KANSAS LEGISLATIVE
DIVISION of POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

Information Systems: Reviewing Specific IT Security Controls Across State Agencies and School Districts (Part 2)

January 2024

Report Number: R-24-001

Introduction

K.S.A. 46-1135 authorizes our office to conduct information technology audits as directed by the Legislative Post Audit Committee. These audits are conducted on a 3-year cycle. During its December 2022 meeting, the Committee approved a proposal to change the format of our IT audits. For CY 2023 we reviewed multiple agencies at the same time, on select IT security controls and issue public reports. Our previous audits were in-depth reviews of IT security at individual agencies, that resulted in confidential reports. The Committee also approved inclusion of a handful of school districts as part of the IT audit work.

Objectives, Scope, & Methodology

Our audit objective was to answer the following question:

1. Do selected state agencies and school districts adequately comply with certain information technology security standards and best practices?

We selected 12 state agencies and 3 school districts as part of this audit. We chose 15 IT security controls across 3 IT control areas. Those areas were Systems Operations and Configuration, Continuity of Operations Planning, and Data Center Security. Aside from 1 best practice, we evaluated IT controls already codified in the state's security and business contingency policies.

We focused on entities' security posture at the time of the audit. Our fieldwork was staggered across the entities, starting on July 12, 2023 and ending December 1, 2023. To assess compliance, we interviewed staff, reviewed relevant policies and procedures and evaluated relevant computer settings. We analyzed asset inventories and did sampling work related to a handful of computer assets. We reviewed vulnerability scan results, continuity of operations manuals, and other applicable documentation as necessary. Lastly, we conducted site visits to all data centers for entities that had them.

We limited our work to a small number of IT areas and a handful of controls. At times, we were unable to test all selected requirements. Because we did not do a more comprehensive review, other security control weaknesses may exist that represent unknown risks.

Additionally, some work included samples. We generally drew samples randomly, but at times we used judgmental sampling. Results from that work cannot be projected. However, problem findings identified as part of that work represented security threats which in and of themselves provided us with reasonable assurance that problems existed.

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. In this report, we summarized IT security findings across 15 entities. Readers may have expected to see findings attributed to individual entities. As agreed to by the Committee, we avoided attributing findings to specific auditees to avoid reducing their security posture further. Finally, we made entity-specific audit documentation confidential under Kansas Open Records Act exemptions K.S.A. 45-221(a) (12) & (45).

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. Because the scope of this audit was to evaluate selected information security controls, our planning, fieldwork, and the final report are designed to meet these standards.

Our audit reports and podcasts are available on our website (www.kslpa.org).

About half of the 15 entities we audited did not substantively comply with selected IT standards and best practices.

Background

All state agencies across 3 branches must follow Information Technology Executive Council policies to protect sensitive information against data loss or theft, and be able to resume critical operations following a disruption.

- Many Kansas agencies collect sensitive data on taxpayers and citizens. This data can include tax records, criminal records, and health care information. Several agencies maintain confidential information that have significant penalties for loss or disclosure.

- Kansans depend on governmental agencies to protect their personal information. For this reason, it's important state agencies adhere to strict IT security policies and procedures.

- 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 and procedures for all state agencies.

- ITEC created various policies, including policy 7230A on IT security standards. This serves as the state's official IT security policy. That policy governs "all Kansas branches, boards, commissions, departments, divisions, agencies and third parties used to process, transmit or provide business capabilities on behalf of Kansas state government." In other words, all state agencies must adhere to the IT security policy. IT security standards generally include requirements for policies and procedures. They also include requirements for physical, system, and application controls. These controls reduce the risk that confidential data is compromised, lost, or stolen.

- The state's IT security policy is similar to security standards published by other organizations. The National Institute of Standards and Technology (NIST) standards come from the federal government. The Center for Internet Security (CIS), and the International Organization for Standardization (ISO) both produce standards that are used widely throughout the world.

- ITEC also created business contingency policies to help entities continue critical operations following any disruption, and resume normal operations within a reasonable period of time. Those policies cover continuity of operations planning and disaster recovery planning. They also cover business impact analyses—the process of analyzing what effects organizational disruptions may have on entities' mission-critical activities.

- Some state agencies may be subject to additional state or federal laws to protect sensitive data. For example, the federal Health Insurance Portability and Accountability Act (HIPAA) requires entities to protect relevant health information. The Internal Revenue Service (IRS) imposes extensive security guidelines for entities that maintain tax data.

In an effort to improve IT security compliance statewide, the legislature passed the State's Cybersecurity Act in 2018.

- It pertained to most executive branch agencies with a few exceptions. Elected office agencies, the Adjutant General's department, the Kansas Public Employees Retirement System, the regents' institutions (universities), and the Board of Regents were exempted. It did not cover judicial and legislative agencies.

- It created the Kansas Information Security Office (KISO) as a separate state agency to administer the Act. KISO helps agencies develop cybersecurity programs and follow state and federal security standards. KISO also provides a cybersecurity training program at no cost to the agencies. KISO is led by the state's Chief Information Security Officer (CISO), who helps coordinate cybersecurity efforts between agencies.

- It also codified cybersecurity service costs. The Act allowed KISO to charge agencies for certain security-related functions. It also allowed agencies to pay for cybersecurity services from several sources, including fee funds.

- The Act clarified that agency heads remain responsible for their agency's security postures. Agency heads have several specific responsibilities. Those include the following:

    - ensuring an agency-wide information security program is established;
    - designating an information security officer;
    - taking part in annual agency leadership training on specific cybersecurity-related topics;
    - notifying the state's CISO about breaches within 48 hours after discovery; and
    - submitting a cybersecurity report to the CISO every 2 years.

In 2023, the legislature passed House Bill 2019 which strengthened or added components in the 2018 Cybersecurity Act.

- It required all public entities experiencing a significant cybersecurity incident to notify KISO within 12 hours of discovery. For purposes of reporting security incidents, the law defined a public entity as any public agency of the state or political subdivision. As such, school districts, counties, cities, and similar governmental entities were included. The law defined significant cybersecurity incidents as those that "result in or likely result in financial loss

or demonstrable harm." The law also established incident notification requirements for government contractors, election data, or criminal justice data.

- It required KISO to perform confidential audits of executive branch agencies. Those audits should cover applicable state and federal laws, rules and regulations, executive branch policies and standards, as well as ITEC policies.

- The Act required KISO to make a cybersecurity awareness training program available to all branches of state government. Previously, the law required KISO to provide awareness training only to executive-branch agencies at no cost. The law also removed the requirement to make the training available free of charge.

- It added new controls agency heads are responsible for: disabling login credentials on the day employees depart, and ensuring employees with access to IT systems get at least 1 hour of IT security training.

Local entities are not required to follow the state's ITEC policies to protect sensitive information and to plan for business contingencies.

- Local entities such as school districts or city and county governments also collect sensitive data on Kansans. This data can include K-12 student records, tax records, and health care information.

- As mentioned earlier, 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 and procedures for state agencies.

- The state's IT security and business contingency policies created under ITEC authority do not apply to local governments including school districts. Local entities may be 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 law requires school districts to implement specific IT security controls.

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

    - creating a K-12 technology council;

    - creating an IT technology webpage (includes 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 districts should consider when developing security policies.

However, the department stopped short of requiring districts to follow a minimum set of security standards.

- In October of this year, the K12 Security Information exchange (K12 SIX), a nonprofit organization for members of the K-12 education community, released guidance on essential cybersecurity protections for school districts. K12 SIX also released implementation standards and a self-assessment tool to help districts implement those security protections.

State and local entities must balance business risks against security risks.

- Government entities across the nation are targets of data breaches because they maintain valuable information. Several recent Kansas-specific security incidents are listed below:

  - On October 12, 2023, a cyberattack shut down the Kansas judicial branch's information systems. This outage affected daily operations of the state's appellate courts and district courts in 104 counties. The Kansas Supreme Court's public statement on November 21 said the attack appeared to be foreign and sophisticated. The statement said criminals had threatened to post stolen data to a dark website.

    At the time of writing this report, state and federal law enforcement and other stakeholders were conducting a comprehensive review. In the meantime, court filings had to be submitted in paper. The judicial branch opened two public access service centers to provide remote support to district courts and allow for searches of public district court cases.

  - On March 28, 2023, the Newton Public School District detected a network security incident. School was canceled for 2 days. According to news reports, the district shut down affected systems to secure the network. They also engaged forensic specialists to investigate the incident. District officials were working with law enforcement, but more information was not publicly available about this event.

- Generally, state agencies and local entities may prioritize their core mission over information security. Agencies focus on their core missions such as collecting taxes, issuing various types of licenses, or protecting the state's natural resources. School districts' missions center on educating children from kindergarten through 12th grade.

- Implementing security controls takes staff, time, and resources. Security controls often can reduce staff speed or limit functionality. This creates a conflict between business needs and security risks.

- Entities must understand and evaluate their security risks to make informed decisions on how to best secure their data, while carrying out their primary missions.

Our IT audits continue to help evaluate the state's IT security posture.

- Except for the IT security audits conducted by our office, there are no regular external evaluations of agencies' security practices to ensure they comply specifically with ITEC security standards. A number of state agencies do receive comprehensive federal audits through the Internal Revenue Service, Social Security Administration, or Center for Medicaid Services. Additionally, a number of agencies with financial systems receive financial audits which includes an IT controls component.

- Since 2014, our office has produced IT security audits on many state agencies. Individual audits were kept confidential under K.S.A. 45-221(a)(12) because their information could jeopardize agencies' security.

- Our office produced public 3-year summary reports in December 2016 (20 agencies), February 2020 (19 agencies), and most recently in December 2022 (21 audits on 20 entities).

- Since 2020, the Legislative Post Audit Committee (LPAC) approved adding a small number of school districts to our audit work. This mandate continued in the current 3-year plan (2023-2025).

- During its December 2022 meeting, LPAC asked us to conduct IT audits for multiple agencies at the same time, but examining fewer controls. We released the first public audit under this new direction in July 2023.

Method

We audited 15 entities on selected controls related to Systems Operations and Configuration, Continuity of Operations Planning, and Data Center Security.

- The 15 entities we audited can be found in **Appendix B.**

    - We selected 12 state agencies based on their inherent risk scores and a lack of previous audit. Specifically, agencies had to have a risk ranking of 'medium' or higher (a scoring system we created based on the type and amount of confidential data agencies maintain, as well as other factors). Second, we selected agencies that had never received an IT security audit from us, or had not been audited by us in at least 5 years.

    - We selected 3 school districts because of their willingness to undergo an audit. In 2021, we conducted a survey of 42 larger school districts to learn which ones were willing to receive an IT security audit. The 3 districts we selected had "opted in" on the survey and were located across the state.

- We evaluated the entities' compliance across 3 subject areas: Systems Operations & Configuration, Continuity of Operations Planning, and Data Center controls. We limited our audit to these areas because our past audits showed agencies struggled to comply in those areas. They also presented a mix of technical and non-technical subjects which helped us stay within legislative time constraints.

- We evaluated 5 controls in each subject area, for a total of 15 controls. Controls are a type of requirement, which if followed, help strengthen entities' information security. We selected these controls because they are generally accepted in the industry as foundational to an entity's IT security posture. 14 of the 15 controls came directly from the state's ITEC policies (ITEC 5300, 5310, and 7230A). We added the last control based on a state law requiring fingerprint background checks for individuals with unescorted access to the state's data center. We thought this was a sufficiently important control to apply to all data centers and therefore added it to our audit program.

- It's important to remember that the state's IT security policy 7230A has 13 areas and nearly 120 controls in total. Other standards issued by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) are larger and more complex. For example, CIS has 18 control areas and over 150 controls. Our review of 15 controls across 3 areas represented a small set of basic security controls. Non-compliance with these may indicate systemic issues with the entities' overall security posture.

- As mentioned previously, Kansas school districts are not subject to the state's IT security or business contingency planning policies. Similarly, KSDE doesn't impose security or disaster resiliency standards on districts. However, KSDE has provided a security standards template for school districts to consider. That document is similar to the state's security policy. The U.S. Department of Education's Office of Safe and Supportive Schools encourages school districts to develop a continuity of operations plan. As a result, we felt comfortable evaluating school districts against the same 15 controls.

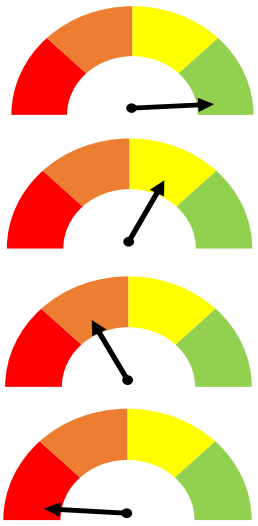
We followed previously established scoring processes during this audit to evaluate entities' security compliance.

- In our prior IT security audits, we developed a robust process to score entities' performance within each control area. Although we only audited 3 areas in this audit, we decided to use the same scoring method:

- We awarded between 0 and 3 points for each control we evaluated. Generally, we awarded 3 points for full compliance and 2 points when the entity was mostly compliant. We awarded 1 point when the entity had taken initial steps towards compliance, and 0 points if the entity had no process in place to adhere to the requirement.

- The resulting points in each area were converted to a percentage which fell into 1 of 4 possible quadrants. **Figure 1** shows the possible results.

Figure 1 - Categorization of Results For 3 Audited Control Areas



Green indicates 76%-100% compliance. This means **minor/no control issues** within the audited area.

Yellow indicates 51%-75% compliance. This means **moderate control issues** within the audited area.

Orange indicates 26%-50% compliance. This means **major control issues** within the audited area.

Red indicates 0%-25% compliance. This means **significant control issues** within the audited area.

Source: LPA methodology

- We set the cutoff for substantial compliance at 50%. Entities scoring above 50% (yellow and green) were considered to have substantively complied in that area. It should be noted this was a fairly liberal threshold. Entities scoring yellow or green generally still had findings to work on.

Overall Outcomes

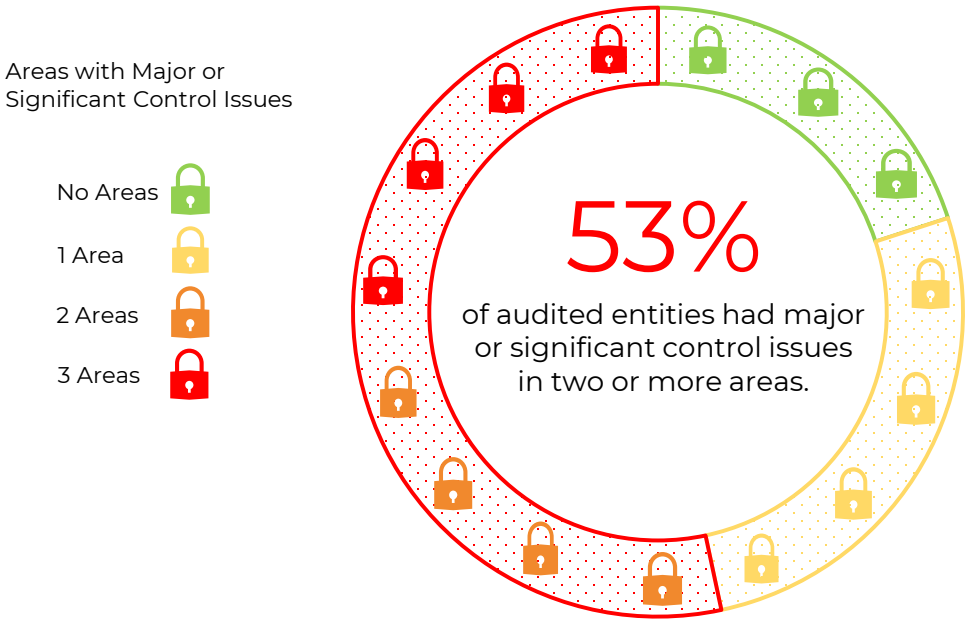
8 of 15 entities did not substantively comply with IT standards and best practices in at least 2 of 3 subject areas we evaluated.

- We expected entities to comply with the controls we evaluated because they were state requirements or generally accepted industry best practices.

- 4 entities did not substantively comply with any of the 3 areas. Another 4 didn't substantively comply with 2 of 3 areas. **Figure 2** shows the entities'

performances across the 3 areas. As the figure shows, only 3 entities substantively complied with all tested areas.

Figure 2: Eight of fifteen entities did not substantively comply with selected IT security controls in two or more areas (a).



(a) Two agencies were evaluated on only 2 of the 3 areas. Those 2 agencies didn't utilize a Data Center so there was nothing for us to review.

Source: Summary of LPA analysis of selected IT security controls at 15 entities.

- When entities don't have adequate security controls, the risk increases that their confidential data is lost or stolen. This can occur when entities have a significant security incident or when they can't recover from a service disruption. Entities can also face financial penalties and reputational damage. Similarly, inadequate business continuity processes increase the risk that entities cannot resume operations timely.

- Based on our interactions with staff, observations made during the audit, and cumulative years of expertise, the findings show there's a continued lack of top management supervision of many entities' IT security functions. This is often referred to as the "tone at the top." It is ultimately the responsibility of entity top management to ensure adequate safeguards are in place. These protections limit the entity's risk to data exposure or loss. They also ensure an entity can resume mission-critical operations as quickly as possible. Unclear or

missing documentation of contractors' roles and responsibilities also contributed to the issues we saw.

Systems Operations and Configurations Results

Entities should actively manage IT assets and monitor networked devices to ensure they are protected from vulnerabilities.

- Although there are many controls that could fit under this category, we selected 5 that we think are the most important.

- We evaluated entity compliance with 5 controls related to systems operations and configuration. Those 5 controls, and our work to test them, are paraphrased below. **Appendix C** also has more details on these 5 controls.

    - IT Asset Inventory: Entities should keep an inventory of IT equipment, update it as changes happen, and review it at least once a year. We reviewed entities' IT inventories to ensure key fields weren't blank or duplicated. We also checked to see if former employees still had assets assigned to them. Lastly, we tested between 5-25 randomly or judgmentally selected computers, laptops, or tablets at each entity to see if they could locate the items.

    - IT Asset Ownership: Inventories must identify and document the ownership of each asset. We reviewed inventories to ensure IT assets had been assigned to individuals. We also checked to make sure they had not been assigned to general areas.

    - Vulnerability Scans: Entities must scan all networked computers and servers for vulnerabilities at least monthly. We checked that scans were set up to scan at least once a month and to look deep enough into system files to see vulnerabilities. We interviewed IT staff and reviewed computer settings and scan results to understand entities' processes for this control.

    - Patch Management: Entities must have a documented patch management process. We interviewed staff about their processes to patch Microsoft and 3rd party software. We also reviewed prior vulnerability scan results to check whether the described processes were effective.

    - Anti-Virus (AV) protection: Entities must use antivirus software on systems that contain restricted-use information. We interviewed staff and viewed software settings to make sure scans were set up correctly. This meant covering necessary machines and keeping users from disabling the protection.

- For this area, 2 points are important to keep in mind:

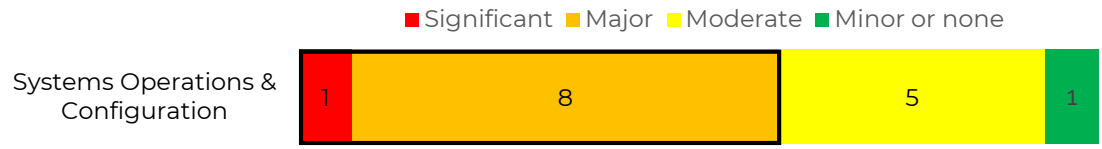
- We requested and reviewed entities' IT asset inventories to check whether key fields were populated, identifying numbers weren't duplicated, and so forth. We didn't verify whether items were missing from the list. Also, the inventories we saw varied considerably in the level of sophistication, what types of assets entities inventory, and the type of information maintained for each asset.

- We didn't run our own scanning tests due to the amount of time it would have taken both to perform and analyze. Instead, we relied on entities to have a process for periodic scanning and resulting scan reports for us to review.

9 of the 15 entities did not substantively comply with the systems operations and configuration controls we evaluated.

- **Figure 3** summarizes our findings in this area. As the figure shows, 1 entity had significant control issues and 8 had major control issues in this area. This accounted for nearly two-thirds of the entities evaluated. As shown in the figure, 5 other entities had moderate control issues. Only 1 of the 15 entities had minor issues (scoring above 75%). Our findings are summarized below.

Figure 3: Nine of fifteen entities did not substantively comply with selected system operations and configuration controls.



Source: Summary of LPA analysis of selected IT security controls at 15 entities

Kansas Legislative Division of Post Audit

- Maintain and update an IT asset inventory including ownership: All entities generally had inventories with IT assets. However, most inventories were missing or had duplicate information in key data fields (e.g. serial numbers), and assets weren't always tied to owners. Many agencies' inventories had computer items still assigned to employees who no longer worked for the entity. More than half of the entities were not able to find 1 or more of the computers we sampled.

- Vulnerability Scans: Given the importance of scanning networked computer assets periodically, we were surprised to find many entities

had serious control issues in this area. 5 entities didn't scan their networked computers at all. 6 more entities didn't scan all networked machines. For example, at least 2 entities did not scan computers of staff working from home or in the field. Staff at 3 entities did not know whether servers housed in contracted data centers were being scanned, or they told us they didn't have access to scan results. Lastly, 5 entity-provided scans were partly or completely uncredentialed. Uncredentialed scans do not provide enough insight into computer vulnerabilities and can provide a false sense of security.

- Patch Management: Some entities relied on automatic patch management for Microsoft vulnerabilities. Some entities had no processes for 3rd party software patches. Entities also relied on staff to pull down available updates and did not check whether those updates were installed. Staff often did not have a documented process to ensure patches actually were applied. At most entities with prior scans available for review, we found old vulnerabilities still existed months or years after a patch came out. This indicated the entity's patching process was inadequate.

- Anti-Virus protection: At several agencies, we found poor AV settings. This included allowing staff to disable the protections. A few entities could not show evidence that weekly scans occurred. Lastly, we noted several entities did not enroll all computers in AV services.

- Weaknesses in system operations and configuration increase the risk that an entity's computers or network will be compromised. According to the Center for Internet Security (the organization that publishes the CIS Critical Security Controls Standards), having a complete, updated IT asset inventory is a critical first step toward knowing what needs to be protected. A systematic approach to scan and patch known vulnerabilities will reduce the risk that attackers can successfully compromise an entity's computers. And having good AV protection lowers the risks that computers can get infected with a virus.

We think top management didn't sufficiently monitor compliance in this area.

- Several entities relied on contracted staff or support from KISO to administer certain systems operations and configurations controls. Contract agreements didn't always include all the expected security services. For example, a couple of entities' contracts only covered vulnerability scanning services for servers, not computers. Officials from at least one of those entities did not appear aware of this until our audit. KISO officials also stated that the ISOs embedded at several entities were not responsible for patching vulnerabilities and that agency IT staff were responsible for that role. Management ultimately is responsible for ensuring all necessary security controls are in place, either through contracting or internal staff.

- Based on our work and interviews with auditees, we noted that scanning and antivirus protection weren't always set up properly. For example, we saw several faulty or incomplete scan reports for networked computers or data center servers. This was the case at entities that relied on KISO for this, as well as entities that managed vulnerability scanning in-house. Management is responsible for ensuring that security controls function as intended, regardless of who is doing the work.

- Lastly, we noted that several entities didn't appear to have sufficient IT staff or sufficiently experienced staff to ensure compliance. Ultimately, management is responsible for systems operations and configurations security, even when delegating work to other parties.

Continuity of Operations Planning Results

Entities should have a formalized plan to return to their regular business operations after having experienced a major disruption.

- Continuity of Operations Plans (COOPs) outline ways to get the entity back to regular operations. They are also intended to minimize downtime. Business Impact Analyses (BIAs) are related to COOPs. They help entities prioritize their critical information systems and set critical timelines related to restoration.

- We evaluated whether the entities complied with 5 controls related to continuity of operations planning. Those 5 controls, and our work to evaluate them, are described below. **Appendix C** has more details on these 5 controls.

    - COOP Maintenance: Entities must put in place, maintain, and test continuity of operations plans. Portions of the plan - which list specific staff with responsibilities - must be reviewed twice a year. We requested and reviewed entities' plans. We also checked that plans did not include former staff.

    - COOP Content: The plan should include information on specific topics. Example topics include disaster detection and response, delegations of authority, orders of succession, and other content. We reviewed entities' plans for such content.

    - Review and Test COOP: Plans should be reviewed and updated every year and tested every 2 years. We evaluated existing plans and whether the entity had tested their plan timely.

    - Business Impact Analysis (BIA): A BIA analyzes what effects a disruption could have on entities' mission-critical activities. It also identifies and prioritizes IT systems to aid in the recovery process. We interviewed

staff, and reviewed documents that may include a BIA.

- Recovery Time & Recovery Point Objectives (RTO and RPO): As part of the BIA, entities should decide how long they think it will take to bring a critical information system back up (RTO). They should also decide how much data they are comfortable with losing in the event systems go down (RPO). This information informs backup processes. We interviewed staff and reviewed applicable documentation for this information.

- In this area, 2 points are important to keep in mind:

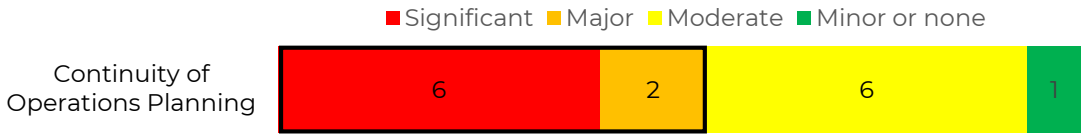
  - COOP requirements for all state agencies have been in place for years. In Fall of 2021, ITEC strengthened the requirements to include BIA, RTO and RPO components. In July of this year, Governor Kelly issued an Executive Order (EO) to mandate agencies under her purview to adopt a COOP by December 2023. During our fieldwork we noted several agencies had been working on their COOP. However, several agencies didn't have an approved COOP at the time of fieldwork, and were therefore listed as non-compliant.

  - We didn't formally review the EO to see how its requirements compare with the requirements set forth in the state's ITEC policies. We noted each has components not present in the other. For example, the EO requires status reports, and ITEC policies mandate COOP tests.

8 of 15 entities did not substantively comply with selected Continuity of Operations Planning controls we audited.

- **Figure 4** summarizes our findings in this area. As the figure shows, 6 entities had significant control issues and 2 had major control issues in this area. This means over half of the entities did not substantively comply (scoring 50% or less) in this area. As shown in the figure, 6 entities had moderate control issues. The remaining entity had minor findings. Our findings are summarized below.

Figure 4: Eight of fifteen entities did not substantively comply with selected continuity of operations planning controls.



Source: Summary of LPA analysis of selected IT security controls at 15 entities

- COOP Maintenance and Content: 4 entities didn't have a plan at all, while 4 entities hadn't finalized their COOP at the time of our fieldwork. 4 plans we reviewed included blanks or departed staff.

- Review and Test COOP: Of the 7 entities with plans that had existed long enough to test, only 3 had tested their plans (fully or partially).

- Business Impact Analysis: Some (7) entities didn't adequately identify and prioritize critical information systems. At least 1 entity did not adequately prioritize its information systems, using vague language such as "quickly" or "as soon as possible."

- Recovery Time & Recovery Point Objectives: Most entities didn't have RTOs or RPOs for their critical systems. 1 entity had created 1 of the few BIAs we've seen. Unfortunately, it used a flawed definition of RPO (a physical location rather than a point in time) in that document.

- COOP-related weaknesses directly affect how quickly and effectively an entity will be able to resume operations following a major disruption. Incomplete COOPs increase the risk that resumption of business functions will be delayed. Untested plans can lead to entities discovering mistakes or gaps in real time. This can increase the risk that critical functions can't resume as quickly. And when entities don't identify and prioritize IT systems, they may not restore them in a way that aligns with organizational goals. When recovery goals aren't thought out ahead of time, entities risk losing more data than they would like. This can directly affect the entities' customers and clients.

Based on our work and prior audit experience, we think management may not sufficiently prioritize Continuity of Operations planning.

- COOP is a form of strategic planning that typically involves activities over and beyond regular day-to-day activities. Without top management buy-in and

attention, strategic planning may be a luxury that staff don't make time for, given their regular day-to-day duties. It also can be difficult to involve all necessary stakeholders and agree on specific content. This is especially true for larger agencies, with many divisions or departments across several physical locations. Lastly, smaller entities may not think they need to create formalized plans because they believe they can adequately deal with situations as they arise.

Data Center Results

Entities should protect the physical space housing their critical information systems from unauthorized access or environmental hazards.

- Entities typically use data centers to house their critical information systems. Data centers must have controls to limit who has access. They also must prevent or limit damage from environmental hazards, such as water, fire, temperature, and humidity.

- We selected 4 data center controls from the state's security policy to evaluate. Additionally, we identified a state law that requires fingerprint background checks for individuals with unescorted access to the state's data center. Even though the state decommissioned the Landon State Office Building data center, we thought this was a sufficiently important control to apply to all data centers and therefore added it to our audit program. Those 5 controls, and our work to evaluate them, are described below. **Appendix C** has more information on these 5 controls.

    - Physical Access Restrictions: Entities should restrict physical access to data centers. We observed data centers to ensure entry doors and server rack doors were locked.

    - Authorized Access: Entities should keep a list of all authorized personnel with data center access. This list should be reviewed and updated once a year and as use privileges change. We reviewed access lists to evaluate the overall number of individuals with unescorted access. This included both entity and non-entity staff. We also confirmed whether the type of staff with access was reasonable.

    - Environmental Controls: Data centers should have controls that limit or prevent damage from water, fire, temperature or humidity. We observed data centers for the existence of required controls.

    - Background checks: Entities should do fingerprint-based background checks on people with unescorted data center access. We interviewed entities about their processes. We also judgmentally sampled a handful of individuals with unescorted access to confirm checks were completed.

- Revocation of access: Entities should revoke data center access as people's roles change. Entities should also recover property issued to departing staff. We interviewed entity staff about their processes to retrieve keys or badges from departing employees. As applicable, we confirmed whether entities recovered those items timely.

- In this area, 2 points are important to keep in mind:

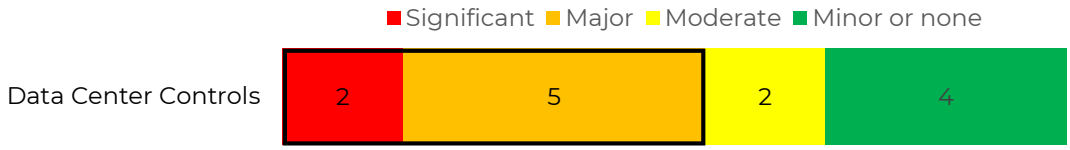
  - 2 agencies told us they didn't have servers to require a data center. Instead, they said their critical systems use cloud-based storage. Hosting data in the cloud has different control challenges than hosting data in a data center. In this audit, we only evaluated data center controls. As a result, we didn't audit the 2 agencies with cloud storage.

  - 3 entities used the state-contracted Unisys data center in Kansas City while 2 others contracted (or subcontracted) with other private data centers. We visited the state's contracted data center to observe its access and environmental controls. Because individuals are not allowed to access that data center without contractor escort, several controls became not applicable. Lastly, we didn't test whether contract staff with unescorted access received background checks. That's because it wasn't feasible to do in the time we had.

7 of 13 entities did not substantively comply with selected data center controls we audited.

- **Figure 5** summarizes our findings in this area. As the figure shows, 2 entities had significant control issues and 5 had major control issues in this area. This means over half of the 13 entities did not substantively comply (scoring 50% or less) in this area. As shown in the figure, 2 entities had moderate control issues, and the remaining 4 entities had minor or no control issues. Below is a summary of our findings.

Figure 5: Seven of thirteen entities did not substantively comply with selected data center controls (a).



(a) 2 of the 15 entities we audited did not have a data center for us to evaluate.

Source: Summary of LPA analysis of selected IT security controls at 15 entities

- Physical Access Restrictions: Many entities had appropriate physical access restrictions at their data center or the contracted data center. Still, we identified entities with issues. For example, 1 entity had created a makeshift data center room within their office. Staff permanently propped open the door to this room because the equipment produced too much heat. This meant all agency staff, and at least 1 non-agency staff who cleaned the office space, had access to the computer equipment located in that room. Another entity housed its servers in an unlocked server rack in the main office next to its copier.

  Lastly, 2 entities who contracted for data center services didn't know about their compliance in this area until our audit. Our cursory review of an independent audit report from the subcontractor indicated physical access controls appeared to be in place. However, because we didn't observe those controls firsthand, and because the auditee and contractor had not done their due diligence, we called it out as problematic.

- Authorized Access: At 3 entities, we noted the number of people with unescorted data center access was unreasonably high. At 1 of those entities, officials were aware of the issue but didn't have mitigating controls to address it. In these cases, the type of individuals with access also appeared to be unreasonable.

- Environmental Controls: Of the 8 entities who managed their own data center, 7 data centers we observed lacked one or more environmental controls. Environmental controls prevent and mitigate damage from water, fire, temperature, and humidity.

- Background checks: Only 2 of 8 entities that allowed staff unescorted data center access required fingerprint-based background checks. A third entity required this level of check, but only for certain staff. Lastly,

our judgmental sample review of staff's fingerprint and non-fingerprint background checks revealed most of these entities didn't have records of all checks. This occurred for several reasons. Sometimes the paperwork wasn't maintained. Other times staff was "grandfathered in" and the entity didn't conduct a check.

  - Revocation of access: Only 2 of the 8 entities that allowed staff unescorted access also had staff with that access leave within a certain timeframe prior to our audit. For those 2 entities, we learned their processes to collect data center keys or badges were not documented. This meant these entities had no assurance whether access revocation happened timely or at all.

- Poor data center controls increase the risk that assets or data could be lost, damaged, or stolen. Entities that use data centers with poor environmental controls risk data loss from fire or water damage. For example, in 2018, Kansas State University experienced a fire in the Hale Library. The university's data center was located in the library's basement. The data center experienced damage from water and fire and also experienced a power outage. Data center control weaknesses can severely disrupt the entity's ability to provide services.

Reasons for noncompliance in this area included unfamiliarity with ITEC requirements and inadequate monitoring by top management.

- Several smaller entities were not familiar with the security control requirements. Several entities did not find it necessary to document or implement certain controls. At least 2 entities asserted they lacked financial resources for certain data center controls. Lastly, management at several entities did not sufficiently monitor whether contractors had the necessary controls in place. Ultimately, top management is responsible to ensure the entity's sensitive data is secure.

Conclusion

Nearly 10 years ago, we recommended the legislature create a more enterprise-level approach to IT security to help improve agencies' security posture. The legislature responded by creating the Cybersecurity Act in 2018. This included the new Kansas Information Security Office and a state Chief Information Security Officer position. The 2023 legislature further strengthened the Cybersecurity Act. ITEC also approved several updates to its policies, including the statewide IT security policy, in recent years.

Despite these improvements, we continue to identify weaknesses with state agencies' basic security controls. In this audit, we selected several smaller state agencies as well as larger ones. While smaller agencies may not hold the most

sensitive confidential data, the audit shows they have similar compliance problems as their larger counterparts.

The Cybersecurity Act explicitly made agency heads responsible for their agencies' security compliance. However, many agencies we reviewed were not compliant with basic security controls. The Act does not include consequences for noncompliance. Additionally, the state currently doesn't have a centralized solution to ensure agency heads are made aware of those responsibilities in a consistent manner. KISO may be the most logical entity to do this for most agencies, but they may not be in the best position to educate elected or non-executive state agencies.

Other factors contributed to the audit's findings. Entities who rely on KISO staff or contract with other entities for IT services did not sufficiently ensure those services were comprehensive or adequate. Additionally, roles and responsibilities were not always clear, in part because written agreements were vague or non-existent. At times, entities and KISO staff we talked to appeared to point to the other party for being responsible. Lastly, the shortage of IT security experts appears to be worsening. It can be challenging to compete with the private sector to find knowledgeable IT staff. However, improving security controls starts with making security a priority at the top and following through on that commitment.

School districts may be further behind in building strong security processes. That's because they are not required to adopt basic security standards or continuity of operations processes. Despite the actions KSDE has taken, it's unlikely that smaller districts with fewer resources will adopt security and resiliency standards. In turn, larger districts are better positioned to adopt and implement security controls, when given the choice.

Recommendations

1. All 15 entities we audited should review the individual control findings they received during the audit. They should determine what actions they can take to remedy the findings and how to prioritize them, in light of their overall risk appetite. As needed, entities could reach out to KISO, KSDE, or K12 SIX for assistance or advice.
    - Pittsburg State University Response: We have reviewed the findings and will determine the necessary actions needed to mitigate the issues. We will put a plan in place to prioritize and implement the needed controls.
    - Department for Children and Families Response: The agency will prioritize corrective efforts around the severity of the control issues brought forward in the LPA audit. Systems operations and configurations will be the first area of focus. While our agency is awaiting an approved inventory management system by another agency, we can address the deficiencies noted in the LPA review with current inventory management processes. Secondly, the agency is in process of adding operational security staff to the IT team. There has not

been adequate operational security staffing in these roles since a centralization effort was imposed upon our agency several years ago. As part of that mandated centralization of security effort, agency security staff were moved from our agency to another agency causing an operational gap in service. After we add back the security staff in line with this audit finding and fill the operational gap, their initial focus will be to address third party patching by making further progress on the existing ECM project. This team will also work with other agencies to identify best practices on supplying vulnerability scans to users connected behind a VPN. Finally, there is an active project to replace existing Server 2008 and Server 2012 servers in the environment. This will help our overall patching posture by removing products that are no longer receiving security patches.
COOP issues can be addressed by implementing a centralized review process. Based on the findings, some plans were more complete than others. A centralized review will help create a cross reference of the existing plans, identify the gaps, and manage the remediation processes that are necessary. Additionally, the agency is already identifying resources to prepare and document a proper tabletop exercise that can address business operations and IT operations to alleviate shortcomings with the tabletop exercise.

- Adjutant General's Department Response: The Adjutant General's Department recognizes the importance of identifying vulnerabilities and gaps to mitigating against risks. The Kansas Division of Legislative Post Audit's report will assist our agency in securing additional services and technical support to ensure compliance with ITEC requirements.
- Board of Emergency Medical Services Response: We appreciate the review and audit as we have found it extremely difficult to maintain awareness of changes, let alone a working knowledge of changes, made to the ITEC policies. We would absolutely recommend, moving forward, that best practices to help agencies achieve the goals of the ITEC policies be developed and those goals clearly communicated prior to implementation of the policy. We feel having a knowledge of the intended goal(s) would assist agencies in identifying and implementing workable solutions to achieve compliance with state policies. As an example: Patch management process should not be a patchwork/haphazard approach developed by each individual state agency when there is clearly a demonstrated, enterprise level need for a scalable solution capable of ensuring patches to computer software are being maintained. This is evidenced from the fact our research into software designed to track patch management and implementation across an agency begins at 500 seats/licenses/devices. As for the findings specific to our agency, we intend to have all addressed within the next 6 months. Many of them were addressed and remedied within a month of the on-site audit being done.
- Insurance Department Response: The agency was pleased to see only minor issues identified for our agency and some of the recommendations have already been resolved. The agency contracts with KHP for building security

and the agency defers to them on the individuals that need to have access in the event of an emergency. The agency will evaluate the remaining findings.

- Board of Pharmacy Response: The Board of Pharmacy appreciates the opportunity for assessment and improvement of its IT security controls. The Board has already taken implementation steps based on LPA's recommendations. The Board also plans to meet with OITS to work toward better/greater insight into the services provided to our agency.
- Kansas Guardianship Program Response: The agency has reviewed the LPA report. Some control findings have already been implemented and plans are ongoing for the other recommendations. The agency is prioritizing control findings remediation.
- Kansas Department of Health and Environment Response: The Kansas Department of Health and Environment agrees with the Legislative Post Audit findings identified during the audit and we have committed to addressing them before the end of 2024. We have prioritized the findings and will work diligently to resolve them within the next 6-12 months. Findings 10.12, 10.13, and 13.3 have been resolved prior to the release of the findings. Findings 6.2.2, 6.3, 6.4, 10.3, 10.4, and 13.5 will be rectified by the end of 2024 or sooner.
- Emporia State University Response: We have reviewed the findings and we do plan to take action to correct those findings to the best of our ability.
- State Fire Marshal Response: Our agency has reviewed the 2023 IT Security Audit Summary, and we are in the process of taking steps to remediate the reported findings.
- Department of Corrections Response: We appreciate the opportunity provided by LPA to address areas of improvement the agency can make in IT security. We will be addressing the findings of the audit in the coming months. Some findings have already been corrected. The agency takes IT security very seriously and will continue to strive to be better.
- Kansas Sentencing Commission Response: The agency recognizes the audit findings and will determine a best path forward toward addressing the identified exceptions. We have an excellent working relationship with KISO and will continue to consult with them to further prioritize these actions.
- Newton School District (USD 373) Response: We are reviewing the findings and creating a plan to address the recommendations.
- Piper School District (USD 203) Response: We have looked at the findings of the KLDPA audit and will be working on updating policies and procedures to encompass the recommendations. We acknowledge the importance of maintaining secure records and data and will continue to grow and improve our policies and actions toward that end.
- DeSoto School District (USD 232) Response: USD 232 appreciates the opportunity to participate in this audit and reporting process. We will use these findings to address areas of improvement and also to reflect on areas of strength.

2. All 15 entities should report their progress to us by July 1, 2024 as part of our 6-month follow up process. As part of the progress report, entities should describe what actions they have taken to address their individual findings, and take a clear position whether they believe individual findings are fixed, in progress, not started, or refused.
    - Pittsburg State University Response: We plan to provide an update to LPA by July 1, 2024 on our progress of addressing the findings in the LPA Audit Report.
    - Department for Children and Families Response: The agency will track efforts that are in progress and be prepared to report progress in the format and timeframe requested.
    - Adjutant General's Department Response: The Adjutant General's Department will report process to the Kansas Division of Legislative Post Audit by July 1, 2024.
    - Board of Emergency Medical Services Response: We see no findings specific to our agency that are impossible to overcome. Knowing the target we are aiming at, we believe we should have all findings addressed and remedied by July 1, 2024. We do not understand the purpose behind requiring a background check for someone to physically have access to a server when that same individual has been granted digital access to the entire file contents of the server, but as that is a best practice, we will ensure the best practice suggestion is implemented. Within systems operations and configurations, we are still researching some software solutions to achieve the intended goals of the policy, but have 'low-teched' a solution until those software solutions can be acquired and implemented. Within COOP, our COOP plan was approved as required by the Governor's Executive Order and scored well above the threshold when graded. This document will continue to be maintained and post-audit, will be physically printed after every update and subsequent approval. Within data center security, we feel nearly all individual findings are fixed. The only individual finding not fixed, but in progress, is to adhere to the best practice previously mentioned.
    - Insurance Department Response: The agency plans to provide a progress report on outstanding items by July 1, 2024.
    - Board of Pharmacy Response: The Board has already taken implementation steps based on LPA's recommendations and anticipates all identified action items will be complete by July 1, 2024. The Board will submit a progress report by the deadline provided.
    - Kansas Guardianship Program Response: The agency will continue addressing the control issues found and report again by the July 1, 2024 deadline. At that time, the agency will have a list of specific controls which have been implemented, planned, or refused.
    - Kansas Department of Health and Environment Response: The Kansas Department of Health and Environment will provide a report by July 1, 2024

that outlines our efforts to address all audit findings in the required format by the Legislative Post Audit.

- Emporia State University Response: We will report back to LPA with our follow-up process by July 1st, 2024.
- State Fire Marshal Response: Our agency will provide LPA with a progress update by July 1, 2024.
- Department of Corrections Response: The agency will take the findings of the audit and plan to have corrections made by the 6 month follow up period.
- Kansas Sentencing Commission Response: The agency recognizes the follow-up process of the Legislative Post Audit and will work with the LPA to report progress on the recommendations by July 1, 2024.
- Newton School District (USD 373) Response: We plan to report progress on the recommendations by July 1, 2024.
- Piper School District (USD 203) Response: We will review the recommendations provided by the KLDPA audit and report any mitigation steps or improvements we implement prior to July 1, 2024.
- DeSoto School District (USD 232) Response: Our organization will take the next few months to evaluate the findings and make several key improvements to our existing systems. We will report on the actions taken in regards to the individual findings.

3. KISO (or other 3rd parties providing services to audited entities) should formalize and specify roles and responsibilities involving security control work. The document should describe what services the contractor provides and what responsibilities remain with the entity. The document should clarify what information entities will receive to monitor the security controls they are ultimately responsible for.
    - Kansas Information Security Office Response: The KISO is working to meet LPA's recommendation. As the KISO continues to mature and standardize its service delivery and as cybersecurity efforts mature in the state, we are working to clearly define cybersecurity operations versus IT operations. KISO is working on a Services Memorandum of Understanding (MOU) document which outlines the services that are available and how to request the services as well as get support for those services. It will also outline roles and responsibilities for those services.

      A KSLOC Baseline of Service for those agencies on the within KS.Loc domain will be developed and will be walked through with agencies to inventory services being consumed as well as discuss new services. An Adhoc Agency Service Inventory will also be developed and will be reviewed with each agency that is not on KSLOC and will reflect whether KISO is providing the service or if the agencies is filling that service themselves. Both service inventories will display who is responsible for the core roles related to the service.

The MOU and Service Inventory will be created for each agency and signatures of acknowledgement will be collected along with the inventory for agency. MOUs will be reviewed annually or as needed if the agency services consumption changes. the agency response from response template here.

4. KISO should ensure that vulnerability scans conducted on behalf of state agencies encompass the expected number of networked computer assets (including computers used remotely and servers housed in contracted data centers), that such assets are scanned at least monthly, and that scans are configured to be credentialed.
   - Kansas Information Security Office Response: The KISO is remediating this finding. Based on audit findings and discovered limitations of vulnerability scanning over the network, the KISO is switching to an agent-based scanning mechanism. Switching to agent-based scanning will allow the scanning of remote assets and ensure that network changes do not impact the effectiveness of scanning. Also, switching to agent-based scanners ensures that all scans are credentialed and eliminates credential failures which causes scan failures. Assets will be covered at all times. Work is being done to build a comprehensive vulnerability management program that each agency can adopt.

5. The legislature should consider amending the Cybersecurity Act to require KISO to educate all new and current agency leaders annually about their responsibilities regarding information security. This may be part of the statutorily required leadership training program or take other forms. Ideally, it should include a deliverable that agency leaders receive to remind them of key information.

6. The legislature should consider the Cybersecurity Act, Safe and Secure School provisions, or other relevant statutes to require the State Board of Education to adopt statewide standards for school districts to implement basic IT security and COOP standards based on current industry best practices.

7. The legislature should consider revising the K.S.A. 75-3707e to require fingerprint-based background checks for staff with unescorted access to any state-operated or contracted data center. Statutory revisions also should consider requiring contractors with unescorted data center access housing state-owned data to receive fingerprint-based background checks.

Agency Responses

On December 13 and 14, 2023 we provided the draft audit report to the 15 audited entities listed in Appendix B as well as the Kansas Information Security Office and the Kansas State Department of Education. Entity officials generally agreed with our findings and conclusions. We reviewed the information officials provided during the review process and made minor changes to our findings and recommendations. Entities had the opportunity to provide general responses to the audit, but none chose to do so.

Appendix A – Cited References

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

- *Information Systems: Reviewing Specific IT Security Controls Across State Agencies and School Districts (July 2023). Kansas Legislative Division of Post Audit.*

- Information Technology Policy 5300 Rev 2 – Continuity of Operations Planning (September 2021). *Kansas Information Technology Executive Council.*

- Information Technology Policy 5310 Rev 2 – Continuity of Operations Planning Implementation (September 2021). *Kansas Information Technology Executive Council.*

- Information Technology Security Standards 7230A (July 2019). *Kansas Information Technology Executive Council.*

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

- State Agency Information Systems: Reviewing Security Controls in Selected State agencies (CY 2014-2016) (December 2016). *Kansas Legislative Division of Post Audit.*

- 3 Year Summary of Security Controls in Selected State Agencies (2017-2019) (February 2020). *Kansas Legislative Division of Post Audit.*

- 3 Year Summary of Security Controls in Selected State Agencies (2020-2022) (December 2022). *Kansas Legislative Division of Post Audit.*

Appendix B – List of Audited Entities

This appendix lists the 15 entities we selected for audit. The list includes each entity's expenditures and FTE.

Agency Name	2022 Expenditures	2022 FTE
Department of Health and Environment	$ 3,831,449,764	1,719.1
Department for Children and Families	$ 1,081,632,973	2,657.9
Adjutant General	$ 297,567,693	293.6
Department of Corrections	$ 283,806,083	517.0
Pittsburg State University	$ 134,457,493	762.0
DeSoto School District (USD 232)	$ 104,823,055	876.5
Emporia State University	$ 97,662,969	747.2
Newton School District (USD373)	$ 56,993,916	570.5
Piper-Kansas City School District (USD 203)	$ 35,803,132	266.5
Kansas Insurance Department	$ 35,660,156	135.5
Kansas Sentencing Commission	$ 7,158,826	14.0
State Fire Marshal	$ 5,939,224	71.3
Board of Pharmacy	$ 3,829,847	19.0
Board of Emergency Medical Services	$ 2,250,227	14.0
Kansas Guardianship Program	$ 1,375,960	10.0

Source: FY 2024 Governor's Budget Report Vol. 2, and Kansas Dept. of Education Data Warehouse, school year 2021-22 (unaudited).

Appendix C – List of Selected Security Controls by Area

This appendix includes the selected controls across the 3 security areas we selected for audit. The list includes the source of each control.

	Area 1 – Systems Operations & Configuration Controls	Source
1	Entities must maintain an asset inventory of Information Systems' components, update the inventory as changes occur, and review the inventory at least annually.	ITEC 7230A 10.3
2	The asset inventory must identify and document the relationships between each of the Information System Components and the ownership of each component.	ITEC 7230A 10.4
3	Entities must perform vulnerability scans against all network connected Information Systems at least monthly.	ITEC 7230A 13.3
4	Entities must have a documented patch management process.	ITEC 7230A 13.5
5	Entities must employ malicious code protection mechanisms on systems that contain Restricted Use Information. Entities must configure AV to conduct weekly scans of files on information systems.	ITEC 7230A 10.12 & 10.13

Source: LPA review of ITEC 7230A

	Area 2 – Continuity of Operations Planning (COOP) Controls	Source
1	Entities must implement, maintain and test disaster recovery, and continuity of operations plans. All entities are responsible and accountable for their own plans. Portions of the plan, which are name-oriented, shall be reviewed semiannually.	ITEC 5300 6.4 ITEC 5310 6.3
2	The COOP provides procedures and guidance to sustain an organization's mission essential-functions for an undetermined amount of time. COOP must include: disaster or disruption detection and response, continuity of essential functions/business, delegations of authority, orders of succession, continuity of facilities and equipment, continuity of communications, etc.	ITEC 5310 6.2.4
3	The entity's continuity of operations plans shall be reviewed and updated annually, and a table-top exercise conducted every two years. Documentation of the exercises should be kept for review based on current state policy.	ITEC 5310 6.3
4	Entities must conduct a Business Impact Analysis (BIA) to identify and prioritize information systems and components critical to supporting the organization's mission/business processes and people.	ITEC 5310 6.2
5	BIAs must identify information system recovery time objectives and recovery point objectives.	ITEC 5310 6.2.2

Source: LPA review of ITEC 5300 and ITEC 5310

	Area 3 – Data Center Controls	Source
1	Entities must restrict physical access to data centers that process, store, or transmit Restricted-Use Information to authorized personnel only.	ITEC 7230A 16.1
2	Entities must maintain a list of all authorized personnel with physical access to data centers that process, store, or transmit Restricted-Use Information. This list must be reviewed and updated annually. This list must be updated as user access privileges change.	ITEC 7230A 16.2
3	Data centers must implement physical environmental controls that mitigate or prevent damage from water, fire, temperature, and humidity for Information Systems that process, store, or transmit Restricted-Use Information.	ITEC 7230A 16.4
4	Entities must conduct fingerprint-based background checks for staff or contractors with unescorted data center access.	Best practice K.S.A. 75-3707e
5	Entities must revoke system access or eliminate unnecessary permissions for user accounts as users are transferred, terminated, or their roles change. Entities must recover all property that has been assigned to terminated personnel.	ITEC 7230A 17.8 and 17.9 K.S.A. 75-7240

Source: LPA review of ITEC 7230A, Kansas Statutes, and Criminal Justice Information Security Policies