AUDIT PROPOSAL

Information Systems: Reviewing Specific IT Security Controls across State Agencies and School Districts (CY 2023-2025)

SOURCE

This audit proposal was suggested by LPA staff to satisfy requirements in K.S.A. 46-1135.

BACKGROUND

Many state agencies and school districts collect and process millions of sensitive records in their computer systems, including individuals' social security numbers, medical and financial records, tax information, and student information. Additionally, several government entities process payments including paychecks, unemployment, or childcare assistance benefits. Government entities often use multiple security layers to protect data and computers from cyber or physical attacks including locked doors, employee badges, network firewalls, and user passwords. While these measures are good, they should be evaluated periodically to ensure the entity's sensitive data is sufficiently protected from accidental or intentional data breaches.

Currently, there is limited oversight of government entities' security controls to ensure they are adequately protecting confidential data. The Kansas Information Technology Executive Council (ITEC) has developed standards across several security areas including security awareness training, access controls, and physical and environmental safeguards. These standards were created to ensure state agencies develop adequate security controls. Additionally, ITEC standards exist for business contingency, which includes continuity of operations and disaster recovery for agencies to ensure critical operations are continued or resumed as quickly as possible after a significant service disruption. Lastly, several other national and international security standards are available for entities to evaluate to secure their environments. Government entities have a significant amount of autonomy in how they develop, apply, and monitor these security controls.

The 2015 Legislature passed K.S.A. 46-1135, which directs our office to conduct information technology audits as directed by the Legislative Post Audit Committee. Those audits are to include an assessment of the security practices at state agencies or any other local subdivision of government receiving funding from or through the state. These audits are conducted on a three-year cycle.

AUDIT OBJECTIVES AND TENTATIVE METHODOLOGY

The audit objectives listed below represent the questions that we would answer through our audit work. The proposed steps below each objective are intended to convey the type of work we would do but are subject to change as we learn more about the audit issues and are able to refine our methodology.

Objective 1: Do selected state agencies adequately comply with certain information technology security standards and best practices? Our tentative methodology would include the following:

- Select 10-15 agencies or school districts to be audited based on our statewide triennial risk assessment and other factors including previous audit coverage, findings, and other threat factors.

- Interview Office of Information Technology Services officials and other stakeholders to identify particular high-risk topics within standard IT control areas to evaluate the agencies on. The topics selected for individual audits should represent significant IT control risks and be based on specific requirements from the Kansas Information Technology Executive Council (ITEC) or best practices from other relevant standard-setting bodies.

- Assess selected entities' compliance through appropriate evidence-gathering techniques based on the selected control topics. Examples include reviewing employee training and other agency records, testing computer vulnerability remediation processes, observing access control settings, reviewing asset inventory policies and processes, observing physical security compliance, interviewing IT and other staff, and other work as applicable, depending on the IT controls selected for review.

- Interview entity officials and staff as needed to understand any compensating controls that they have implemented to comply with selected IT controls.

ESTIMATED RESOURCES

These audits will be conducted by our 3-person information technology audit team.

Note: This audit proposal results in 2 public reports each covering about 10-15 entities during the calendar year.