

Office of the City Auditor
Kansas City, Missouri

Highlights

Why We Did This Audit

We did this audit because security controls for the city's e-service systems are important to protect the information the systems contain. Businesses and individuals using the on-line systems to make a variety of payments to the city are required to provide credit card numbers, taxpayer identification numbers, social security numbers, business revenue figures, and other personally identifiable information. Unauthorized access to these systems could result in lost/compromised data, service unavailability, or identity theft.

Our work focused on the control and security of the e-services systems and related data.



For more information, please contact the City Auditor's Office, at 816-513-3300 or auditor@kcmo.org.

To view the complete report go to www.kcmo.org/auditor and click on Audits and Memos.

PERFORMANCE AUDIT

E-Service Systems Security

What We Found

The city currently offers the public a number of e-services for making on-line payments. Businesses and individuals can pay earnings taxes, convention and tourism taxes, water bills, as well as traffic and parking tickets. The public is also able to register for Parks and Recreation classes and electronically obtain permits through the city's website. On-line payments totaled about \$10 million and Automated Clearing House transfers totaled about \$40 million in fiscal year 2009.

The city's e-service systems and data appear to be reasonably secure. An outside firm performed an information security assessment and rated the city's network security above average. The assessment also identified a number of high risk vulnerabilities in the e-service applications, which were resolved by the Information Technology Department (ITD). Another outside firm's assessment determined that the city complies with the payment card industry's data security standards. The periodic external assessments and ITD's corrective actions based on these assessments provide reasonable assurance that the city's e-service systems and related data are secure.

The Information Technology Department's security policies do not always clearly define security responsibilities and while the city follows a number of the recommended e-service security practices, some are not included in ITD's written policies and procedures. This includes requiring departments to reconcile on-line payments.

The city also lacks an entity wide information security management program that encompasses all information security, including application level systems and programs. An overall information security program would provide the foundation for the city's information security control structure and reflect senior management's commitment to addressing security risks.

What We Recommend

We make several recommendations to further improve internal controls related to the city's e-service systems security.

- The city manager should develop and implement an entity wide information security management program.
- The director of information technology should develop and implement more comprehensive written policies and procedures to improve overall system security; strengthen internal controls; and improve communication about e-services security issues between the information security group, web development group, and user departments.
- The director of finance should develop and implement policies and procedures related to reconciling on-line payments.

Management agrees with all the report recommendations.