E-Services Follow-Up Audit
March 2015

Lori Brooks, City Auditor
Susan Edwards, Assistant City Auditor

City Auditor's Office

March 27, 2015

Honorable Mayor and Members of the City Council:

I am pleased to present the E-Services Follow-Up Audit. The audit objective was to determine the implementation status of prior audit recommendations.

Audit follow-up results indicate that management fully implemented three prior audit recommendations, partially implemented one recommendation, did not implement two recommendations, and one recommendation was no longer applicable.

We would like to thank the Information Technology Department personnel for their cooperation during the audit and their implementation of our prior audit recommendations.

Lori Brooks

Lori Brooks, CPA, CIA, CGAP, CRMA
City Auditor

c: Trey Yelverton, City Manager
Theron Bowman, Deputy City Manager
Jim Parajon, Deputy City Manager
Gilbert Perales, Deputy City Manager
Dennis John, Chief Information Officer

E-Services Follow-Up Audit
Table of Contents

Page

Executive Summary 1

Audit Scope and Methodology 3

Status of Prior Audit Recommendations Matrix 4

E-Services Follow-Up Audit

Office of the City Auditor
Lori Brooks, CPA
City Auditor

Project #14-10 ***March 2015***

Executive Summary

Three of seven prior audit recommendations were fully implemented

Fully Implemented

Consider implementing a continuous security threat assessment process

Seek Service Level Agreements for web services

Identify risks and develop a methodology to identify and resolve security vulnerabilities

Partially Implemented

Ensure vendors provide attestation of PCI compliance and an external assessment of their internal control environment

Not Implemented

Work with E-commerce vendors to mitigate risks

Establish a methodology to periodically assess vendor control environments and PCI compliance

No Longer Applicable

Assess/monitor AMANDA transaction logs

The City Auditor's Office has completed a follow-up audit of the E-Services Audit released in August 2013. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit objective was to determine the implementation status of prior audit recommendations.

Management concurred with all seven recommendations in the initial audit report. Audit follow-up indicates that the Information Technology Department has fully implemented three of the recommendations, partially implemented one, did not implement two, and one recommendation is no longer applicable.

The Information Technology Department has fully implemented the following:

- Considered implementing a continuous security threat assessment process for the City's E-commerce websites.
- Included Service Level Agreements for web services in new contracts.
- The Information Technology Department engaged a vendor to assist in identifying risks associated with technology and developed a methodology to address security vulnerabilities.

The following is the current status of the recommendation that has been partially implemented:

- Reports related to PCI compliance were provided. However, reports of an external assessment of the internal control environment related to web services have not been provided.

Two recommendations have not been implemented. These recommendations include working with E-commerce vendors to mitigate risks identified in the original audit and establishing a methodology to periodically assess the adequacy of vendor control environments and vendor compliance with PCI standards. Action to address these recommendations was delayed. It is anticipated that the implementation of a security program in FY 2015 will address these recommendations.

One recommendation related to the monitoring of AMANDA transaction logs to ensure sensitive data is not retained in the buffer is no longer applicable. A new Arlington Permits Public Portal was implemented in March 2014. This new portal uses a hosted order page to collect credit card information, thus this information is no longer collected or stored on any City servers.

Internal Audit recommends that the City Manager assure that appropriate action is taken upon implementation of the security program proposed by the Chief Information Officer.

For additional details, please see the recommendation matrix beginning on page 4 of this report.

Audit Scope and Methodology

The following methodology was used in completing the audit.

- Discussed the current implementation status of the recommendations with Dennis John, Chief Information Officer.
- Reviewed the FY 2014 and 2015 budgets for the Information Technology Department.
- Reviewed the Information Technology Risk Assessment performed by CliftonLarsonAllen LLP.
- Reviewed attestations of PCI Compliance from Tyler Technologies and Policereports.us.
- Reviewed the Information Technology Risk Assessment Update completed in December 2014 by CliftonLarsonAllen LLP.

Status of Prior Audit Recommendations

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
1. The Chief Information Officer, with assistance from application system owners, should consider implementing a continuous security threat assessment process for the City's E-commerce websites.	Concur	As part of the implementation of a funded IT security program which was requested during the 2014 budget process, the Department of Information Technology will make the implementation of security threat assessment process an expectation of this program. Security resources will work with system providers and external vendors to set security expectations and establish who will be responsible for testing, frequency of testing and responding to results of these tests.	Chief Information Officer	March 31, 2014 (subject to budget resources)	Implemented **Management Comment:** The IT Department submitted a budget issue for a security program that was deferred as part of the 2014 Budget. The FY15 budget included $225k to partially fund an ongoing IT Security program. Resources from CLA were engaged in Nov. & Dec. 2014 to refresh the security audit and assist in prioritizing risks identified. CLA results ranked Security Consulting, expansion of Threat & Vulnerability tools and expansion of Logging and Alert tools as highest priorities fitting in to the FY15 funding allocation. FY16 priorities will include annual internal and external testing and other recommendations from implementations/results from FY15 implementation. **Internal Audit Comment:** This recommendation is deemed implemented since the recommendation was to ***consider*** implementing a continuous security threat assessment process. Based on the budget issues submitted in FY 2014 and FY 2015 for funding for a security program, it was determined that management had considered implementing a continuous security threat assessment process.
2. The Chief Information Officer should work with E-commerce vendors to mitigate the risks identified.	Concur	With the establishment of a security threat assessment process established in the above audit recommendation, the Chief Information Officer with resources from a funded IT security program will work with vendors to mitigate identified risks.	Chief Information Officer	Ongoing, based on risk program process from above response	Not Implemented **Management Comment:** The audit recommendation would require IT staff to work with application owners to change their application code, database code or other vendor owned infrastructure affecting their applications. The skills and security expertise required to work with vendors at this level does not currently exist within the COA IT

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
					department. These higher skills set would be needed to allow us to work productively with the identified vendors. The IT Department submitted a budget issue for a security program that was deferred as part of the 2014 Budget. The ability to take action on this finding is dependent upon the establishment of a funded security program with qualified individuals who possess skills and availability beyond what is currently provided in the IT department. With the initiation of a security program in FY15, recommendations from CLA resources and review and recommendations from security professionals resources engaged in FY15 will assist in reviewing risk comprehensively, prioritizing highest vulnerabilities and allocating funding to the most effective use in a security program. This will include expertise in reviewing 3rd party compliance and recommendations of remediation to these vendors where appropriate. **Internal Audit Comment:** Based on information provided by the CIO, Internal Audit determined that no action had been taken to address the vulnerabilities identified in various E-commerce applications. It is anticipated that this recommendation will be addressed with the implementation of the security program in FY 2015.
3. The Community Development and Planning Director, in conjunction with the Chief Information Officer, should require AMANDA project staff to assess/monitor AMANDA transaction logs to ensure sensitive data is not retained in its buffer.	Concur	As part of system version upgrades to the AMANDA application currently underway and continuing into 2014, IT will work to automate the process of clearing any sensitive data which should not be retained.	IT Department	June 30, 2014	No Longer Applicable **Management Comment:** The new Arlington Permits Public Portal went live on March 22, 2014. The Arlington Permits Public Portal was implemented using a new format for collecting credit card transaction data. Using CyberSource hosted order page to connect credit card information, the City no longer

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
					receives this sensitive information on our servers. Under the new AMANDA version and configuration, this credit card information is never collected or stored on any of our AMANDA servers and therefore there is no need to clear this sensitive data from our transaction log files or our buffers. This requirement was completed as of 3/22/2014. **Internal Audit Comment:** This recommendation was deemed to be no longer applicable. Based on information provided by the CIO, the need to monitor transaction logs and buffers was eliminated with the upgrade to a new version of AMANDA. With the new version, no credit card information is ever stored on the City's servers. All information is collected on a third party site.
4. Upon contract renewal, the Chief Information Officer (in conjunction with department directors and the City Attorney's Office) should seek Service Level Agreements for City of Arlington web services, emphasizing software quality, service standards, liability and security.	Concur	IT will work with vendors, and City of Arlington department directors and the City Attorney's Office to include service level agreements where acceptable in the renewal of vendor contracts for application services.	IT and Other City Departments	As contracts expire and are renegotiated.	Implemented **Management Comment:** Ongoing. IT continues to monitor new or renewing contract with vendors who provide E-commerce applications to the City for opportunities to establish or enhance Service Level Agreements. **Internal Audit Comment:** The CIO provided examples of new contracts that include Service Level Agreements. Thus, this recommendation was deemed implemented. However, this action will be ongoing as new contracts arise and existing contracts renew.
5. The Chief Information Officer should ensure that the police reports vendor provides an attestation to their PCI compliance and that Tyler Technologies and the police reports vendor provide an external assessment of their internal control environment related to web services	Concur	Information Technology along with APD will work to obtain PCI compliance documentation from Policereports.us and will work with both APD and the City's Municipal Court to obtain appropriate validation of their vendor's internal control	IT and Arlington Municipal Court	December 31, 2013	Partially Implemented **Management Comment:** Tyler Technology was contacted and provided their current PCI compliance documentation. Policereports.us was contacted and also provided their current PCI compliance documentation. **Internal Audit Comment:** Reports related to

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
provided to the City.		environment.			PCI compliance were provided. However, reports of an external assessment of the internal control environment related to web services have not been provided.
6. The Chief Information Officer, in conjunction with the Chief Financial Officer, should establish a methodology to periodically assess the adequacy of its vendors' control environments and the vendors' compliance with PCI standards.	Concur	As part of the implementation of a funded IT security program, the Department of Information Technology will work with the Chief Financial Officer to establish a requirement that vendors who perform e-commerce functions on behalf of the City of Arlington annually supply copies of SSAE16 and PCI compliance documentation.	IT with assistance from FMR	March 31, 2014	Not Implemented **Management Comment:** The audit recommendation would require IT staff to have a much higher level of training and understanding of PCI compliance in order to communicate and test expectations with vendors. The skills and security expertise required to work with vendors at this level does not currently exist within the COA IT department. These higher skills set would be needed to allow us to work productively with the identified vendors. The IT Department submitted a budget issue for a security program that was deferred as part of the 2014 Budget. With the initiation of a FY15 security program and implemented use of a security consulting vendor, IT will utilize these services to assist in the development of an effective vendor review program combined with the skills of the security vendor to assess the adequacy of a vendors control environment. **Internal Audit Comment:** The CIO indicated that the IT Department has started requesting PCI and SSAE 16 reports from vendors. However, this task is spread among a number of individuals and there is no monitoring to assure that the reports are received. Additional action is necessary to fully implement this program. The reports should be reviewed and tracked to assure that they are adequate and that they are received from all vendors. It is anticipated that this recommendation will be addressed with the implementation of the security program in FY 2015.

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
7. The City Manager should require that the City's Information Technology Department identify risks associated with technology and develop a methodology to identify and resolve security vulnerabilities. Such resolution may include the identification of the need for additional resources (training, staff, consultants) and/or reassignment of existing personnel or other resources.	Concur	The City's Information Technology Department contracted with Clifton Larson Allen, an information security services firm, to conduct a risk assessment of the City's technology network's vulnerabilities to both external and internal threats. The firm's recommendations included a priority to identify a resource whose responsibilities would include developing, implementing and monitoring security and compliance functions for the City's Information Technology systems. The FY 2014 IT Budget Requests include funding for said resource.	Chief Information Officer	2nd Qtr. FY14	Implemented **Management Comment:** During the 2012 CLA Security audit, the vendor identified issues and assisted the IT department staff in correcting identified vulnerabilities. IT also engaged a monitoring service to assist with identifying additional threats on a real-time basis. Development of additional risk/threat processes as recommended in this audit finding require a much higher level of training and understanding than currently available within the IT staff. The IT Department submitted a budget issue for a security program that was deferred as part of the 2014 Budget. The FY15 budget included $225k to partially fund an ongoing IT Security program. Resources from CLA were engaged in Nov & Dec, 2014 to refresh the security audit and assist in prioritizing risks identified. The Dec14 CLA results reflected substantial progress made with limited resources in addressing risks identified in the FY13 Security audit. CLA Dec14 results ranked Security Consulting, expansion of Threat & Vulnerability tools and expansion of Logging and Alert tools as highest priorities fitting into the FY15 funding allocation. Engaging a security consultant dedicated to Arlington IT will directly address staff training, tools, and resources required to appropriately manage a security program at the City of Arlington. **Internal Audit Comment:** This recommendation was deemed implemented. An information security services firm was engaged and completed a risk assessment in 2013. The same firm completed an update to that risk assessment in December 2014.

AUDIT RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE	IMPLEMENTATION STATUS
					Through the security program, the IT Department has also developed a methodology to address security vulnerabilities