MEMORANDUM

Legislative Division of Post Audit
800 SW Jackson, Suite 1200
Topeka, KS 66612-2212
voice: 785.296.3792
fax: 785.296.4482
web: www.kslpa.org

TO: Members, Senate Ways and Means Committee
FROM: Scott Frank, Legislative Post Auditor
DATE: March 5, 2015
SUBJECT: Written Testimony Supporting House Bill 2010

Please accept my written testimony in favor of House Bill 2010, which would amend the Legislative Post Audit Act to create a new form of IT audit—systems implementation audits.

NOTE: This bill is identical to Senate Bill 7, which was passed by the Senate on February 25. My testimony here is almost identical to my testimony on Senate Bill 7. To save space, I have removed all of the attachments from my original testimony.

Issues With Government IT Projects

As of September 2014, the State of Kansas had 17 active IT projects under development that were each expected to cost at least $250,000, including two that were expected to cost at least $18 million.

Currently, these projects are overseen at three different levels. First, all such projects are overseen centrally by the Enterprise Project Management Office within the Office of Information Technology (OITS). Second, each branch of government has a Chief Information Technology Officer (CITO) who is responsible for overseeing the projects within his or her own branch. Each CITO is also responsible for working with the other CITOs to coordinate IT projects across all three branches. Finally, the Legislative Branch CITO provides periodic progress reports on the status of all large projects to the Legislature's Joint Committee on Information Technology (JCIT). This system of oversight relies heavily on self-reported status reports that are prepared by the manager for each project and compiled by the Enterprise Project Management Office.

Despite these three layers of oversight, several recent projects within the state have run significantly behind schedule, come in over budget, or have not delivered the functionality that was expected. For example, the Department of Administration's SMART accounting system was implemented in 2010 but has not functioned as expected. Similarly, the Department of Revenue's Division of Motor Vehicles has worked for the past several years on a system to upgrade the state's motor vehicle registration and drivers' license systems. The motor vehicle system was deployed in 2012 and experienced a number of problems which created long delays in some counties. The drivers' license system has yet to be implemented and as of October 2014 was nearly three years behind schedule. Perhaps most notable is the Department of Labor's Unemployment Insurance Modernization project. The project began in 2004, stopped and restarted several times with different vendors, and was finally canceled in 2011 with only a few usable components completed.

Unfortunately, unsuccessful government IT projects are common. Various articles in online literature suggest that 25-50% of all government IT projects run over budget, are not completed on time, or fail to deliver the functionality that was expected. In 1995, Legislative Post Audit developed a guidance document for agencies that summarized many of the reasons why IT projects in Kansas had under delivered or completely failed. Those reasons included agencies failing to conduct an adequate needs assessment before the project started, putting staff in charge of overseeing the project who lacked adequate project management training and experience, and not implementing an adequate quality control process to check the vendors' work.

Systems Implementation Audits

Historically, audit offices in most states rarely get involved in evaluating a government IT project until after it has failed. For example, Legislative Post Audit was directed to evaluate problems associated with the Department of Revenue's aforementioned motor vehicle system. While audits such as this are useful in determining who was at fault and what went wrong with a specific project, the lessons learned from these audits are not easily transferred to other projects. As a result, after-the-fact audits of specific projects are limited in their ability to prevent future problems.

At least two state audit offices have taken a more proactive approach to auditing IT projects in order to more effectively prevent problems before projects fail. In Virginia and Colorado, the state auditors conduct continuous audits of ongoing IT projects, also known as systems implementation audits.

These states assign auditors who have been trained in project management methodologies to monitor high-risk IT projects early in the process. The auditors attend all project planning and status meetings, and review bi-weekly status reports to monitor the progress of their assigned projects. They look for indications that the project might be in trouble, including many of the kinds of issues identified in our 1995 guidance document. The advantage of having an outside auditor embedded in a project is that outside auditor may recognize the signs of trouble more easily than a project manager who has a vested interest in the success or failure of the project.

When the auditors identify problems that indicate a project may be at risk, the audit office communicates the problems to agency management, to the central IT agency, and if necessary, to the Legislature. The goal is to identify problems early, when there are more options for addressing them, rather than allowing the problems to compound and have the project fail.

Provisions of House Bill 2010

The first key provision of House Bill 2010 would add a new category of audits to the Legislative Post Audit Act—information technology audits. This new category of audits would include the proposed systems implementation audits described above, as well as our current IT security audits which examine the controls agencies place around their most sensitive data. Under the provisions of House Bill 2010, all information technology audits would be conducted at the direction of the Legislative Post Audit Committee.

The second and most important provision of House Bill 2010, would give the Post Auditor additional flexibility in reporting on any problems that arise during a systems implementation audit. Under current law, the findings of any audit are confidential until after they are presented to the Legislative Post Audit Committee in an open meeting. In the case of systems implementation audits, this would mean that potential problems with an IT project could not be communicated to anyone outside the agency until after a Post Audit Committee meeting. This could significantly slow down the ability of those who govern these IT projects to respond to problems.

House Bill 2010 addresses this key reporting issue by giving the Post Auditor the authority to immediately communicate potential problems regarding a specific project to the Legislative Post Audit Committee, JCIT, and the three CITO's. This provision would be unique to systems implementation audits, but is critical because timely feedback is essential to correcting problems with IT projects.

Implementing House Bill 2010

Staff Resources

We would plan to conduct the systems implementation audits within our existing resources. Based on our conversations with Virginia and Colorado, the auditors who monitor these projects should be certified as Project Management Professionals (PMP) to make sure they have the necessary expertise and credibility. This type of training is available through the Office of Information Technology Services, but would take time to acquire. We estimate that it would take us about 6-12 months to develop the capacity to monitor projects.

Selecting Projects

We would start by monitoring just a couple of projects, but even when the audits were up to full capacity we would not have the resources to monitor all of the state's large IT projects. Consequently, the Legislative Post Audit Committee would need a process to select the projects that would be audited. Virginia uses a risk-based approach, focusing its efforts on projects that are expensive, have a longer timeframe, are especially complicated, or involve agencies that have a poor history with IT projects. We would suggest a similar approach for Kansas, the details of which would be worked out by the Legislative Post Audit Committee through its committee rules.