KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

Availability, Cost, and Quality of Centralized IT Security Services

July 2022

Report Number: R-22-012

Introduction

LPA staff suggested this audit to satisfy committee rule 1-5(c). The Legislative Post Audit Committee authorized it at its May 5, 2021 meeting.

Objectives, Scope, & Methodology

Our audit objective was to answer the following questions:

1. Are the cybersecurity services offered through KISO sufficiently comprehensive to meet statutory requirements and state agencies' needs?
2. Does KISO provide cost-effective security services to state agencies?

To answer these questions, we reviewed relevant state and federal requirements. We also talked to officials and reviewed information from the Kansas Information Security Office (KISO) and the Office of Information Technology Services (OITS). This included expenditure and revenue information they reported for fiscal years 2020-2022. We also surveyed 57 top information technology officials from executive branch agencies. Finally, we talked to officials from and reviewed LPA cybersecurity audit reports for a selection of 7 executive branch agencies.

Our method didn't include reviewing whether KISO's cybersecurity services aligned with Information Technology Executive Council (ITEC) requirements. LPA cybersecurity audits review ITEC's cybersecurity control requirements, but our audit scope didn't include this. We also didn't review whether our selection of 7 agencies had current cybersecurity control issues. Finally, the opinions expressed by survey respondents and officials from our selection of 7 agencies aren't projectable to all state agencies.

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. But we encountered data limitations that prevented us from answering one of the audit questions.

Audit standards require us to report limitations on the reliability or validity of our evidence. KISO doesn't track its costs separately for each service and officials recently changed the way they calculate agency fees. This prevented us from assessing the accuracy of service costs, the cost-effectiveness of KISO's services, and KISO's compliance with applicable federal requirements (i.e., 2 CFR Part 200).

Audit standards require us to report confidential or sensitive information we have omitted when circumstances call for this. In this audit, we omitted agencies' cybersecurity service use and LPA cybersecurity audit results. State law (K.S.A. 45-221(a)(12) & (45) and K.S.A. 46-1135) allows us to keep these things confidential to safeguard agencies' cybersecurity.

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 reviewed KISO and OITS's controls for ensuring their financial data are accurate and agencies' controls for monitoring whether KISO provides services as contracted. We found KISO's service contracts contained errors and were ineffective for providing monitoring controls, especially regarding KISO's service fees.

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

KISO offers cybersecurity services that appear to satisfy state law, but few agencies use KISO's most advanced services and some don't seem to know what their agencies need or receive.

Background

The 2018 Kansas Cybersecurity Act created the Kansas Information Security Office (KISO) to reduce state agencies' cybersecurity risk.

- The Legislature enacted the Kansas Cybersecurity Act (K.S.A. 75-7236, et seq.) to help prevent cyberattacks against state agencies' systems. The Act established KISO within the Office of Information Technology Services (OITS).

- OITS provides information technology services to state agencies. These include statewide data center and KANWIN network services. State law (K.S.A. 75-4705 and K.S.A. 75-4709) generally requires state agencies to use OITS's services.

- KISO is responsible for coordinating cybersecurity services for state agencies. **Figure 1** shows the 15 KISO responsibilities outlined in state law. As the figure shows, state law does not require KISO to directly provide many services. Instead, it requires KISO to facilitate agencies' cybersecurity. Further, agencies are not required to use most of KISO's services.

- KISO provides cybersecurity for OITS's data center and KANWIN network services, so most agencies benefit from at least some of KISO's services. But the Act specifies agencies remain responsible for ensuring their own cybersecurity. Because of this, KISO offers agencies a range of cybersecurity services, but it can't require agencies to use them.

- Any state agency can use the cybersecurity services KISO offers. But some may choose to get services from their own staff or through third-party vendors rather than KISO. That's because agencies have different ideas about their needs and how well KISO may meet them. For example, some agencies must follow specialized state and federal requirements related to things like tax or criminal justice data that they think the agency or a different service provider can better meet than KISO.

Figure 1. KISO offers services that appear to align with the Kansas Cybersecurity Act requirements we could review.

Kansas Cybersecurity Act requirement	**Does KISO offer services to meet the requirement?**	**Related KISO service category**
Provide agencies a cybersecurity training program at no cost	✓	Basic
Help agencies develop, implement, and monitor cybersecurity programs	✓	Basic, Intermediate, Advanced
Facilitate measurement of the efficiency and effectiveness of agencies' cybersecurity programs	✓	
Facilitate agency cybersecurity governance	✓	Advanced
Provide agencies cybersecurity guidance for IT projects	✓	
Help agencies develop compliant cybersecurity programs	✓	
Help agencies develop business continuity plans	✓	
Help agencies set their cybersecurity roles and responsibilities	✓	
Administer the Kansas Cybersecurity Act	✓	Activities beyond security services
Coordinate external cybersecurity resources, including helping agencies contract with vendors	✓	
Work with external agencies as needed to strengthen agency cybersecurity	✓	
Provide cybersecurity threat briefings to the Information Technology Executive Council	✓	
Provide annual status reports to ITEC and the Joint Committee on Information Technology	✓	
Carry out other duties as necessary	✓	
Create and manage cybersecurity controls meeting state and federal requirements	Could not be determined	

Source: Interviews with KISO officials and LPA analysis of KISO's service descriptions.

KISO offers agencies 3 cybersecurity service levels.

- KISO organized the services it offers agencies into 3 levels: enterprise security services, technical security services, and information security officer services. For simplicity, we refer to these 3 levels of service as basic, intermediate, and advanced services in this report.

- KISO offers 18 basic services to agencies.

    - Agencies that use OITS's services automatically benefit from 8 basic KISO services. The services are focused on securing OITS's services, so agencies may not know they're getting them. For example, agencies using communication services such as KANWIN or ks.gov email also benefit from related services such as a network firewall or suspicious email filtering.

    - Agencies that use KANWIN can choose to opt into the other 10 basic services KISO offers. They don't have to sign contracts or pay more for them. These services aren't focused on securing OITS's services like the automatic basic services. Instead, they're focused on the cybersecurity needs of the agencies getting them, such as scanning agency systems for vulnerabilities or providing security awareness training.

- KISO offers 5 intermediate services that agencies can opt to receive. These are generally higher-level versions of the basic services. They're tailored to the specific agency and involve giving KISO control, such as setting up and managing a separate firewall specifically for the agency's system. Agencies that want intermediate services generally must sign a contract with KISO and pay for them. KISO officials said agencies can get impromptu services without a contract if they need them, though.

- Finally, KISO can provide agencies advanced services. These involve providing an information security officer to the agency to provide cybersecurity leadership. These staff are responsible for things like developing agency policies that comply with state and federal requirements. Agencies that want advanced services generally must sign a contract with KISO and pay more for them. But KISO officials said agencies can get impromptu services without a contract if they need them.

KISO Services and the Cybersecurity Act

KISO offers services that appear to align with the Cybersecurity Act requirements we could review.

- We compared the services KISO offers to its duties under state law. We reviewed KISO's service catalog, talked to KISO officials, and reviewed available supporting documentation.

- **Figure 1** shows whether KISO appears to meet its duties. As the figure shows, KISO meets all 14 duties we could review.

- For instance, KISO must help agencies develop, implement, and monitor cybersecurity risk management programs. All its service levels should help do this. KISO must also facilitate agencies' cybersecurity governance. It offers this through its advanced services and optional trainings for agency officials.

- We couldn't conclude whether KISO created a cybersecurity framework that meets state and federal requirements like Information Technology Executive Council (ITEC) standards. KISO officials told us all their services meet the required standards. But confirming this would require us to assess agencies' systems and we didn't do that because of time and resource constraints.

KISO's services may not have as many effects as the Legislature intended because few agencies use intermediate or advanced services.

- The Legislature implemented the Cybersecurity Act to reduce state agencies' cybersecurity risk and reduce the chances of cyberattacks. KISO officials said using all 3 service levels would provide the strongest cybersecurity because it would address all aspects of the Act.

- However, as **Figure 1** shows, many of the services KISO offers are optional intermediate and advanced services. For instance, of the 15 Cybersecurity Act requirements, KISO meets 5 through advanced services.

- However, few executive branch agencies use intermediate or advanced services. The Act excludes certain agencies, such as elected officials' agencies and the Kansas Public Employees Retirement System. But we reviewed them because many still choose to use KISO's services. As of February 2022:

  - 65 of 74 agencies received at least automatic basic services by using KANWIN.

  - 15 of 74 agencies had contracts with KISO for intermediate services, including things like continuously monitoring for and preventing system attacks.

  - 10 of 74 agencies had contracts with KISO for advanced services, including things like developing the agency's disaster recovery and business continuity plans.

- We don't know how many agencies may have gotten impromptu intermediate or advanced services without contracts.

- Because most agencies don't use KISO's intermediate and advanced services, KISO may not be as effective as it could be. Agencies may get adequate cybersecurity through their own staff or third-party vendors. But the

Legislature intended the Cybersecurity Act to consolidate the state's cybersecurity efforts, which doesn't appear to be happening so far.

KISO Services and Agency Needs

We surveyed 57 executive branch agency officials and reviewed 7 agencies in detail to understand officials' opinions on whether KISO's services meet agencies' cybersecurity needs.

- Our survey included all executive branch agencies using the KANWIN network. We excluded agencies that don't at least use KANWIN because they don't receive KISO's basic services even though some of those agencies may receive KISO's intermediate or advanced services. We surveyed agencies' top IT officials, such as chief information officers or IT directors. Some agencies share top IT officials, so these 57 officials led more than 57 agencies. 8 were OITS employees who work in agencies as part of OITS's efforts to consolidate cabinet agencies' IT leadership structure.

- 50 of 57 officials (88%) responded. In addition to KISO's automatic basic services, 37 (74%) said their agencies received optional basic services. 14 (28%) said they received intermediate services. And 13 (26%) said they received advanced services. Some may have gotten impromptu services without contracts.

- We also reviewed 7 executive branch agencies in detail. We included agencies that used many KISO services and some that only benefited from a few basic services. We talked to these agencies' top IT officials about their experiences with KISO's services.

- We also reviewed these 7 agencies' confidential LPA cybersecurity audit results to ensure our selection varied in how they performed. We included agencies with many cybersecurity control issues and agencies with few issues.

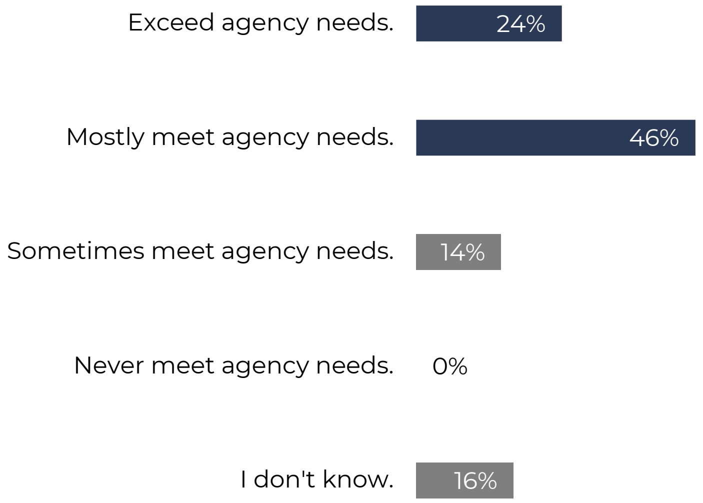
- Our selection included the Board of Healing Arts, the Department of Agriculture, the Department of Revenue, the Kansas Public Employees Retirement System, the Racing and Gaming Commission, the Secretary of State's Office, and the State Treasurer's Office.

Agency officials expressed mostly positive opinions about KISO's services.

- **Figure 2** shows survey respondents' opinions about whether KISO's services met agency needs. As the figure shows, most respondents expressed positive opinions. For instance, 23 respondents (46%) said KISO's services mostly met agency needs, and 12 (24%) said KISO's services exceeded agency needs.

Figure 2. Most survey respondents thought KISO's services met agencies' needs overall.

Question: Overall, how would your agency rate KISO's ability to meet your agency's needs with their IT security services?



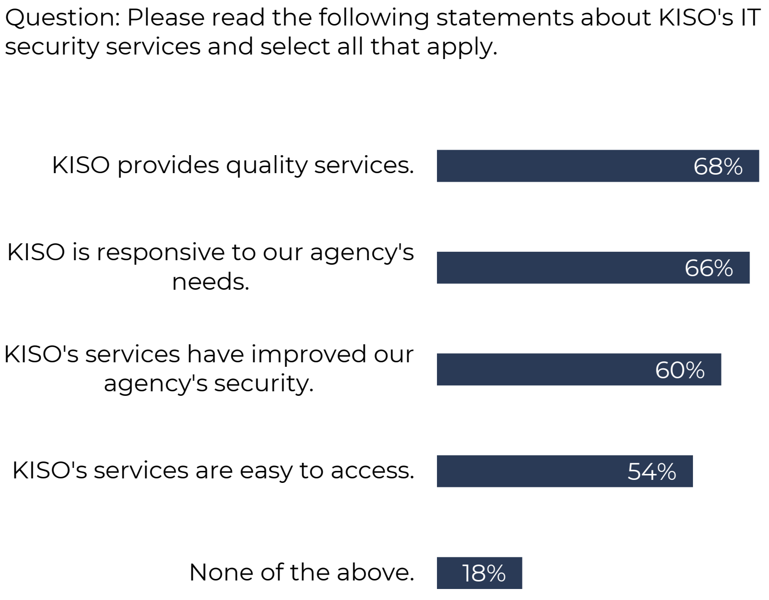
Source: LPA survey of executive branch agencies' top IT officials.

Kansas Legislative Division of Post Audit

- When asked about specific service levels, respondents were most positive about KISO’s intermediate and advanced services. For example, 12 agencies receiving advanced services (92%) said they mostly met or exceeded their agencies’ needs. Conversely, 34 agencies that received basic services (68%) said automatic basic services mostly met or exceeded their agencies’ needs.

- **Figure 3** shows whether respondents agreed with several statements about KISO’s services. As the figure shows, most respondents had positive opinions about KISO. For example, 34 respondents (68%) said KISO provides quality services, and 30 (60%) said KISO’s services had improved their agencies’ cybersecurity. But 9 (18%) didn’t think any statements applied.

Figure 3. Most survey respondents had positive opinions about KISO.



Source: LPA survey of executive branch agencies' top IT officials.

Kansas Legislative Division of Post Audit

- Further, officials from 5 of the 7 agencies we reviewed had positive overall opinions of KISO services or staff. They praised things like KISO's vulnerability scanning, security awareness training, and information security officers.

However, agency officials may not always know what their agencies' needs are or what services they receive from KISO.

- Some survey responses suggested respondents may not be knowledgeable about KISO's services. For example, 11 respondents (22%) didn't know whether their agencies had cybersecurity needs KISO wasn't meeting. This could be because they don't know what services they received, whether these services met their needs, or what their needs were to know if KISO was meeting them.

- Some respondents also said they didn't know what services their agencies got. 5 (10%) didn't know whether they received optional basic services and 16 (32%) didn't know whether they had signed contracts for intermediate services.

- State law (K.S.A. 75-7240(c)) requires executive branch agencies to designate an information security officer. KISO offers this through its advanced services. But 22 respondents (44%) said their agency didn't have an information security officer, and 8 (16%) didn't know whether they did. This suggests some respondents don't know this is something their agencies need.

- Further, the contracts between agencies and KISO for intermediate and advanced services had errors. This suggests neither agencies nor KISO were using them to determine whether agreed-upon services were provided.
  - KISO's intermediate and advanced service contracts outline how KISO's services should work. They specify things like KISO's role, the agency's role, what the agency should receive, and how much the agency will pay KISO.
  - 2 of the 7 agencies we reviewed had contracts for intermediate or advanced services. But neither said they used their contracts to ensure KISO provided the right services. Officials from 1 agency said they'd never looked at their contract and weren't sure what their responsibilities were.
  - We reviewed all 15 agencies' contracts for intermediate services and 12 agencies had contracts with errors. They showed incorrect billing practices or identified the wrong service provider or agencies getting services.
  - Neither KISO nor agency officials ensured the contracts accurately showed what agencies should expect. KISO officials said they haven't had the staff capacity to ensure these contracts stay updated. But accurate contracts are important for establishing common service expectations.
- Finally, officials from the 7 agencies we reviewed suggested they had limited knowledge about KISO's services. For example, 2 said they didn't know whether their agency or KISO was responsible for basic tasks like fixing issues identified by vulnerability scans. And 3 suggested they may have used more of KISO's services if KISO had made them better aware of them.

Some agency officials told us they didn't use more KISO services they knew about because they were concerned about losing control of their agencies' security.

- Officials from 6 of the 7 agencies we reviewed expressed concerns about using more of KISO's services.
- 5 officials told us they didn't use KISO's services because they wanted to keep control or the ability to make changes on their own. 3 of these 5 mentioned their firewalls specifically, including 2 who said KISO couldn't meet their specialized firewall needs.
- 2 officials said their agency didn't want to use KISO's services because doing so might create new vulnerabilities. 1 said allowing KISO to access their system to manage their services would open a new connection an attacker could exploit.

- KISO officials thought concerns about their services creating vulnerabilities reflected agencies' lack of knowledge or resistance to giving up control. KISO officials said agencies using basic services keep control, but agencies using intermediate and advanced services give up some control. KISO officials thought using contracts made these arrangements clear, but these contracts aren't kept up-to-date. KISO officials also acknowledged an inherent limitation of providing services for the entire state is that they may not always be able to meet certain specialized needs.

LPA cybersecurity audits of the 7 agencies we reviewed suggest using KISO services doesn't automatically correspond to better audit results.

- State law (K.S.A. 46-1135) gives our office authority to audit agencies' cybersecurity controls. LPA reviews whether agencies have controls meeting state requirements and best practices. We compared the LPA cybersecurity audit results for the 7 agencies we reviewed to what they might expect to get from KISO's services. We didn't re-evaluate their cybersecurity controls.

- Not all KISO's services directly relate to areas LPA cybersecurity audits review. We focused on 3 areas that appear to align closely with KISO's basic and intermediate services.

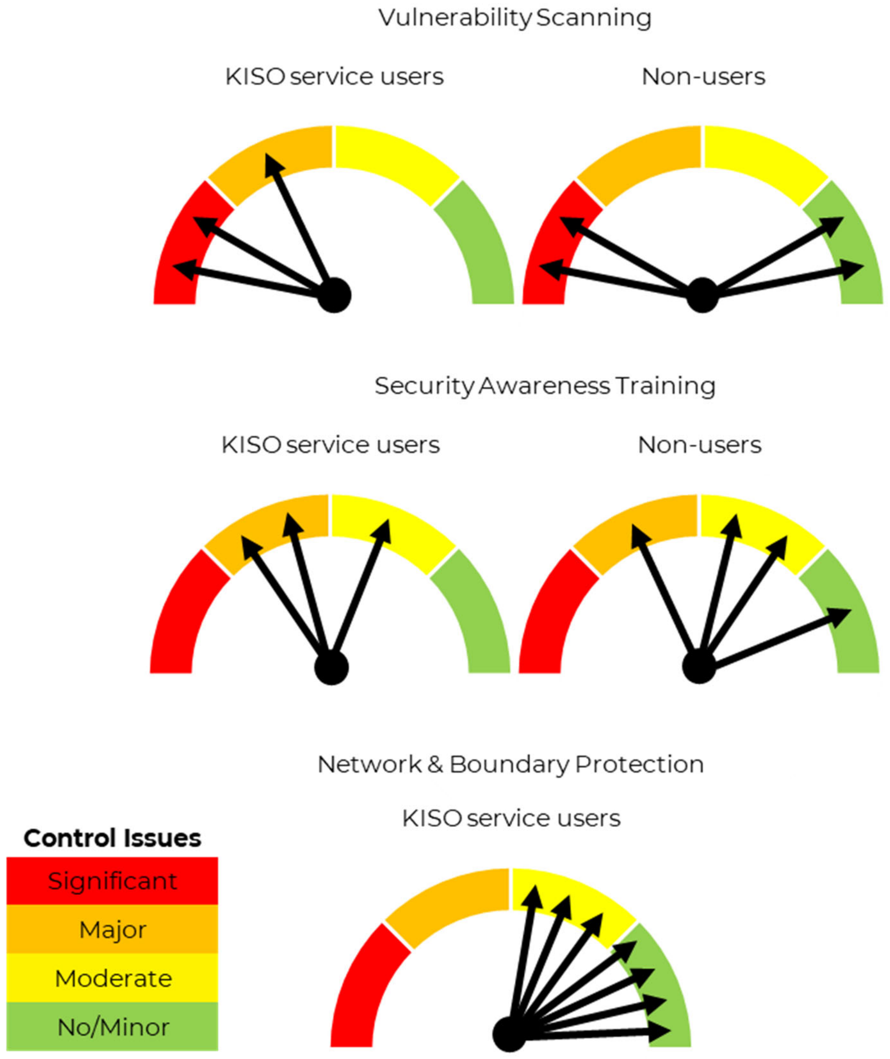
- Using KISO's services didn't appear to consistently improve agencies' performance in these 3 audit areas.

    - **Figure 4** shows LPA audit results for the 7 agencies we reviewed. Agencies can have either no/minor, moderate, major, or significant control issues. As the figure shows, agencies using KISO's services didn't consistently have better audit results than agencies who didn't use KISO's services.

    - For example, the figure shows 3 agencies used KISO's vulnerability scanning. LPA audits found 2 had significant and 1 had major control issues. By contrast, 4 agencies didn't use KISO's scanning. Although 2 had significant control issues, 1 had minor issues and 1 had none.

- Overall, agencies that were more actively engaged in their cybersecurity seemed to have the fewest issues. Agency officials indicated they performed best when they understood KISO's and their roles in ensuring KISO's services work.

Figure 4. For 3 cybersecurity areas, agencies using KISO's services didn't always have better audit outcomes than non-users.



Source: Analysis of LPA cybersecurity audits of 7 selected agencies.

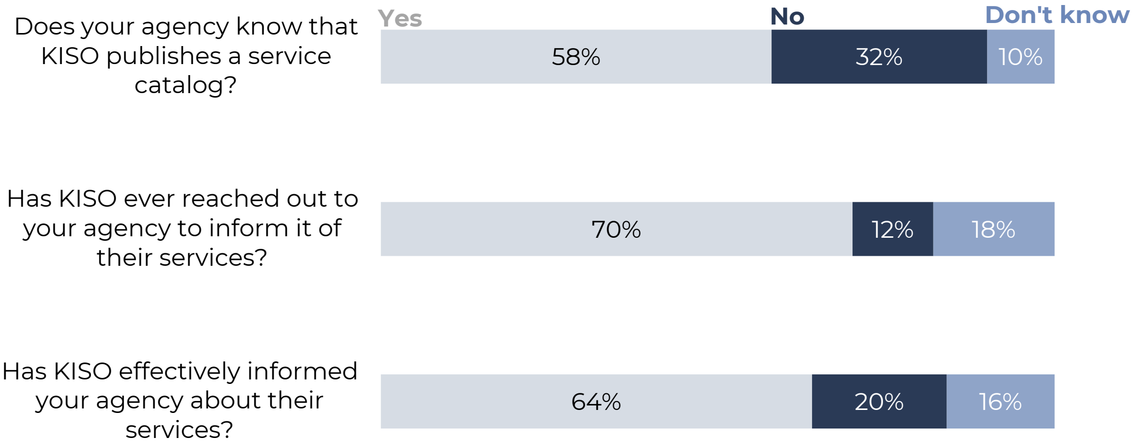
Kansas Legislative Division of Post Audit

Agencies may not be aware of the services KISO provides because KISO's communication with agencies isn't proactive enough.

- Proactive agency education and communication about KISO's services would likely help KISO meet agencies' needs. Specifically, it could help agency officials better understand cybersecurity, their agencies' risks, and how KISO's services might help.

- **Figure 5** shows survey responses related to whether officials knew about KISO's service offerings. As the figure shows, 21 respondents (42%) didn't know KISO published a service catalog showing the services they offered. 15 (30%) said KISO had not informed their agency of its services or they didn't know if it had. 18 (36%) said KISO had not effectively informed their agencies about its services or didn't know if it had.

Figure 5. Some survey respondents didn't know about KISO's services.



Source: LPA survey of executive branch agencies' top IT officials.

Kansas Legislative Division of Post Audit

- Respondents also described several ways they thought KISO could communicate more proactively. They told us it's difficult for non-experts to understand cybersecurity requirements. They suggested KISO do more to help interpret and apply these. They also suggested KISO more proactively promote their services so agencies are aware of and can budget for them, such as through communications staff. Finally, respondents said KISO should provide better training on things like how to use KISO's tools or know whether their agencies' systems are secure.

- KISO officials said they do many of these things when agencies reach out to them. For example, KISO officials said they help interpret requirements and can provide unpublished guidance when agencies ask. KISO officials also said they train agencies to use their services when they first sign up. But they address issues and provide further training when asked, such as in response to agency staff turnover. They said they're reluctant to recommend particular products or tools because they don't know the details of agencies' systems or their specific needs.

- KISO officials agreed they could communicate better. They said more proactive agency education and communication may help agencies understand their services. They said they're working toward more regular contact with agency officials through things like trainings, meetings, and regular information bulletins. Ultimately, KISO officials said they'd like to hire a public information officer but don't have a way to fund this position.

We can't say whether KISO's services are cost-effective because of data limitations.

KISO is funded through fees it collects from agencies.

- Since its creation, KISO has been funded through fees collected from state agencies. It must cover its costs with fees it charges agencies using its services. It doesn't receive a regular appropriation.

- Agencies pay a single fee for each of OITS's services and KISO's basic services. KISO is part of OITS, so OITS bills agencies on KISO's behalf. KISO officials told us they set basic fees using estimates of how much it'll cost to provide cybersecurity for OITS's 3 main services: the statewide KANWIN network, ks.gov email, and data center services. These fees cover costs for things like staff, software licenses, and major projects like moving agencies to a new data center. OITS adds its own overhead costs for things like human resources and finance staff.

- KISO's basic service fees cover both automatic and opt-in services. Agencies using KANWIN and benefiting from KISO's automatic basic services can also receive KISO's optional basic services without paying more. Agencies pay the same fees whether they get all KISO's basic services or not.

- KISO negotiates contracts with agencies that choose to use its intermediate and advanced services. KISO officials told us these services' fees come from KISO's estimates of how much it'll cost to provide them to each agency. For example, they said they charge larger agencies more because they expect they'll have greater service needs. Intermediate and advanced service fees generally cover the staff time required to provide these services.

We can't say whether KISO's services are cost-effective because of data limitations.

- We reviewed fiscal year 2020-2022 accounting and financial data and talked to KISO and OITS officials to determine KISO's costs and revenues. We also reviewed intermediate and advanced service contracts.

- We couldn't determine how much KISO spends on each basic and intermediate service it provides agencies for two main reasons.

  - KISO doesn't track how much it costs to provide each individual service because its staff, software, and tools support multiple services and service levels. For instance, KISO officials said they use the same staff and tools to provide both basic- and intermediate-level services.

  - KISO doesn't track how much it costs to provide cybersecurity for each of OITS's services. These also share resources, such as KISO staff who work with multiple OITS services. But KISO estimates this to decide how much to charge for each OITS service. KISO officials said they aren't sure how accurate these estimates are, partially because KISO started this in fiscal year 2021. For that year, for example, KISO estimated 60% of its basic service costs would relate to securing KANWIN, 30% would relate to data center services, and 10% would relate to ks.gov email.

- Prior to fiscal year 2021, KISO didn't track its costs like it does now. Instead, KISO simply added all its fees to OITS's KANWIN charges. In fiscal year 2019, KISO considered charging a separate cybersecurity fee for basic services that would take effect in later fiscal years. But KISO officials said they ultimately bundled their fees with OITS's 3 main services after agencies pushed back against this idea.

- We also couldn't determine whether KISO's services are effective in meeting agency needs as described earlier in this report. As such, we couldn't determine whether its services are cost-effective.

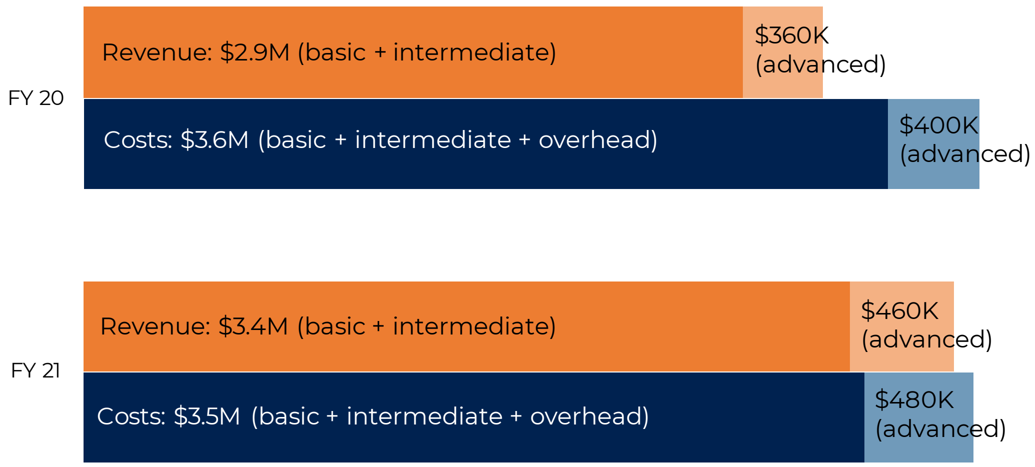
According to KISO's data, KISO's revenues were less than its costs in fiscal years 2020-2021.

- **Figure 6** shows KISO's overall costs and revenues in fiscal years 2020-2021 as reported by OITS and KISO officials. They said all are actuals except estimated fiscal year 2020 revenues. We couldn't independently verify these data because of the data limitations we encountered. As the figure shows, KISO reported spending about $4 million total providing services each year. It reported receiving about $3.3 million in agency service fees in fiscal year 2020 and about $3.9 million in fiscal year 2021.

  - Most of KISO's revenue came from basic services. KISO charges agencies by how much service they use. For instance, KISO officials said they charged agencies $5.58 per KANWIN connection per month for about 30,000 total connections in fiscal year 2021. This equaled about $2 million total of the $3.4 million KISO charged agencies for basic and intermediate services. OITS added this amount to the fees agencies paid for KANWIN.

  - KISO also charged 14 agencies about $100,000 total for intermediate services and 10 agencies about $460,000 total for advanced services in fiscal year 2021.

Figure 6. KISO officials told us KISO's revenues were less than its costs in fiscal years 2020 and 2021.



Source: Interviews with KISO and OITS officials and review of SMART accounting system data (unaudited).

Kansas Legislative Division of Post Audit

- The federal government requires OITS and KISO's costs and revenues to align. OITS and KISO officials must review this alignment annually. We didn't evaluate this because KISO's fees are only part of OITS's overall agency fees. We also don't know how KISO's costs and revenues have changed over time because KISO significantly changed how it calculates fees for basic services in fiscal year 2021. There aren't comparable historical data.

KISO officials also don't know if their services are cost-effective because of a few limitations.

- KISO does some things to compare its staff salaries to market costs as we describe more later. However, it doesn't do anything to compare its services and spending to benchmarks to know if they're cost-effective.

- Companies produce national estimates on things like cybersecurity spending per staff person, but KISO officials told us they can't compare their spending to those estimates as a benchmark for a couple of reasons.

  - They don't know how much agencies spend on cybersecurity overall. KISO knows how much agencies spend for KISO's services. But KISO doesn't know how much agencies spend on cybersecurity services they receive from their own agency staff or third-party vendors. As we found in our 2019 audit of OITS, no one tracks the state's total IT spending, including cybersecurity.

  - KISO also doesn't know how many agency staff use its services. For instance, OITS charges agencies for KANWIN by the number of network connections. Multiple staff could use 1 connection without KISO knowing.

- Finally, KISO officials said private companies' cybersecurity costs often aren't published because it's considered proprietary information. KISO can't compare its costs to what third-party vendors providing similar services might be spending or what agencies might pay them.

Most agency officials we interviewed couldn't speak to whether KISO's services are cost-effective.

- Officials from 5 of the 7 agencies we reviewed said they couldn't comment on the cost-effectiveness of KISO's services. 2 said another department handled the billing and the agency's IT leadership didn't know how much KISO's services cost. Agency officials can't determine cost-effectiveness if they aren't aware of both how much services cost and how well they meet agency needs. The other 3 said they couldn't comment because they didn't use enough of KISO's services.

- Officials from the other 2 agencies thought KISO's prices were reasonable. 1 said KISO charged fees similar to those of other service providers, but they also thought KISO could be more responsive to service requests given what their agency pays. Officials from the other agency said KISO's basic services are cost-effective. Specifically, they said they'd have to pay more to get monitoring, security awareness training, and vulnerability scanning from a third-party vendor.

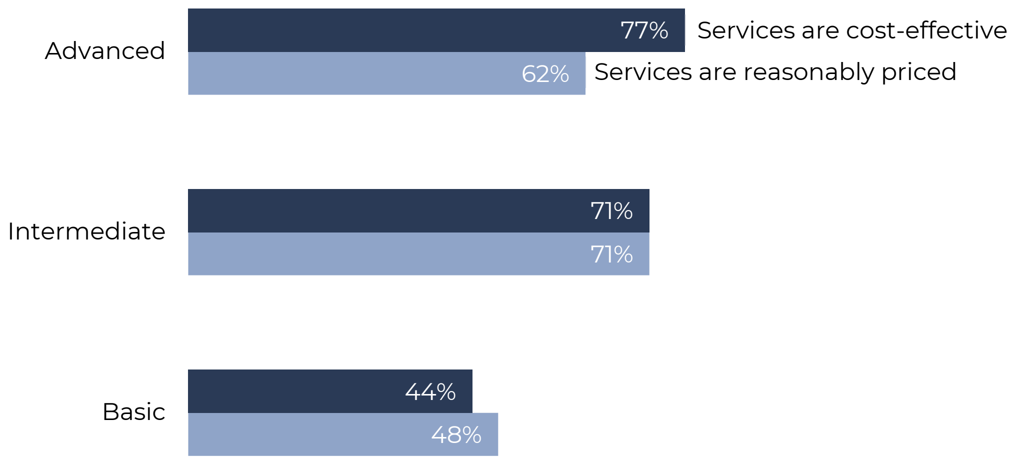
Survey respondents had generally positive opinions about KISO's cost-effectiveness, but some may not know about KISO's fees or what to compare them to.

- We also asked the 57 agency officials we surveyed for their opinions on the fees they paid for KISO's services.

- **Figure 7** shows respondents' opinions about KISO's prices and cost-effectiveness. We asked respondents whether they agreed with several statements. As the figure shows, most respondents expressed positive opinions about KISO's intermediate and advanced services. For example, of the agencies using intermediate services, 10 (71%) said these services are both cost-effective and reasonably priced.

Figure 7. Most survey respondents had positive opinions about intermediate and advanced services' costs.

Question: Please read the following statements about KISO's IT security services and select all that apply.



Source: LPA survey of executive branch agencies' top IT officials.

Kansas Legislative Division of Post Audit

- But some survey respondents may not be knowledgeable about KISO's fees or cybersecurity pricing. For instance, 1 said they couldn't tell whether basic services are cost-effective because they're bundled into OITS's service fees. KISO officials said they don't break these out in agencies' bills or publish them anywhere. Another respondent said they didn't have anything to compare to KISO to know whether their services are cost-effective.

KISO officials described steps they take to limit their costs, some of which may have unintended negative effects.

- Although KISO officials can't determine whether their services are cost-effective, they said they try to minimize their costs to keep agencies' fees lower.

- KISO pays salaries below industry averages and other service providers. This likely helps keep KISO's costs down. But noncompetitive wages and chronic openings may impact KISO's service quality.
  - We compared KISO's salary bands to industry data from the U.S. Bureau of Labor statistics and salaries paid and rates charged by 6 third-party vendors. These vendors included Allied Global, Bradford Galt, Charter

    Global, Global Solutions Group, Information Technology Group, and Levi Ray & Shoup.

    - KISO's non-information security officer positions offer salaries between about $55,000 and $94,000 depending on experience. But 2021 U.S. Bureau of Labor Statistics data show the average salary for Kansans in this field, including entry-level jobs, is about $92,000. KISO officials told us they've offered senior-level jobs to applicants who took entry-level jobs elsewhere for more money.

    - KISO's information security officer positions offer salaries between $85,000 and $102,500. But the 6 vendors whose contracts we reviewed all offered at least $130,000.

    - KISO officials said they have long-term openings of 6 months or longer for these positions that show they can't compete. KISO officials said they try to use existing staff to provide advanced services to agencies that have requested them while they seek to hire more information security officers.

- KISO officials also told us their ability to buy in bulk helps keep their costs down. KISO purchases software and tools for the entire state, rather than for 1 agency at a time. For example, KISO officials said they buy firewalls that will work for the largest number of agencies. They said they sometimes get discounted rates as a result.

- Finally, KISO officials said they've taken other steps to keep costs down. For example, they're using software licenses they've already paid for rather than going to new subscription service models.

Conclusion

Although the Legislature passed the Kansas Cybersecurity Act to improve executive branch agencies' cybersecurity, it's not clear whether this is actually happening. State law created the Kansas Information Security Office (KISO) to help agencies meet statutory cybersecurity requirements. But it left the responsibility for requesting those services and for agencies' cybersecurity with individual agencies. In practice, few executive branch agencies have requested and received KISO's intermediate and advanced services. And it's those more advanced services that address many requirements in the Cybersecurity Act. Together, this means KISO may not be as effective as the Legislature envisioned. Few agencies have received KISO's more advanced services for several reasons, including agencies' hesitation to give up control of their cybersecurity and KISO's lack of communication regarding what services are available.

Recommendations

1. The Kansas Information Security Office should more proactively educate state agencies about cybersecurity and KISO's available services.
    - Agency Response: The KISO will leverage existing communications and marketing resources within OITS to enhance outreach and visibility to agencies. In addition, further efforts will be made to coordinate with agency leadership to help communicate the value of their cybersecurity tools.

Agency Response

On May 23, 2022 we provided the draft audit report to the Department of Administration, Office of Information Technology Services, and Kansas Information Security Office. Their response is below. Agency officials thought our conclusions lacked important context about the iterative nature of developing holistic cybersecurity services. We did not change our findings or conclusions to include this information. However, the agencies' response provides additional explanation.

Department of Administration, OITS, and KISO Response

The creation of the Kansas Information Security Office (KISO) in 2018 was a critical step in elevating the importance of cybersecurity and information security in the State of Kansas. The Kansas Cybersecurity Act (KCA) set out to develop a foundation for cybersecurity across the executive branch with KISO as the lead organization.

The KISO provides critical security tools and services to many of the State of Kansas enterprise systems.

A few key highlights of KISO accomplishments over the past four years include:

- The KISO processes and analyzes approximately 60 billion information system security logs annually.
- In 2021, the centralized log management solution was recognized by Chief Security Officer magazine for a CSO50 award for thought leadership and business value. Industry leaders like Verizon, FedEx, Cisco, and Intel are other recipients of this award.

In the four years since the Kansas Cybersecurity Act (KCA) was signed into law, cybersecurity and information security efforts have been an iterative and evolving process. A fully matured IT security posture requires methodical scaling of operations and assurance processes as well as identifying stable funding mechanisms that don't punish smaller agencies.

The assumptions in the LPA report regarding KISO costs and services do not consider the iterative nature of developing a holistic security posture. In other words, the KCA was designed to take time to put into effect. Considering that the KCA did not carry out a funding mechanism or allow KISO authority to compel agencies to comport with KISO standards, KISO could not ensure a comprehensive IT security regime following the passage of the KCA. From the assumptions made in this report, KISO disagrees with some of the conclusions of the Legislative Post Audit.

Rates

The KCA did not provide funding support for the KISO. Therefore, the KISO had to establish some way to recover costs. The only way to recover costs is to either seek an appropriation from the legislature or to charge agencies for services.

The pay-for-service model is a solution that incentivizes agencies to spend very little on cybersecurity; Therefore, with no rate establishment or allocation of direct funding, security rates were built into enterprise service rates.

When the KISO was first created in 2018, efforts to establish a specific cybersecurity rate met significant pushback from agencies, so the rate was never implemented.

This solution ties security to overall IT operations and does not create a race to the bottom for security services. However, additional security services must be negotiated and billed to agencies.

Comprehensive security services from KISO are offered to agencies who are able and willing to pay for those services. The KISO believes this is an ineffective and inefficient model of funding.

All agencies need a minimum level of comprehensive cybersecurity and information security services. Some agencies also require a significantly higher level of security than others. The current funding model does not afford the KISO the ability to build specialized services to meet unique agency needs unless they are willing to pay for it. In addition, if services are provided a la carte style, or optional, agencies may choose to forgo key minimum cybersecurity capabilities at the expense of other agencies and the State of Kansas.

KISO Operations

The goal of the Kansas Information Security Office (KISO) is to provide the highest level of cybersecurity and information security capabilities across the state in the most effective and efficient manner.

The KISO is a “chargeback” office. For this reason, coupled with the resistance to the establishment of a separate security rate, many of the KISO operations are directed at providing security to the enterprise resources such as the state network KANWIN, supporting the managed datacenters, and providing security tools to the executive branch email solution.

Services and solutions are delivered to agencies in multiple ways. In some instances, the KISO manages the entire service from beginning to end. In other situations, the KISO leverages economies of scale by buying in bulk and providing several solutions for agencies to implement and manage at no cost to them. This allows agencies to not have to procure the solutions on their own with agency funds.

The Kansas Information Security Office is staffed with a highly professional and dedicated civil servant staff. Many of these employees hold highly in-demand industry certifications in information security and cybersecurity and represent the largest concentration of those certifications in the State of Kansas. The country as a whole is facing a dramatic shortage of cybersecurity professionals.

Cybersecurity and information security are a team effort that requires many people to actively participate.

There are three major types of security controls – managerial, operational, and technical. These security controls must work together for meaningful success within cybersecurity programs. In many cases, the KISO is only providing the technical components of the security controls and agencies are still responsible for the operational and managerial portions of the controls. This is evident in two of the three audit areas referenced in the report. For both security awareness training and vulnerability scanning, the KISO is providing a solution at no cost to the agencies. The agency still maintains most of the responsibility for the management and operation of those tools.

The KISO continues to mature and refine operations and the security operations of the agencies. Again, this is an iterative process, and the LPA's methodology that focuses on a specific point-in-time assessment is missing critical context.

Centralization and Authority

Nationwide trends indicate that enterprise-wide security operations must include centralized authority to enforce security standards.

Notably, the KCA did not grant the KISO any authority to compel agencies to abide by KISO standards.

In 2020, Deloitte and The National Association of State Chief Information Officers (NASCIO) conducted a study across the states to identify and address the numerous cybersecurity challenges states face. In their conclusion, they recommended states work to centralize cybersecurity efforts and fund them.

The centralized cybersecurity model is the best way to leverage scarce resources and provide the highest level of cybersecurity capabilities across the entire enterprise. Adding cybersecurity as an additional duty to other IT personnel can lead to challenges, inefficiencies, and gaps. IT Security is a highly specialized field, and the tasks of Security Engineers, Security Analysts, and Information Security Officers cannot be easily or effectively replicated by general IT staff. Organizations need resources dedicated to the complexities of cybersecurity.

Report Recommendation
As recommended by the LPA report, communication and marketing of security services are an area that KISO can mature.

The KISO will leverage existing communications and marketing resources within OITS to enhance outreach and visibility to agencies. In addition, further efforts will be made to coordinate with agency leadership to help communicate the value of their cybersecurity tools.

KISO and CITO Recommendation
As has been well documented, cyber threats around the country are rising, changing, and becoming increasingly more sophisticated. It is a critical moment to plan for enhancing future cybersecurity operations and allowing the State of Kansas to meet and address the increasing risk to the State of Kansas.

In an effort to continue advancing cybersecurity within the State of Kansas Executive Branch, the CITO and the KISO recommend amending the KCA to give the KISO the ability to set mandatory information security and cybersecurity policies and standards. In addition, the increasing cyber risk to the State of Kansas requires additional cybersecurity tools and capabilities that need to be applied across the board to protect all agencies. In order to ensure that the State can adapt to the increasing cyber risks and properly mitigate those risks, while affording the KISO the ability to respond to those risks in the most efficient and effective manner, cybersecurity funding should move to consistent and reliable appropriation model.

These steps will greatly enhance the KISO's ability to not only manage threats and risks but to create a holistic security posture that includes all agencies regardless of whether they have the resources or not.

Appendix A – Cited References

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

<u>Public reports</u>

1. Information Technology Consolidation: Evaluating Whether Consolidating Executive Branch IT Services is Feasible and How Much it Might Save (July, 2019). *Kansas Legislative Division of Post Audit.*

2. Occupational Employment and Wage Statistics (May, 2021). *U.S. Bureau of Labor Statistics.*

3. Occupational Outlook Handbook (2021). *U.S. Bureau of Labor Statistics.*

Confidential reports

4. Board of Healing Arts IT Security Audit (December, 2020). *Kansas Legislative Division of Post Audit.*

5. Department of Agriculture IT Security Audit (December, 2021). *Kansas Legislative Division of Post Audit.*

6. Department of Revenue IT Security Audit (August, 2021). *Kansas Legislative Division of Post Audit.*

7. Kansas Public Employees Retirement System IT Security Audit (December, 2020). *Kansas Legislative Division of Post Audit.*

8. Racing and Gaming Commission Arts IT Security Audit (October, 2021). *Kansas Legislative Division of Post Audit.*

9. Secretary of State IT Security Audit (February, 2020). *Kansas Legislative Division of Post Audit.*

10. State Treasurer's Office IT Security Audit (July, 2019). *Kansas Legislative Division of Post Audit.*