SCOPE STATEMENT

State Agency Information Systems:
Reviewing Security Controls in Selected State Agencies (CY 2013)

Each year, most state agencies collect and process sensitive and confidential data in their computer systems, including citizen social security numbers, medical information, and income data. Some agencies are responsible for protecting millions of confidential records, which makes them a potentially enticing target for hackers.

Often, agencies use multiple security layers to protect data and computers from cyber or physical attack. Potential security layers include perimeter security, physical security, and host security. Because no one layer can protect an agency against all threats, it is important to have multiple controls that complement each other and are independently secure. Weak or missing layers can create holes in the agency's overall security, which increases the risk for agency data to be compromised.

Currently, there is limited oversight of agencies' security controls to ensure that agencies are adequately protecting confidential data. The Kansas Information Technology Executive Council (ITEC) has developed guidance to assist state agencies in developing adequate security controls, but ITEC doesn't monitor or audit how well those controls are implemented. Consequently, agencies have a significant amount of autonomy in how they develop, apply, and monitor security controls.

The Legislative Post Audit Committee approved information system audits as an adjunct to the division's compliance and control audits. This information system audit looks at eight important information technology security areas across a broad selection of state agencies.

This information security audit answers the following questions:

1. **Do selected state agencies have an adequate security management process to assess, manage, and monitor IT risks?**

2. **Do selected state agencies adequately control passwords?**

3. **Do selected state agencies provide adequate security awareness training to all staff?**

4. **Do selected state agencies adequately patch servers and workstations?**

5. **Do selected state agencies have adequate anti-virus to protect their networks from viruses and other malicious software?**

6. **Do selected state agencies adequately control mobile devices connected to their network?**

7. **Do selected state agencies adequately monitor their network to detect and prevent breaches?**

8. **Do selected state agencies have adequate policies and procedures for <u>continuing operations in the event of an emergency</u>?**

To answer these questions, we would perform an overall evaluation of each agency's security management process. Specifically, for each security area, we would review agencies' policies and procedures and compare them to state IT requirements and best practices. We would also interview agency officials and staff to determine how well policies and procedures are being followed in practice, and would survey agency staff to determine their knowledge of IT policies and procedures. Where possible, we would perform direct test work to determine whether agency actions in these security areas were achieving the intended results. We would perform additional work in these areas as necessary.

Estimated resources: 3 staff for 9 months (plus review)

Agencies Selected for Audit

1. Department of Administration
2. Department of Aging Disability Services
3. Department of Children and Families
4. Department of Health and Environment
5. Kansas Attorney General
6. Kansas Board of Regents
7. Kansas Bureau of Investigation
8. Kansas Highway Patrol
9. Kansas Public Employees Retirement System