,500 students are larger.

- We found that none of the 20 districts had practices in place for all 12 controls across the 3 categories we evaluated. **Figure 2** summarizes the selected districts' overall compliance with the 3 categories of controls we reviewed. As the figure shows, no districts had adequate practices in all 3 categories we reviewed, but many districts had practices in place for 1 or more categories

Figure 2. No school districts had adequate practices for all 3 categories of controls we reviewed.



Source: LPA review of school district practices and evidence of implementation.

- School districts are not held to uniform IT standards for their accounting system access controls, which could contribute to these results. There are no legal or regulatory requirements for school districts relevant to accounting system controls. KSDE also provides little guidance or direction. Many smaller school districts had limited staff. This was especially true for specialized IT security or accounting. This is a significant barrier to improving accounting system controls for smaller districts. As a result, smaller districts may rely more heavily on built-in system processes, institutional knowledge, and informal staff processes to ensure accounting system security.

- Lack of adequate access controls for accounting systems makes school districts more vulnerable to accidental or intentional misuse of district resources. That's because bad actors continually attempt to exploit business

and government agencies' weaknesses through phishing, ransomware attacks, to name a few.

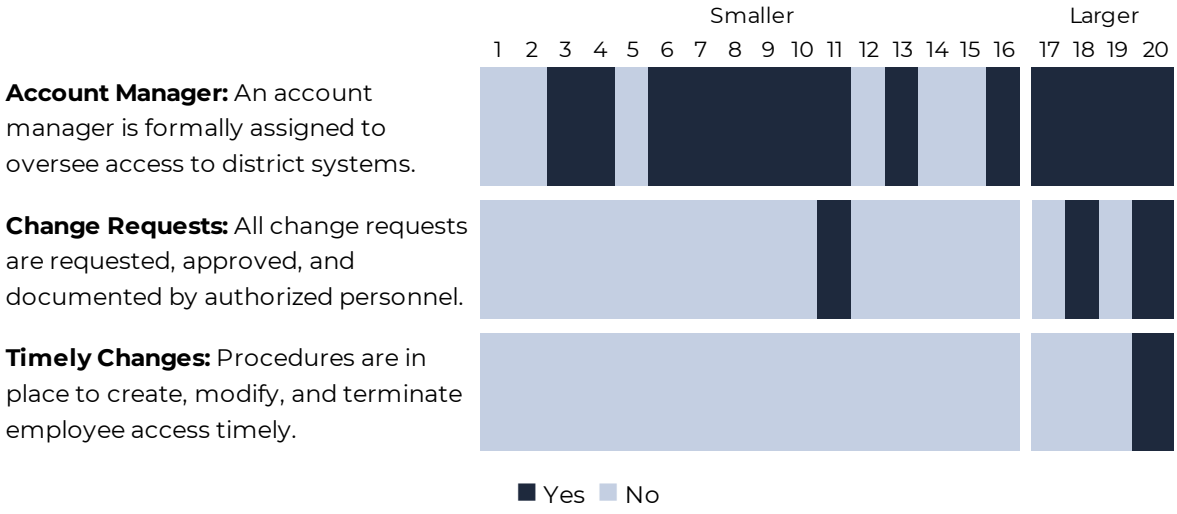
Account Management

Almost all school districts we reviewed (19 of 20) lacked all expected account management control practices within their accounting systems.

- We reviewed 3 account management controls in each district. These controls help regulate account access to districts' accounting systems. **Figure 3** shows a summary of the results for the account management controls we reviewed, like ensuring practices are in place to create, modify, or terminate account access.

- As the figure shows, only 1 district had adequate practices for all 3 of the controls we evaluated. The remaining 19 districts did not have adequate practices in one or more of the 3 controls. We describe our findings, and our work to arrive at those findings below.

Figure 3. Most school districts we reviewed did not have adequate account management controls in place in practice.



Source: LPA review of school district practices and evidence of implementation.

Kansas Legislative Division of Post Audit

- Many districts (14 of 20) had adequate practices related to account managers. We saw evidence that account managers were in place for 14 of the 20 districts we reviewed. For these districts we could see that an account manager was formally designated within the districts' accounting systems. This allows them to do things like create or modify staff access levels. The 6 remaining districts lacked a formally designated account manager for their accounting system. In those cases, districts officials told us they informally assign those responsibilities to staff. However, they were unable to provide

adequate evidence to show those informal practices were in place. That's because there was no documentation to support (e.g., user log, change request, etc.) that these individuals were assigned or performed the role of account manager.

- Few districts (3 of 20) had adequate practices related to formally documenting change requests. We looked to see if districts used checklists, software, or other processes to document system change requests, such as requiring that requests be in writing. One district was able to demonstrate a process that automatically documented change requests. In this case, we were able to observe that change requests (submitted by staff) were automatically logged within their system software. This process automatically notified and required action or approval from relevant staff for each step of the process. However, in many cases, district officials described an ad-hoc process related to change requests. For example, 1 district's officials told us staff may initiate requests verbally. However, there was no consistent process documenting those changes. In these cases, districts lacked a formal process for us to evaluate.

- Only 1 of the 20 districts had adequate practices to make access changes in a documented and timely manner (i.e., creating, modifying, or terminating employee access). We looked to see if districts used formal processes, checklists, or software to ensure access requests were timely. However, only 1 district was able to demonstrate that those practices were in place. For example, staff in one district told us they wait to deactivate an account until after the user receives their final paycheck (can be weeks later). However, there was no clear guidance on how soon after the final paycheck staff should terminate access. As a result, a departed employee still had access to the system for several weeks after leaving employment. In other cases, district officials told us that change requests should happen "ASAP" or "quickly" but lacked any further specificity. We did not consider these practices adequate. That's because these districts did not have detailed enough timelines for modifying account access.

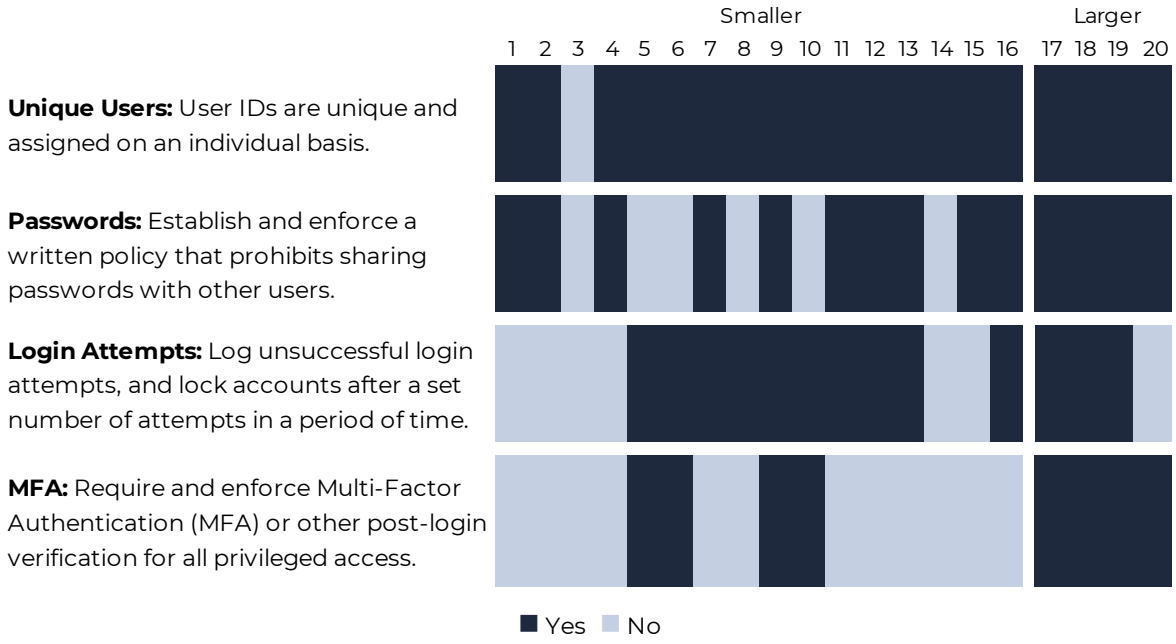
- Inadequate account management controls may result in staff gaining or keeping unauthorized access to the accounting system. For instance, former staff with continued access to the accounting system may be able to make unauthorized changes. Without account management controls, current staff may easily be able to gain access to the accounting system at a higher level than they should. This would give bad actors the opportunity to commit fraud. This leaves districts vulnerable to bad actors and the potential for improper account creation or access, whether intentional or unintentional.

Identity Management

Most school districts we reviewed (16 of 20) also did not have all expected identity management practices in place within their accounting systems.

- The 4 controls we reviewed in this category help protect against unauthorized use of accounts. **Figure 4** shows a summary of our results for those controls, including the requirement for Multi-Factor Authentication on high-risk accounts.

Figure 4. Most school districts we reviewed did not have adequate identity management controls in place in practice.



Source: LPA review of school district policies and evidence of implementation.

Kansas Legislative Division of Post Audit

- As the figure shows, only 4 of the 20 districts we reviewed had adequate practices for all 4 identity management controls we reviewed. The remaining 16 districts lacked adequate practices in one or more of these areas. However, most districts did have at least 3 of the controls that we reviewed. We describe our findings, and our work to arrive at those findings below.

- Most districts had adequate practices related to unique user IDs, passwords, and failed login attempts.

    - Most districts (19 of 20) had adequate practices related to assigning unique user IDs. In these cases, we were able to see evidence of processes, checklists, or controls in the software that required IDs to be unique and assigned to a specific user. For example, some districts' accounting software had built in controls that required user IDs to be unique. In these

cases, we were able to observe that the software would not allow duplicated user IDs such as "admin."

- Most districts (14 of 20) had adequate practices to prohibit password sharing between employees. We reviewed districts' acceptable use policies related to password settings. 14 districts provided acceptable use policies that strictly prohibited sharing passwords. In many cases, we saw that employees had signed an acceptable use policy, meaning they formally agreed not to share their passwords. The remaining districts had no standard practices in this area.

- Most districts (13 of 20) had adequate practices to lock system accounts after a pre-determined number of failed login attempts. We reviewed system software settings with district staff. Staff demonstrated that settings were in place to lock accounts after a certain number of failed attempts. However, the number of failed logins allowed (before locking an account) varied by district. Best practice suggests that accounts should be locked after a certain number of failed attempts. We evaluated whether districts set a threshold for failed attempts before locking an account. We did not evaluate the appropriateness of those thresholds.

- Less than half of districts (8 of 20) required Multi-Factor Authentication (MFA) for users to access the accounting system. MFA is a security process that requires users to provide 2 or more verification factors to gain access to an account. It's important these accounts use MFA to verify that users are who they say they are. We asked district officials to demonstrate that MFA settings were in place for accounting system users. 8 districts demonstrated that MFA was required. These districts showed us the accounting system settings requiring MFA or showed us in real time that the MFA requirement popped up when staff attempted to log in. However, 12 districts did not have any MFA set up within their systems. Some districts' officials told us that their systems did not have MFA as an option. A few districts had MFA set up but either allowed staff to bypass it or failed to require MFA for each login. We did not consider these practices to be appropriate because they largely bypass the intention of MFA.

- It's important that all 4 controls in this category be in place because identity management controls should overlap by design to minimize the risk of compromise. School districts that lack 1 or more of these controls for their accounting system are more vulnerable to unauthorized access. For example, not having log-in limits on the system that also does not require MFA increases the risk for successful brute-force attacks from hackers and unauthorized internal or external access. Hackers gaining access to the system can do things like lock down the accounts and demand ransom or otherwise gain access to the funds held within the accounting system.

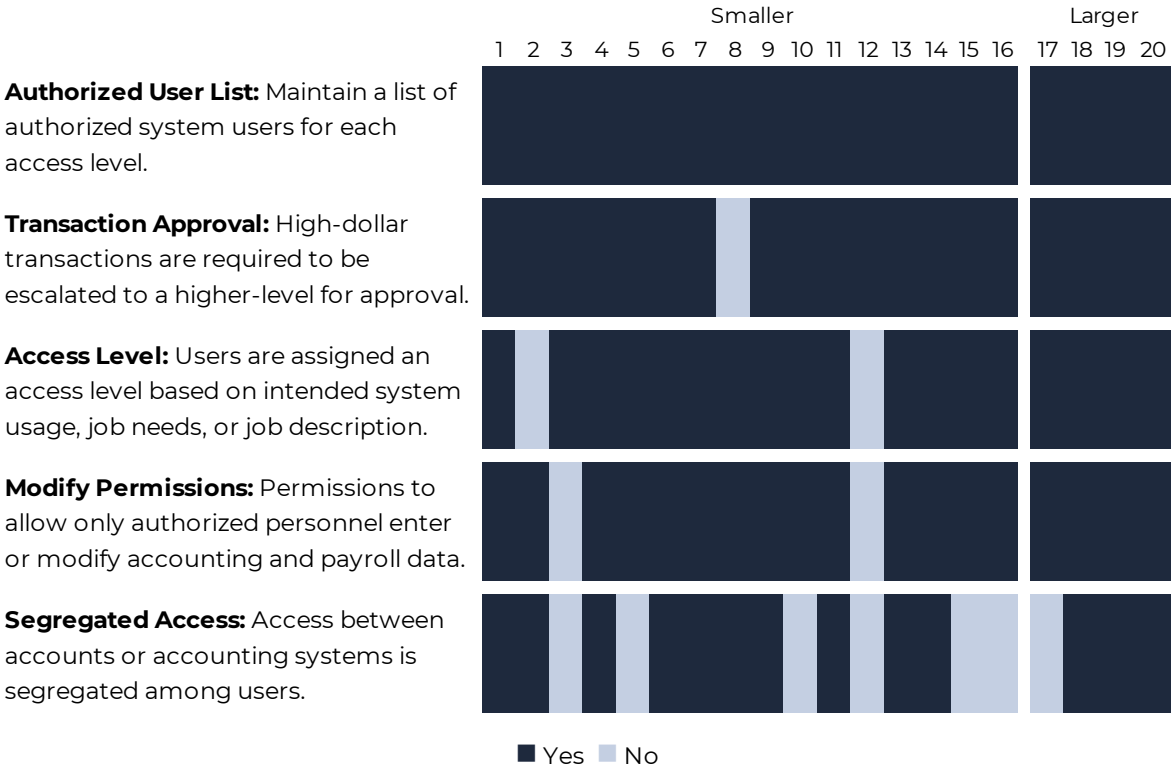
User Limits

About half of the school districts we reviewed (11 of 20) had all expected controls in place to limit user access to their accounting systems, and most school districts had at least 4 of the 5 controls we reviewed.

- The 5 controls we reviewed in this category help ensure the level of user access within the accounting system corresponds to the needs of their job. That's because districts should limit access accounting systems based on a staff member's role, job description, or intended use (i.e., read-only rights versus modify rights). We also looked for evidence that districts had adequate segregation of duties. For example, we expected to see that no single user had unmonitored access to school funds.

- **Figure 5** shows a summary of the results for the user-limits controls we reviewed, like ensuring the district has limited staff access based on their job role or needed use.

Figure 5. Most school districts we reviewed did have adequate user limit controls in place in practice.



Source: LPA review of school district practices and evidence of implementation.

Kansas Legislative Division of Post Audit

- As the figure shows, 11 of 20 districts had adequate practices for all 5 of the control areas. The other 9 districts lacked 1 or more of the expected controls we reviewed, but most districts had at least 4 of the 5 controls we expected to see. We describe our findings, and our work to arrive at those findings below.

- All 20 districts maintained a list of authorized users. Districts should maintain a list of system users, by permission level. We reviewed district user reports to ensure this was the case. All districts were able to provide evidence of a user report that contained permission levels. In most districts, these reports were automatically maintained and generated through their software systems.

- Nearly all districts had adequate practices related to requiring additional approval for high-dollar purchases, assigning user access levels, and ensuring only authorized personnel could modify data.

    - All but 1 district had practices in place to ensure high-dollar transactions required additional levels of approval. We looked for processes requiring additional approval for high-dollar transactions. We verified that recent high-dollar transactions had additional levels of approval (e.g., a superintendent sign off or documentation of board approval). In most cases, districts adopted a policy that purchases over $20,000 require board approval. We saw examples of board approval for these types of transactions. A couple of districts choose other dollar thresholds. We only evaluated that districts set a threshold for additional approval. We did not evaluate the appropriateness of that threshold.

    - All but 2 districts had practices in place to ensure employee access levels were based on intended accounting system use. We reviewed district processes, checklists, and software settings to ensure districts had adequate practices related to assigning access levels based on intended system usage. Generally, district staff demonstrated that system access was assigned based on job function, building code, or some other indicator of their responsibility. For example, we were able to see that teachers were assigned limited system access based on their title. In other cases, we saw that principals were assigned access based on their school building. However, 2 districts lacked adequate practices. Officials from these 2 districts were unable to demonstrate that access levels were based on job function or role. Specifically, neither district had clear criteria for granting system access based on intended use. In both districts, we found that the superintendents were granted broad access to all system accounts, despite not requiring this level of access for their job.

    - All but 2 districts had adequate practices to ensure only relevant personnel had modification permissions to accounting system data. We reviewed system software settings to ensure staff had appropriate modification rights based on their access levels. Generally, districts were able to demonstrate that modification rights were appropriate. But in 1 district, we found that modification rights were tied to a single desktop computer

rather than to a specific user. This type of setup limits the district's ability to discern between authorized and unauthorized access to their system. For example, if the credentials for the computer were shared between staff, it'd be difficult to assess who modified the system. In the second district, we found that broad modification rights for all accounts were granted to 5 staff such as the athletic director, the building principals and the transportation director. That's problematic because these staff did not need access to modify data in the accounting system to do their job.

- Some districts (7 of 20) did not have adequate segregation of duties practices. We expected districts to have practices in place that prevented any single user from having unmonitored access to districts' accounts for all phases of a transaction. We reviewed user access reports and system software settings for the selected districts. We found that 13 districts had adequate segregation of duties. In these cases, we could see that no single user had unrestricted access to the accounting systems. Instead, multiple employees were responsible for overseeing and administering the transactions in the system. However, 7 districts did not have adequate segregation of duties. Instead, only one person was able to access and approve the use of school funds. No other employees had access to review or approve those transactions. In most cases, these were smaller districts with only 1 to 3 system users. District officials told us that it is difficult to segregate duties between so few administrative staff. However, other similar sized districts had processes to separate these responsibilities between staff by doing things like escalating all purchases to the superintendent.

- User limit controls help prevent and detect fraud. Lack of controls in this area creates significant financial risk to districts that internal fraud could be taking place undetected. Especially in cases where districts have very few accounting system users, there are few staff with eyes on the system to watch for evidence of fraudulent activity. Bad actors may be able to do things like create fictitious vendors or employees to pay or otherwise embezzle school district funds with little threat of being discovered. Few users with broad access also increase the risk of collusion where multiple staff members agree to manipulate financial records.

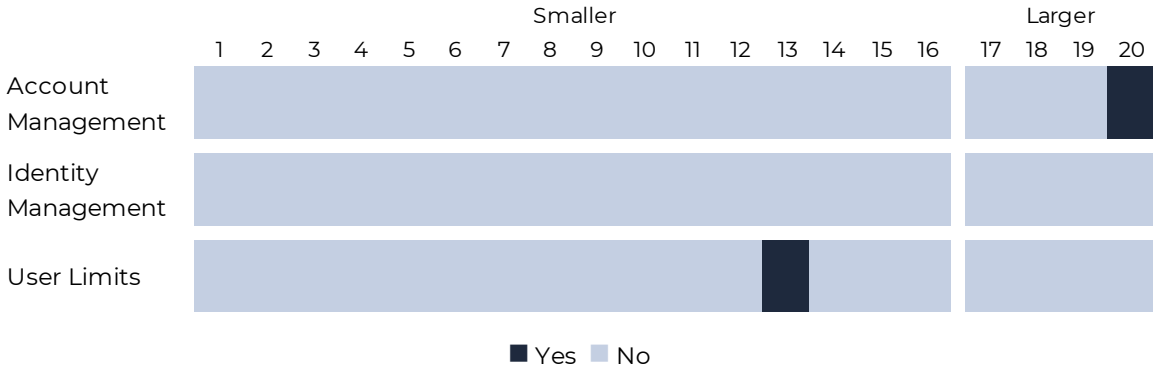
Finally, very few of the 20 districts we reviewed had adequate written policies related to any access controls for their accounting systems.

- In addition to practices that districts use, we looked to see whether districts had formal, written policies. We evaluated whether the 20 districts we selected had adequate formal, written policies in place to address each control across the 3 categories we reviewed. We determined that a district had adequate policies if it had written policies for all 3 account management controls, all 4 identity management controls, and all 5 user limit controls.

- Districts generally did not have written policies in place. **Figure 6** shows the districts with policies in place for each of the 3 control categories we reviewed.

As the figure shows, very few districts had adequate written policies, and none of the 20 districts had adequate policies across all 3 categories.

Figure 6. No school districts had adequate written policies for all 3 categories of controls we reviewed, and very few had policies at all.



Source: LPA review of school district policies.

- Some district officials said they relied on built-in security features from their software vendors. These were things like the software system automatically assigning unique usernames and requiring multi-factor authentication. However, we expected districts to maintain written policies that describe their expectations regarding standard IT security controls (e.g., passwords and MFA) as well as accounting practices (e.g. assigning access levels and modification rights).

- Formal, written policies ensure that staff expectations are clear and that staff have a consistent understanding of those expectations. Written expectations also help ensure processes remain consistent. That's especially important when staff with specific roles or knowledge about the accounting system leave the district, or the district changes software vendors.

Smaller school districts tended to lack more access controls for their accounting systems, but all districts could benefit from formalized policies.

- Across all 3 categories we evaluated, larger districts were more likely to have adequate control practices in place. 3 of the 4 larger districts had adequate practices in at least 2 of the 3 categories we evaluated. That's likely because larger districts tend to have more staff dedicated to managing their IT systems, including the accounting system. In theory, these staff can focus more time on implementing security controls and best practices. Further, many larger districts have more modern accounting systems that have more built-in security capabilities such as unique usernames or MFA.

- Across all 3 categories we evaluated, only 1 of the 16 smaller districts had adequate control practices in place in at least 2 categories. District officials

from smaller districts told us that they did not have written policies due to their size. Many of these districts also have few system users, which gives the impression of limited risk. Some districts told us that having few users meant that there were fewer opportunities for IT security issues to occur. However, districts often have misplaced trust in small or seasoned staff. Districts may let down their guard in these cases and be more susceptible to fraud. Further, hackers outside the district have a better chance of gaining access to a system when controls are lacking.

- Smaller districts also tended to have fewer staff and less turnover, which means that the process of creating, modifying, and terminating accounts happens infrequently. As a result, district officials told us that informal practices are adequate in their situations.

- No districts had adequate written policies across all areas we reviewed. A couple of larger districts told us that they were currently in the process of writing policies. Many smaller districts told us that written policies had not been developed given their district staff size. Both large and small districts told us that their accounting system software's built-in features were sufficient in many cases. However, policies are important because they establish clear and consistent expectations across staff which helps secure districts' accounting systems from unauthorized use.

KSDE told us that districts have been moving to computerized systems quickly, and it was not surprising that districts have very few policies.

- We talked with KSDE officials about our results. They told us that accounting systems have evolved very quickly. Further, officials noted that for many controls such as segregation of duties and differentiating access levels, having few staff is a limiting factor.

- KSDE officials also told us that many districts rely on the Kansas Association of School Boards (KASB) for guidance in writing policies. This means districts often do not have many policies beyond those they adopt from KASB. KASB guidance does state that superintendents are responsible for ensuring that accounting systems have internal controls, but this is too vague to be considered sufficient for the types of access controls we evaluated. It was unsurprising to KSDE officials that many districts lacked district-level formal policies specific to accounting system access. KSDE officials told us that their own guidance is more focused on practices rather than formalized policies.

- KSDE officials told us that they do not require that districts have any specific policies or practices in place. However, we talked with officials about the resources they provide to districts. They told us that KSDE provides guidance in line with the controls we reviewed in this audit on an individual basis when districts ask for specific assistance in this area. They told us that IT staff at KSDE have also presented security guidance in the past, and they currently have plans to provide more formal guidance in the future.

Conclusion

The lack of written policies or well-defined practice leaves districts' accounting systems vulnerable to unauthorized access. We found that school districts are not held to any standard set of IT security requirements. As such, districts took different approaches to managing their accounting system access. Larger districts met more of the access controls we evaluated. That's largely because they have the staff, software, and knowledge to maintain a more secure system. Smaller districts tended to lack many of the access controls we evaluated. In several cases, smaller districts described ad-hoc or informal practices related to access controls. While smaller districts may have less staff and little turnover, it's still critical they implement access controls to help prevent unauthorized access to this sensitive information system.

Recommendations

1. We recommend that the Kansas State Department of Education develop resources such as policy templates and provide routine guidance to school districts related to accounting system access controls, specifically in the 3 categories of account management, identity management, and user limits controls.

2. We recommend that the districts in our selection implement security practices related to accounting system access controls, specifically in the 3 categories of account management, identity management, and user limits controls and codify those practices in written policy.

Agency Response

On August 19, 2025 we provided the draft audit report to the Kansas State Department of Education and the 20 school districts in our selection. We made minor changes to the draft based on officials' feedback. KSDE and school district officials generally agreed with our recommendations and agreed to make changes based on them. A few districts contended that they already have best practices in place related to access controls. We agree that all districts have at least some access controls in place. However, none of the 20 districts were able to demonstrate that practices were in place to address all 12 of the access controls we evaluated.

Kansas State Department of Education Response

KSDE provides ongoing information for IT security to school districts. This

information is primarily provided through conference presentations, working group participation, and responding to school district questions. KSDE is already working on more formal guidance for IT security best practices that will be provided to districts for their consideration.

KSDE is also happy to provide this information to the Kansas Association of School Boards (KASB). KASB is better positioned to provide districts with model policy for the local school board's consideration.

The guidance presented will cover the three areas suggested by LPA (account management, identity management, and user limits/controls). KSDE does not provide districts with specific accounting guidance as each district is required to have an audit by a Certified Public Accountant who would provide this type of guidance.

District 1 Response

We want to thank the Legislative Post Audit team for the recommendations to improve our access controls of accounting systems within our school district. We are evaluating these recommendations and plan to work with our school district personnel to improve our access control systems based on these recommendations and appreciate the thorough and professional nature of the LPA report.

District 2 Response

The Board of Education will adopt accounting system access and security policies at their next meeting. These policies will address account management, identity management, user access limits, and oversight and security.

District 3 Response

Our district acknowledges the recommendation and recognizes the importance of implementing robust security practices within our accounting system. We will review and enhance our current procedures related to account management, identity management, and user access limits to ensure they align with best practices. Additionally, the district will codify these procedures in written policy to provide clear guidance, maintain accountability, and support consistent application across all relevant staff. Implementation timelines and responsible parties will be identified to ensure these controls are effectively integrated into daily operations.

District 4 Response

Thank you for your recent findings and recommendations regarding the security of our accounting system. We appreciate the thoroughness of your review and your commitment to helping us maintain compliance and protect the integrity of our financial processes.

As a small school district, we would like to provide some context that we hope will be

considered in the evaluation and implementation of recommended controls. Unlike larger districts, which often have multiple staff dedicated to accounting and finance functions, smaller districts like ours often operate with very limited personnel. In some cases, a single individual is responsible for managing the entire accounting system, from processing payroll to reconciling accounts and generating reports. This staffing limitation creates inherent challenges when implementing certain controls, such as segregation of duties, which are standard practice in larger organizations.

We fully acknowledge that changes in our internal processes need to take place to strengthen accountability and mitigate risk. While limited staffing presents challenges, it does not eliminate our responsibility to ensure strong financial oversight. We are committed to reviewing your recommendations and working toward realistic, effective improvements that enhance the security of our accounting system while remaining feasible within our operational constraints.

Additionally, when new requirements are introduced by the Kansas State Department of Education (KSDE), it can be especially burdensome for small districts to respond quickly and efficiently. While we fully support the goal of increased accountability and security, it is important to recognize that policies and procedures designed for a district of 25,000 students are not always scalable to one serving 250. Flexibility and adaptability in control expectations are essential to ensure compliance without overextending already limited resources.

We welcome the opportunity to work with your team to explore practical, risk-based alternatives that achieve the necessary safeguards while acknowledging the operational realities of small districts. Your continued partnership and understanding are greatly appreciated as we strive to maintain both security and efficiency in our financial operations.

District 5 Response

The district contends that the recommended practices regarding accounting system access controls—including account management, identity management, and user limits controls—are currently in place and actively followed. However, we acknowledge the need to strengthen these practices by formalizing them in written policy. We will research best practices and develop formal, documented policies to ensure that these procedures are consistently applied and clearly communicated.

District 6 Response

We have received and read your audit report Evaluating Access Controls of School District Accounting. We have carefully reviewed the document, and while we do have good access controls in place, we are working on implementing written policy and/or guidelines in regards to our internal controls.

District 7 Response

Our school district plans to create a more formal policy on system access controls in

the areas of Account Management, Identity Management, and user limits. The software system we utilize has processes already built into the system, but will rewrite the processes built in into the system into policy for our district office.

District 8 Response

We plan to implement these changes in our district.

District 9 Response

We will put our practices and procedures into written documents. We have already begun this process.

District 10 Response

We agree with both recommendations and recognize the importance of strengthening access controls within accounting systems to enhance security and accountability.

First, we support the recommendation for the Kansas State Department of Education to develop standardized resources such as policy templates and to provide ongoing guidance to school districts. Establishing consistent practices across the state—particularly in the areas of account management, identity management, and user limits controls—will help ensure that all districts are equipped to manage system access effectively and securely.

Second, we concur with the recommendation that the selected districts implement robust security practices in these three key areas and formalize them in written policies. Clearly documented procedures not only help maintain compliance and transparency but also support continuity and risk management across district operations.

Together, these steps will promote stronger internal controls and better protect financial systems throughout Kansas school districts.

District 11 Response:

Thank you for all of your work on the audit. Our plans to implement recommended changes suggested.

District 12 Response

Our district appreciates the recommendations provided through this audit. The district agrees with the importance of strengthening security practices related to accounting system access controls.

We will review our current procedures in the areas of account management, identity management, and user limits to ensure they align with best practices. In addition,

we will work to develop and codify these practices into written policy for consistency and accountability.

Our goal is to implement these improvements in a timely manner to enhance the security and integrity of our accounting systems.

District 13 Response

Response to the Report:

We found the report to be thorough and enlightening regarding the state of access control of school districts accounting systems across the State of Kansas. The report clearly details areas of need in this area that would provide increased security measures to ensure better controls.

*Note: This audit work took place at an absolute HORRIBLE time of the school year. We were in the process of trying to close out the budget from the previous school year when this all took place. Our key people who needed to be doing that work had to be taken from that essential work to accomplish this audit work. That was EXTREMELY disheartening. This audit was important, but it needed to take place at a different time of the school year.

Response to the Recommendations for Us:

1. We plan on adding a form to our on-boarding documentation that will trigger giving employees access to the accounting program.
2. We will be implementing a multi-factor authentication post-login verification for privileged access.
3. We are adding a form to our exit paperwork for when an employee leaves us that will trigger removing an employee from our accounting system upon exist from the system.

District 14 Response

Our district plans to implement the recommended security controls. We currently try to follow security procedures. However being a small district, it can be difficult to follow such procedures because of the lack of staff and resources.

District 15 Response

The district has already started the process of writing new policy for district office processes.

The district's security practices related to accounting system access controls will be on the work list for policy review or new policy. The following categories of:

- Account management
- Identity management

- Use limits controls

will be addressed during the 2025-2026 school year.

District 16 Response

I agree with the findings and will work to implement written policies surrounding procedures for timely change processes for termination of employee access or change requests.

In response to the segregated access control, we have multiple steps in place to oversee transactions across several layers, requiring signatures from more than three people. We have one board clerk and one superintendent. However, I can see that one more person with access would allow more transparency.

District 17 Response

Since the audit has finished the district has taken multiple steps to incorporate suggestions from the LPA. Some of the items include but are not limited to:

- Creating clear policies in handbooks outlining the appropriate enhanced access level(s) to individuals in specific roles;
- Incorporating forms to fill out by the appropriate administrator for enhanced access to individuals which are reviewed by administration;
- Setting up clear timelines for when enhanced access needs to be adjusted, including employee termination

Additional policies/practices are in the process of being developed and implemented as it relates to user limits and will be implemented as soon as they are complete.

District 18 Response

Our district acknowledges the importance of formalizing security practices related to accounting system access controls. While many of these practices were already in place, we recognize that they were not fully documented in written policy. To address this gap, the district is actively developing comprehensive Handbooks and Standard Operating Procedures (SOPs) that will document and establish practices in the areas of account management, identity management, and user limits controls. These documents will serve as both guidance and accountability measures to ensure consistent implementation, regular review, and continuous improvement of our access control practices.

District 19 Response

Our district will collaborate with other public school districts, the Kansas Association of School Boards and the Kansas State Department of Education to develop and implement written policies and procedures that ensure effective account

management, identity management, and secure user access controls within our financial accounting systems.

District 20 Response

Response to the audit:

We appreciate the opportunity to review the Legislative Post Audit report and its recommendations. We recognize the importance of robust access controls to safeguard our accounting systems and data as well as maintain accountability.

The audit's findings related to account management, identity management, and user limits have been carefully reviewed by district leadership. While several practices are already in place and being followed, we acknowledge that enhancements and formalization in written policy will further strengthen our internal control environment.

Accordingly, the district intends to use the audit's findings and recommendations to:

- Codify Practices in Policy: Document and consolidate existing practices into written policies to ensure consistency and sustainability.
- Refine Account Management: Strengthen procedures for authorizing, approving, and documenting user access to ensure appropriateness and timeliness.
- Enhance Identity Management: Evaluate authentication and account verification processes and implement improvements where necessary.
- Review and Limit User Access: Continue to restrict system access to only those duties essential to an employee's role and ensure prompt removal or modification of access when no longer required.

The district intends to implement the recommendation provided. These steps will improve the effectiveness of our access controls and support ongoing compliance with best practices for security and accountability.

Response to the Recommendation:

The district intends to implement this recommendation. Existing practices in these areas will be consolidated and codified in written policy, and enhancements will be made to ensure comprehensive account management, strengthened identity management, and proper user limits.

Appendix A – Cited References

This appendix lists the major publications we relied on for this report.

1. Marshall Public Schools (September, 2021). *Missouri State Auditor*.

2. School Districts' Self-Reported IT Security Practices and Resources (October, 2021). *Kansas Legislative Division of Post Audit*.