KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

3 Year Summary of Security Controls in Selected State Agencies (2017-2019)

February 2020

Report Number: R-20-006

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 three-year cycle. This three-year summary report answers the following question:

Do state agencies adequately comply with significant information technology security standards and best practices?

Between January 2017 and December 2019, we audited 19 agencies. **Appendix A** lists the individual agencies, their expenditures, and their approved FTE.

All our annual audit work evaluated some similar IT control areas. Examples include security awareness training, access control/account security, and vulnerability remediation. However, some of the work was unique to certain years. For example, our 2017 audit work included Cloud Technology and Mobile Device controls that we did not audit in all years.

Within each IT control area, we generally measured an agency's compliance based on the state's specific IT security standards. Those standards are codified in ITEC policies 7230A and 5310, and state law. We also reviewed compliance with certain best practices. We did this because the state's standards had not been updated to include some widely accepted industry standards.

To assess agency compliance, we interviewed staff, reviewed relevant policies and procedures, and evaluated relevant computer settings. We reviewed security awareness training documentation and other security controls. We also inspected data centers and performed vulnerability scans on agencies' computers. Lastly, we conducted limited social engineering tests.

We issued reports to each agency throughout the three-year audit cycle as soon as the work was done. These reports are confidential under K.S.A. 45-221 (a)(12) & (45) because releasing that information could jeopardize the agencies' IT security.

This summary report does not conform to generally accepted government auditing standards. That is because our earlier IT audits were not conducted according to standards. Starting in 2019, they have been.

More than 50% of the agencies we audited between 2017 and 2019 did not substantially comply with applicable IT security standards and best practices.

State Responsibilities and Initiatives

Under established security standards, state agencies must protect sensitive information against data loss or theft.

- Government agencies across the nation are consistently targeted because they maintain valuable information.
  - In March 2017, hackers targeted a system administered by the Kansas Department of Commerce's contractor America's Job Link Alliance and accessed more than 5.5 million social security numbers belonging to individuals from 10 states.
  - In March 2018, an attacker used a Minnesota Department of Human Services' employee's compromised email account to try to defraud coworkers.
  - In March 2018, the city of Atlanta suffered a ransomware attack that took a third of the city's software programs offline or partially disabled them. An Atlanta official said the restoration effort for all affected computers took about 12 weeks. Many police dashcam video files were permanently deleted.

- Many Kansas agencies collect tax, health, student, or other sensitive personal information. Examples include K-12 student records, tax returns, and health care information. Several agencies maintain confidential information that have significant penalties for loss or disclosure.

- Kansans depend on agencies to keep their information protected because they have no choice but to use the agency's services.

- The Legislature created the Information Technology Executive Council (ITEC) in 1998. ITEC has established security policies state agencies must follow.

- The state's ITEC security policies are similar to other available security standards. They include requirements for policies and procedures, physical controls, system controls, and application controls. Together they form a multi-layered approach to safeguard confidential data and are designed to help agencies create a strong security posture.

State agencies must balance their business needs against security risks.

- Generally, state agencies are not in the information security business. Their focus is on accomplishing their core missions such as collecting taxes, housing inmates, monitoring air and water quality and so on.

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

- Agencies must evaluate and understand their security risks to make informed decisions while carrying out their primary mission.

Several statewide initiatives are aimed at improving the state's information security.

- In 2011, Governor Brownback initiated IT centralization through executive order 11-46. This order required all non-regent IT directors under the Governor's jurisdiction to report to the Executive Chief Information Officer. It was intended to increase the efficiency and uniformity of IT within the executive branch.

- The 2018 Cybersecurity Act (K.S.A. 75-7236 et seq.) aimed to help reduce the risk of cybersecurity breaches within state agencies. Important features of the Act are as follows:

    - **It pertains to most executive branch agencies with a few exceptions.** Exempted agencies include elected office agencies, the Adjutant General's department, the Kansas Public Employees Retirement System, the regents' institutions, and the Board of Regents.

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

    - **It codified cybersecurity service costs.** The Act allows agencies to pay for cybersecurity services from several sources, including fees. It also allowed KISO to charge agencies for certain security related functions and required those fees to be used only for cybersecurity purposes.

    - **It clarified that agency heads remain responsible for their agency's security posture.** Agency heads must ensure an agencywide information security program has been established, designate an information security officer, participate in annual agency leadership training on statutorily prescribed cybersecurity-related topics, notify the CISO about breaches within 48 hours after discovery, and submit a cybersecurity report to the CISO every two years.

- In July 2019, ITEC revised the IT security standards agencies must follow. Prior to that revision, those standards were last updated in November 2014.

IT Security Audit Results

11 of the 19 (58%) agencies we audited over the past 3 years did not substantively comply with applicable IT security standards.

- At the start of each calendar year, we selected specific requirements to audit from the state's ITEC standards in place at the time. We also added several best practices. For example, our audit plans included testing 78 items across 13 areas in 2017 and 52 items across 9 areas in 2019.
- We evaluated whether agencies addressed each item in our audit plan. We then used professional judgment to score any vulnerabilities we found. In 2017 and 2018, we analyzed the likelihood and impact of the vulnerabilities to categorize them as either critical, high, moderate, low, or technical. In 2019, we simplified our method to a point system (3 points meant fully compliant, 0 points meant not compliant at all). For this summary report, we translated our 2019 noncompliance ratings as follows: 0 points = critical, 1 point = high, and 2 points = moderate.
- To fail an audit, findings needed to exist in several IT areas, and be severe enough for us to conclude the agency did not sufficiently comply with standards. 11 of the 19 agencies' we audited during the past three years failed their audit and 8 agencies passed.
- However, all agencies had at least some vulnerabilities, ranging from a low of 4 noncompliance items to a high of 35. In other words, no agency passed with a fully clean review.
- **Figure 1** shows the number of findings across <u>all 19 agencies</u> by IT control area and severity.

Figure 1
Heatmap of IT Security Findings Across 19 State Agencies (CY 2017-2019)

Security Areas	Critical/High (a)	Moderate/Low	Total
Vulnerability Remediation	35	9	44
Incident Response/Continuity of Operations	34	14	48
Security Awareness Training	22	24	46
Data Protection	20	25	45
Network and Boundary Protection	10	13	23
Account Security	10	36	46
Physical/Data center Security	10	26	36
Mgmt. and Contract Review	9	9	18
Selected Information Systems (b)	33	48	81
Total Number of Vulnerabilities (c)	**183**	**204**	**387**

(a) This heatmap is sorted based on the highest to lowest number of critical/high vulnerabilities across nine areas.
(b) This category included tests within Account Security, Data Protection, and Vulnerability Remediation.
(c) This excludes technical vulnerabilities identified in individual audits.
Source: LPA summary of IT security audits of 19 agencies conducted from January 2017 to December 2019.

- As the figure shows, a handful of areas had the most significant security weaknesses. Those areas included vulnerability remediation, incident response/continuity of operations planning, security awareness training, and data protection.

- We also reviewed specific IT systems that maintained or processed confidential or sensitive data for most of the audited agencies (last line of table). Findings in this area are discussed in more detail at the end of the report.

The security findings summarized in this report are similar to those in previous summary reports.

- Our audit work varies from year. Nevertheless, we consistently evaluate certain security areas we think are most important and part of a basic security system.

- Agencies across the state continue to have similar IT security issues since 2003. Results in this 3-year summary (CY 17-19) are similar to the results from the previous 3-year report (CY 14-16). Areas of greatest concern include inadequate scanning and patching processes, security awareness training, data protection, and incident response and continuity of operations planning. Several audits we produced in earlier years also identified control weaknesses with patching, security awareness training, data protection, account security, and business continuity planning.

- We do not audit the same agencies within each 3-year period. However, we have audited several agencies for the second or third time during the past decade. Some of these agencies have improved their security posture from one audit to the next, while others had repeat findings.

A lack of proper top management attention and inadequate resources generally were the main reasons for compliance problems.

- Agency top management ultimately is responsible for its information technology governance, risk management, and compliance. However, new agency heads may not be aware of their security responsibilities in the first place. This was the case for at least two of the agencies we audited. Additionally, top management may not set sufficient or consistent expectations or monitor results. For example, at one agency IT management overestimated the effectiveness of existing controls and underestimated other risks. At another agency, management relied on its existing controls despite staff turnover. Lastly, at several agencies, we noted top management exempted themselves from their own training protocols, was slow to implement security controls, or made a conscious decision to favor business activities over security.

- Inadequate IT security staff resources and high turnover within IT divisions make it difficult to create or maintain a security baseline or retain institutional knowledge. Several agencies with notable resource issues had no or few security staff to carry out the work even when those agencies were relatively large and held sensitive data. At a few agencies, IT positions remained vacant for months, or specific IT duties transferred to other staff. This contributed to security activities being dropped. Conversely, agencies that invested in IT resources and experienced staff generally had a robust security posture.

Most Significant or Common Security Weaknesses Across Agencies

Most agencies (79%) did not properly scan or patch their computers to keep them secure.

- Over time, vulnerabilities in computer software are discovered that could allow someone to break in or otherwise harm an agency's network. Agencies must periodically scan for known vulnerabilities. More importantly, agencies must test and apply patches to keep their computers secure.

  - **Many agencies did not scan their computers at all or performed only partial scans**. For example, one agency did not scan their computers due to bandwidth issues. Another agency only scanned computers that were managed by central IT. A third agency did not scan its internal servers on a regular basis.

  - **Most agencies did not properly patch their computers**. Our scans measured agencies' computers based on the Common Vulnerability

Scoring System (CVSS). The CVSS is a free and open industry standard to measure the severity of computer system vulnerabilities. A CVSS result of 70 on a computer equates to that machine containing 10 "high" vulnerabilities as classified by the industry. Many agencies had a CVSS average exceeding 70 – and often in the hundreds – indicating these agencies did not properly patch serious Microsoft and 3rd party software vulnerabilities. At least six agencies' computers had CVSS-recognized vulnerabilities that dated back a decade.

  - **Most agencies also used unsupported software, applications, or operating systems**. When those products become too old to maintain, vendors no longer release security updates for them. Those products are considered "unsupported." Our scans frequently found unsupported versions of common software such as Adobe Acrobat and Java. We also found unsupported internet browsers and operating systems such as Windows XP or Windows Server 2003.

- Without a systematic approach to identify and patch known vulnerabilities and eliminate unsupported products, agencies leave their computers open to attack from hackers. This increases the risk those computers are used to compromise the agency's network or even other agency systems.

Many agencies (63%) did not have adequate incident response or continuity of operations plans or did not appropriately test them.

- When events like a security breach, power outage, or natural disaster occurs, it is important for agencies to have a plan to follow. An incident response plan lays out steps to follow after a security incident, such as a network breach. Similarly, a continuity of operations plan (also called "business contingency plan") outlines the agency's strategy to keep the agency operational and minimize downtime. Once plans are in place, agencies should test them to ensure they work the way management intends and important information is not left out.

  - **Some agencies did not have an incident response plan while other agencies' plans were inadequate**. Additionally, four agencies that had an incident response plan did not test it to make sure it would be adequate if needed.

  - **Several agencies did not have an adequate continuity of operations plan.** For instance, one agency had not updated its plan in more than three years. Another agency's continuity of operations plan did not have any information concerning its IT systems. Three agencies did not have a plan at all.

- Having adequate plans and testing them regularly helps agency officials get through security breaches or natural disasters. Without them, agencies are less likely to be able to protect their resources and continue their operations.

Most agencies (89%) did not provide adequate security awareness training or failed our social engineering tests.

- Security awareness training educates employees on why security controls are necessary and where risks come from. One of those risks is social engineering—the art of manipulating, influencing, or deceiving people to circumvent internal controls and gain control over computer systems.
    - **Security awareness training processes were inadequate in a variety of ways.** Several agencies did not provide security awareness training to new employees who should receive training within their first three months on the job. At least one agency did not provide annual training to their staff as required. Several agencies did not have a dedicated training program at all or were missing key components. At two agencies we found executive level staff exempted themselves from attending.
    - **Most agencies failed simulated phishing email tests**. We tested eight agencies by sending simulated phishing emails claiming such things as notice of traffic violations, unread Twitter messages, or a failed package delivery. At five additional agencies, we relied on the agency or OITS to perform similar tests (five agencies opted out and we did not perform this test at one agency). Of the 13 agencies tested, only one agency had no staff who clicked on links. The other 12 agencies had between 3% and 22% of the tested staff who failed the test.
    - **Staff at several agencies did not dispose sensitive information properly.** For example, employees at one agency left sensitive documents in a box under their work areas even though secure locked shredding bins were nearby. The documents in the box included several names and social security numbers as well as a completed tax return. At another agency, the shred box was not properly locked and contained employee names and ID numbers, employee signatures, and two complete 16-digit procurement card numbers.
- Security awareness training is important because people are the weakest link in an agency's security posture. Agencies use technical hardware and software to implement security controls at several levels. However, all it takes is for one untrained employee to plug in a virus-infected flash drive or click on a phishing email link to bypass those controls.

Most agencies (89%) did not adequately encrypt, back up, or destroy electronic data.

- Agencies need to protect their data so that only authorized individuals can access it. Encryption is a sophisticated way to scramble electronic data so it can only be read by those who have the code to unscramble it. Additionally, agencies should maintain a copy of their data they can use in case something goes wrong with the primary data. Agencies should store the backup data sufficiently far away from their primary location and test the backup data to ensure it will work if it is needed. Lastly when agencies get rid of outdated hardware, they should ensure they destroy sensitive data on those devices.

- Six agencies did not encrypt sensitive data when transmitting it outside their network boundary. Several agencies did not test their backups to ensure they would work if needed. At least two agencies had their back up data located within a half mile from their primary data center. Several agencies did not follow proper destruction protocols when disposing of old drives or computer hardware.

- Agencies without backup data could face severe disruption should their primary data become unusable. When back up data is too close to the agency's primary location, the risk increases that a catastrophic event wipes out both data sets. Lastly, without encryption or an adequate destruction process, agencies risk their confidential data being accessed and used by unauthorized individuals.

Other Security Weaknesses Across Agencies

Several agencies (63%) did not adequately protect their network boundaries.

- A network firewall serves as a protective barrier between an agency's network (and the computers on that network) and the Internet. Agencies can use firewall rules and exceptions to control who gets access to their network.

- At least two agencies we audited did not have their own firewalls; they relied on other entities' firewalls to protect their data. Two other agencies were using firewalls with software or hardware that was outdated. Another agency did not properly log network communications.

- Because a network firewall is often an agency's first layer of defense, it is critical its software is up to date with the latest security patches. Agencies who share a firewall are at greater risk of exposing their networks and data to unauthorized access because they are not in full control of the firewall rules or exceptions. Using a separate firewall device is one of the best ways to limit this risk.

Nearly all agencies (95%) lacked at least one important account security control.

- Account security controls are designed both to limit and track who has access to an agency's network and data. One common control is to require account passwords to be a certain length or to contain letters and special characters. Another control locks out users from trying to log in to their accounts if they enter the wrong password too many times. This prevents hackers from trying numerous passwords until they find one that works. A third control prohibits administrative accounts—accounts that can make any changes to the system including adding or deleting users—from being shared by more than one person.

- Many agencies had shared network accounts such as "HelpDesk." One agency did not meet complex password requirements. Another agency did not restrict the number of times a user could enter incorrect passwords. One agency left accounts of former employees open for more than six months. At least two agencies shared accounts between IT staff to perform administrative tasks, such as creating or deleting users.

- When account security processes are weak, it is easier for unauthorized individuals to circumvent them and gain access to an agency's network and data. Shared administrative accounts make it more difficult to determine who made a specific network or system change.

Most agencies (79%) had poor access or environmental controls for their data centers.

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

- Many agencies did not sufficiently limit access to their data centers. At one agency, more than 60 individuals, including an administrative assistant, had unescorted access even though it was staffed 24/7. Another agency had issued 17 key cards to allow 24/7 access to its primary and backup data centers. This included two access cards not linked to a specific person. We identified several staff, including locksmiths and support staff had access which we questioned as necessary. Several other data centers we evaluated lacked environmental controls to protect the agency's data from fire, water, or humidity damage.

- Poor data center access controls increase the risk that individuals could lose, damage, or steal assets or data. Agencies that use data centers with poor environmental controls risk data loss from fire or water damage. These problems could severely disrupt the agency's ability to provide services.

Several agencies (58%) had management, contract, or policy-related weaknesses.

- Agency policies should describe rules for how staff should use agency-issued equipment and the internet. In addition, Kansas law requires most executive-branch agencies to designate someone to oversee their security programs. Lastly, agencies should incorporate language into IT-related contracts that protects both the agency and its data.

- We found agencies had problems in all three areas.

  - One agency's policies did not define limits on how the internet should be used.
  - Several agencies did not designate someone to oversee their security programs as required by law.
  - We reviewed IT-related contracts at several agencies and found contracts often did not include language to allow the agency to validate its contractor's security controls. Additionally, some contracts were missing clauses on how confidential data should be handled after the contract is terminated.

- When agencies do not set clear expectations through polices, it is more difficult to hold employees accountable for risky actions (e.g. using the internet inappropriately). Similarly, entities that use contractors should not simply assume the contractors will take the necessary precautions to protect the agency's sensitive data.

<u>Review of Specific Information Technology Systems</u>

Significant security issues exist within agencies' specific IT systems.

- At 17 of the 19 agencies we audited, we also reviewed specific IT systems that maintained or processed confidential or sensitive data. For those systems, we reviewed a limited number of account security, data protection, and vulnerability remediation controls similar to the agencywide tests within our audits.

- We found a significant number of problems within agencies' specific IT systems. Here are a few examples of what we found:

  - **Agency systems had poor account security.** At one agency, a former employee still had access to the system at the time of our audit despite not having worked for the agency for four months. Another agency had not configured any password settings for the system we evaluated: Agency IT staff was able to set up a test account with a one-character password.

  - **Agency systems were missing data protection.** At one agency, the system's developers actively programmed within the live production environment. A mistake made during programming could affect the system which was actively being used. The same agency also was not backing up the system or its data, so if something went wrong with the system it risked losing all of their data.

    - **Agency systems were not sufficiently scanned and patched.** For example, at one agency, the system server had seven critical or high vulnerabilities, one of which was four years old.

- Our audit results show security weaknesses exist not only at an agency-wide basis, but more importantly on systems that hold sensitive data most important to an agency's mission.

Conclusion

Our IT security audit work over the past three years revealed significant weaknesses in several security control areas across the 19 agencies we audited. Agencies consistently struggled in four areas: vulnerability remediation (scanning and patching computers), incident response and continuity of operations planning, security awareness training, and data protection. These themes are consistent with issues we identified in our prior 3-year summary in 2016. Problems appear to be the result of two main issues: insufficient management oversight and lack of adequate IT resources.

The state will face significant consequences if hackers are able to access an agency's network or confidential data because of poor security controls. A significant security breach could disrupt an agency's mission-critical work and their reputation would be sorely damaged. A breach also could require costly customer credit report monitoring and could create legal liabilities or financial penalties for the state.

Although the state has taken steps to strengthen security by passing the Cybersecurity Act and centralizing some IT positions and services through the Office of Information Technology Services (OITS), more needs to be done to create a stronger security posture across state agencies.

Recommendations

We did not make any recommendations for this summary audit. All 19 agencies we audited during the past three years received individual recommendations to fix the problems identified. Based on the initial responses to the audits, agencies generally planned to remediate most findings. We conduct follow up work the following calendar year to check on agencies' progress. Our follow up work from audits performed in 2017 and 2018 showed that agencies said they fixed only about half (46%), of the critical, high and moderate findings. Agencies said the remaining findings were still in progress of being fixed (45%) or not started or refused (9%). Follow up work for agencies audited in 2019 will take place in Fall 2020.

Appendix A – List of Audited Agencies - 2017-2019 IT Security Audit Cycle

This appendix includes the list 19 agencies we audited between January 2017 and December 2019. The list includes each agency's expenditures and approved FTE.

Agency Name	FTE Staff (FY 2018)	Expenditures (FY 2018) (a)
Kansas State Department of Education	258	$4,945,800,000
Kansas Dept. of Health and Environment	1,165	$2,682,300,000
University of Kansas	5,347	$918,100,000
Department for Children and Families	2,508	$616,300,000
Department of Administration	419	$238,600,000
Fort Hays State University	1,077	$149,600,000
Pittsburg State University	976	$108,500,000
Department of Commerce	283	$105,600,000
Kansas Highway Patrol	881	$89,400,000
Larned State Hospital	943	$66,600,000
Osawatomie State Hospital	374	$41,500,000
Kansas Bureau of Investigation	330	$37,500,000
Kansas State Treasurer	39	$30,100,000
Board of Indigents' Defense Services	197	$29,400,000
Kansas Neurological Institute	436	$24,900,000
Attorney General's Office	152	$23,000,000
Kansas State Library	30	$5,400,000
Kansas Secretary of State	36	$3,900,000
Pooled Money Investment Board	5	$700,000

(a) Rounded to the nearest $100,000
Source: Governor's Budget Report, FY 2020, Volume 2